GRUNDBEGRIFFE DER MATHEMATIK

F. Kasch, B. Pareigis

Vorlesungs-Ausarbeitung, 1974

V O R W O R T

Die beiden Verfasser halten zur Zeit die Anfängervorlesungen in Mathematik an der Universität München. In diesen Anfängervorlesungen werden eine Reihe von mathematischen Grundbegriffen benutzt, zu deren Entwicklung in den Vorlesungen selbst nur wenig Zeit zur Verfügung steht.

Es war der Wunsch der Hörer der Vorlesungen, diese Grundbegriffe sollten zu einer Ausarbeitung zusammengestellt werden.

Unter diesem Gesichtspunkt sind die Ausführungen der ersten III Kapitel zu beurteilen. Insbesondere soll betont werden, daß weder Vollständigkeit bei der Behandlung eines Themas angestrebt wird, noch Begriffe eingehend behandelt werden, die Gegenstand der Anfängervorlesung selbst sind(wie z.B. lineare Vektorräume).

Von diesem Gesichtspunkt sind wir im IV.Kapitel abgewichen, wo der Aufbau des Zahlbegriffes von den Peanoschen Axiomen ausgehend bis zu den komplexen Zahlen dargestellt wird, obwohl diese Überlegungen in der Vorlesung enthalten waren. Dafür sind zwei Gründe maßgebend. Einerseits handelt es sich dabei um Überlegungen, die für Anfänger verhältnismäßig schwierig sind, so daß eine schriftliche Unterlage nicht überflüssig sein dürfte. Zum anderen gibt es Anfängervorlesungen, in denen dieser Aufbau des Zahlbegriffes nicht enthalten ist. Für Studenten derartiger Vorlesungen bietet diese Ausarbeitung die Möglichkeit des Selbststudiums, da alle dazu notwendigen Hilfsmittel hierin enthalten sind.

München, den 22.2.1974

F. Kasch

B. Pareigis

INHALTSVERZEICHNIS

I.Kapitel:Grundbegriffe der Mengenlehre

§ 1 Einleitung S. 3
§ 2 Axiome der Mengenlehre S. 5
§ 3 Geordnete Paare und Produktmengen S. 21

II.Kapitel:Relationen, insbesondere Abbildungen, Aquivalenzrelationen und Ordnungen

§ 1 Definition und allgemeine Eigenschaften S. 24
§ 2 Abbildungen S. 26
§ 3 Aquivalenzrelationen S. 37
§ 4 Ordnungen S. 44

III.Kapitel:Algebraische Grundstrukturen

§ 1 Allgemeine Operationen und Monoide S. 51
§ 2 Gruppen S. 57
§ 3 Ringe und Körper S. 67
§ 4 Moduln S. 79

IV.Kapitel:Aufbau des Zahlensystems

§ 1 Natürliche Zahlen S. 82
§ 2 Ganze Zahlen S. 92
§ 3 Rationale Zahlen S. 99
§ 4 Reelle Zahlen S. 110
§ 5 Komplexe Zahlen S. 124

I. GRUNDBEGRIFFE DER MENGENLEHRE

§ 1 Einleitung

Als Sprache zur Formulierung mathematischer Begriffe und Zusammenhänge wird heute allgemein die Sprache der Mengenlehre benutzt. Es gilt daher zunächst, die Grundbegriffe der Mengenlehre in entsprechendem Umfang bereitzustellen. Das bedeutet, daß wir von der umfangreichen Mengenlehre nur die einfachsten Anfangsgründe darstellen.

Mit der Entwicklung der Mengenlehre sind vor allem die Namen George Boole (1815-1864) und Georg Cantor (1845-1918) verbunden. G.Boole stellte als erster die algebraischen Operationen mit Mengen (Durchschnitt, Vereinigung, Komplementärmenge) heraus, während G.Cantor als eigentlicher Begründer der Mengenlehre(insbesondere der Theorie der Kardinal- und Ordinalzahlen)betrachtet werden muß. Zur weiteren Verbreitung der Mengenlehre bis zum heutigen Stand, wo die Mengenlehre zur mathematischen Allgemeinbildung eines jeden Mathematikers gehört, hat vor allem das Buch von F.Hausdorff "Grundzüge der Mengenlehre", 1.Auflage 1914, beigetragen.

Von G.Cantor stammt die folgende inhaltliche "Definition" einer Menge:
"Eine Menge ist eine Zusammenfassung von bestimmten wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens (welche die Elemente von M genannt werden) zu einem Ganzen."
Daß es sich dabei tatsächlich nicht um eine mathematische Definition handelt, ist klar, denn die darin vorkommenden Begriffe sind selbst undefiniert. Dennoch ist diese Formulierung geeignet,

eine gewisse intuitive Vorstellung vom Begriff der Menge zu geben.

Wir werden hier auf eine explizite Definition einer Menge überhaupt verzichten(müssen!) und uns mit einer impliziten Definition begnügen. Implizite Definitionen sind vom synthetischen Aufbau der Geometrie (z.T. bereits aus der Schule) her wohlbekannt. Auch hier wird nicht definiert, was etwa Punkte, Geraden und Ebenen sind, sondern es werden nur die Beziehungen definiert, die zwischen ihnen bestehen sollen. Z.B. wird gefordert, daß durch zwei verschiedene Punkte genau eine Gerade bestimmt sein soll, die diese Punkte enthält und daß zwei verschiedene Geraden (im affinen Falle) entweder keinen oder genau einen gemeinsamen Punkt enthalten sollen. Durch derartige axiomatische Bedingungen werden Punkte und Geraden implizit (aber in Übereinstimmung mit der intuitiven geometrischen Vorstellung) definiert.

Ganz entsprechend geht man beim Aufbau der Mengenlehre vor. Es wird nicht definiert, was "Mengen" und "Elemente" sind, sondern es werden nur die Beziehungen definiert, die zwischen ihnen bestehen sollen und Konstruktionsprinzipien angegeben, um aus gegebenen Mengen weitere Mengen zu gewinnen. "Mengen" und "Elemente" werden also auf diese Weise nur implizit definiert, allerdings auch jetzt wieder in Übereinstimmung mit der intuitiven Vorstellung etwa im Sinne der Cantorschen "Definition".

§ 2 Axiome der Mengenlehre

2.1. Mengen und Elemente

Im Sinne der Ausführungen in der Einleitung betrachten wir gewisse nicht weiter definierte Objekte, und zwar einerseits Mengen und andererseits Elemente.

Mengen werden meist durch große lateinische Buchstaben $A,B,C,\ldots$, $A_1,A_2,A_3,\ldots$, Elemente meist durch kleine lateinische Buchstaben $a,b,c,\ldots,a_1,a_2,a_3,\ldots$ angegeben.

Ferner benutzen wir das Symbol $\in$ und zu einem Element x und einer Menge A die Zeichenreihe $x \in A$ bzw. $x \notin A$.

(M 1) Axiom der Elementebeziehung und der Existenz

a) Für jedes Element x und jede Menge A besteht genau eine der beiden Beziehungen:

   $x \in A$ In Worten:"x ist Element von A" oder "x liegt in A" oder "x enthalten in A" oder "x in A" oder "x aus A".

   $x \notin A$ In Worten:"x ist nicht Element von A" oder "x liegt nicht in A" oder "x nicht enthalten in A" oder "x nicht in A" oder "x nicht aus A".

b) Es gibt mindestens eine Menge.

c) Zu jedem Element x gibt es mindestens eine Menge A mit $x \in A$.

Wir weisen darauf hin, daß man zum Aufbau der Mengenlehre die Forderung c) vermeiden kann, doch ist sie für unsere Zwecke bequem und entspricht auch völlig der intuitiven Vorstellung,

daß es Elemente "nur als Elemente von Mengen" gibt. Ferner könnte man die Forderung der Existenz einer Menge in b) auf später verschieben oder ganz weglassen. Doch gehen wir ja von der Vorstellung aus, daß es Mengen geben soll, denn sonst würden wir keine Theorie darüber machen. Die Existenz einer Menge folgt auch nach c) , wenn man die Existenz eines Elementes fordert. Umgekehrt folgt aufgrund von b) und weiterer Axiome die Existenz von Elementen, insbesondere wird sich ergeben, daß jede Menge auch Element ist.

2.2. Gleichheit und Teilmengen

Es soll jetzt axiomatisch festgelegt werden, wann zwei Mengen (im Sinne der Mengenlehre) gleich sein sollen. Das wird ganz der Vorstellung entsprechen, daß eine Menge durch die in ihr enthaltenen Elemente bestimmt sein soll.

(M 2) Axiom der Gleichheit

Zwei Mengen A und B sollen genau dann gleich sein, in Zeichen: $A = B$, wenn sie die gleichen Elemente enthalten.
Mit abkürzenden Symbolen geschrieben:

$$A = B \;:\Longleftrightarrow\; \bigwedge a \in A\,[a \in B] \;\wedge\; \bigwedge b \in B\,[b \in A]\,.$$

Sind zwei Mengen A und B nicht gleich, dann schreibt man $A \neq B$.

Folgerung: Für beliebige Mengen A,B,C gilt:

1) Reflexivität: $A = A$
2) Symmetrie: $A = B \Longrightarrow B = A$
3) Transitivität: $A = B \wedge B = C \Longrightarrow A = C$

Beweis: Diese Eigenschaften folgen unmittelbar aus der Gleichheitsbedingung.

Wir können jetzt definieren, was unter einer Teilmenge einer gegebenen Menge zu verstehen ist.

D e f i n i t i o n:

1) Die Menge A heißt Teilmenge oder Untermenge der Menge B, in Zeichen $A \subset B$, genau dann, wenn jedes Element von A auch Element von B ist.
   Mit abkürzenden Symbolen geschrieben:
   $A \subset B :\Longleftrightarrow \bigwedge a \in A \,[a \in B]$.
2) Ist A nicht Teilmenge von B, dann wird $A \not\subset B$ geschrieben.
3) A heißt echte Teilmenge von B, in Zeichen $A \subsetneq B :\Longleftrightarrow$ $A \subset B \wedge A \neq B$.

Aus dieser Definition erhält man unmittelbar die

F o l g e r u n g:

1) Reflexivität: $A \subset A$
2) Antisymmetrie: $A \subset B \wedge B \subset A \Longrightarrow A = B$
3) Transitivität: $A \subset B \wedge B \subset C \Longrightarrow A \subset C$

Man beachte den Unterschied zwischen $\in$ = "ist Element von" und $\subset$ = "ist Teilmenge von".
Das Zeichen $\subset$ wird auch Inklusionszeichen genannt.

Sind $a_1, a_2, \ldots, a_t$ die Elemente einer Menge A, dann benutzt man auch die Schreibweise $A = \{a_1, \ldots, a_t\}$. Dabei wird nicht vorausgesetzt, daß die Elemente $a_1, \ldots, a_t$ alle voneinander verschieden sind. Z.B. gilt

$$\{1,2\} = \{2,1,2,1,1\} ,$$

denn jedes Element der links stehenden Menge ist auch in der rechts stehenden Menge enthalten und umgekehrt. Nach (M 2) besagt dies aber, daß diese Mengen gleich sind.

Eine entsprechende Schreibweise $A = \{...\}$ wird auch bei unendlichen Mengen verwendet, wenn es möglich ist, die Elemente von A eindeutig zu kennzeichnen. Davon werden wir sogleich Gebrauch machen, wenn wir uns im nächsten Abschnitt mit der Frage beschäftigen, wie man aus einer Menge Teilmengen aussondern kann.

2.3. Die Bildung von Teilmengen, Durchschnitt und Komplement

(M 3) Teilmengenaxiom
Sei A eine Menge und $\mathfrak{L}(x)$ eine Aussageform, so daß für jedes $a \in A$ $\mathfrak{L}(a)$ entweder eine wahre oder falsche Aussage ist. Dann gibt es eine Teilmenge B von A, die genau die Elemente $a \in A$ enthält, für die $\mathfrak{L}(a)$ wahr ist. Für B wird

$$B = \{ a \mid a \in A \wedge \mathfrak{L}(a) \}$$

geschrieben.

Da wir die Begriffe "Aussageform" sowie "wahre" und "falsche Aussage" nicht definiert haben, ist die Formulierung dieses Axioms nicht vollständig. Diese Begriffe können jedoch mit genügender Genauigkeit präzisiert werden. Für unsere Zwecke genügt aber die gewählte "weiche" Formulierung. Wir können und wollen in diesem Rahmen sowieso keinen völlig formalisierten, axiomatischen Aufbau der Mengenlehre geben, sondern nur einen Eindruck von den wesentlichen Grundbegriffen eines solchen Aufbaues.

Machen wir uns die Bedeutung des Teilmengenaxioms an Beispielen klar. Dabei wollen wir voraussetzen, daß die folgenden Mengen bereits gegeben sind:

$\mathbb{N} = \{1,2,3,\ldots\}$

= Menge der natürlichen Zahlen

$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}$

= Menge der ganzen Zahlen

$\mathbb{Q}$ = Menge der rationalen Zahlen

$\mathbb{R}$ = Menge der reellen Zahlen

Bei einem systematischen Aufbau der Theorie werden diese erst später eingeführt.

B e i s p i e l e für Teilmengen:

1) $\{x \mid x \in \mathbb{N} \wedge x \text{ gerade}\}$

= Menge der geraden natürlichen Zahlen

2) $\{x \mid x \in \mathbb{N} \wedge x < 10\}$

$= \{1,2,3,..,9\}$

3) $\{x \mid x \in \mathbb{N} \wedge x \text{ Primzahl}\}$

= Menge der Primzahlen

4) $\{x \mid x \in \mathbb{R} \wedge 1 \leq x \leq 2\}$

Diese Menge bezeichnet man auch als das abgeschlossene Intervall $[1,2]$, während

$\{x \mid x \in \mathbb{R} \wedge 1 < x < 2\}$

das offene Intervall $(0,1)$ genannt wird.

5) Sei A eine Menge und seien $a_1, \ldots, a_n$ Elemente von A, dann ist

$$\{a_1, \ldots, a_n\} = \{a \mid a \in A \wedge (a = a_1 \vee a = a_2 \vee \ldots \vee a = a_n)$$

eine Teilmenge von A.

Nimmt man im Teilmengenaxiom für $\mathfrak{A}(x)$ eine Aussageform, die für kein $a \in A$ eine wahre Aussage liefert, so erhält man eine Teilmenge von A, die kein Element enthält und die daher die leere Teilmenge von A, in Zeichen $\emptyset$, genannt wird. Als Aussageform, die nach (M 1) kein $a \in A$ erfüllt, kann man $x \notin A$ wählen.

D e f i n i t i o n:

$\emptyset := \{a \mid a \in A \wedge a \notin A\}$

Nach dieser Definition hängt die Menge $\emptyset$ zunächst von A ab, so daß wir zunächst auch $\emptyset_A$ schreiben wollen. Sei B irgendeine weitere Menge und $\emptyset_B$ die zugehörige leere Teilmenge, dann gilt

$$\emptyset_A = \emptyset_B \ ,$$

denn offensichtlich ist (M 2) erfüllt, da beide Mengen kein Element enthalten. Es ist also sinnvoll, den Index A wegzulassen.

Gleichzeitig hat sich ergeben, daß $\emptyset$ Teilmenge jeder beliebigen Menge ist, was auch sofort aus der Definition der Teilmenge folgt.

Wir hatten in (M 1) gefordert, daß mindestens eine Menge A existiert. Nach der vorstehenden Überlegung existiert dann die Menge $\emptyset$. Da $\emptyset = A$ nicht ausgeschlossen ist, ist also bisher nur die Existenz der leeren Menge $\emptyset$ sichergestellt. Die Existenz weiterer Mengen wird sich aus (M 5) ergeben.

D e f i n i t i o n:

1) Seien A und B Mengen.
   Dann ist der Durchschnitt von A und B, in Zeichen $A \cap B$, die Teilmenge der Elemente aus A, die auch in B liegen.
   $$A \cap B := \{a \mid a \in A \wedge a \in B\}$$
2) Die Komplementärmenge von B in A, in Zeichen $A \setminus B$, ist die Teilmenge der Elemente aus A, die nicht in B liegen.
   $$A \setminus B := \{a \mid a \in A \wedge a \notin B\} .$$

Der Leser mache sich zur Übung die folgenden einfachen Eigenschaften klar.

F o l g e r u n g e n:

1) $A \cap B = B \cap A$

2) $(A \cap B) \cap C = A \cap (B \cap C)$

3) $(A \cap B) \subset A \ \wedge \ (A \cap B) \subset B$;

Gilt für eine Menge C :

$$C \subset A \ \wedge \ C \subset B \ ,$$

dann folgt $C \subset (A \cap B)$.

4) $A \setminus B = A \setminus (A \cap B)$

5) $A \setminus (A \setminus B) = A \cap B$

6) $A \setminus \emptyset = A \ , \ A \setminus A = \emptyset$.

Den Durchschnitt von zwei Mengen kann man zunächst für endlich viele Mengen verallgemeinern:

$$A_1 \cap A_2 \cap \ldots \cap A_n := \{a \mid a \in A_1 \wedge a \in A_2 \wedge \ldots \wedge a \in A_n\} ,$$

denn auch diese Bildung fällt unter das Teilmengenaxiom. Will man den Durchschnitt von "mehr" als nur endlich vielen Mengen bilden, so steht bei dem derzeitigen Stand unseres Wissens die folgende Möglichkeit zur Verfügung (bei der wir allerdings nicht wissen, ob sie tatsächlich mehr liefert).

D e f i n i t i o n:

Sei $\mathfrak{A} \neq \emptyset$ eine Menge, deren Elemente selbst Mengen sind.

Sei $A_0 \in \mathfrak{A}$, dann wird als Durchschnitt von $\mathfrak{A}$, in Zeichen

$\bigcap \mathfrak{A} = \bigcap_{A \in \mathfrak{A}} A$ definiert:

$$\bigcap \mathfrak{A} = \bigcap_{A \in \mathfrak{A}} A := \{a \mid a \in A_0 \wedge \bigwedge A \in \mathfrak{A} \ [a \in A]\}$$

Offensichtlich hängt diese Definition nicht von der Wahl des $A_0 \in \mathfrak{A}$ ab; wir haben diese Schreibweise nur gewählt, um zu betonen, daß diese Definition unter das Teilmengenaxiom fällt. Es genügt jedoch

$$\bigcap_{A \in \mathfrak{A}} A = \{a \mid \bigwedge A \in \mathfrak{A} \ [a \in A]\}$$

zu schreiben. Diese Menge ist dadurch ausgezeichnet, daß sie

die größte Menge ist, die Teilmenge von jedem $A \in \mathfrak{A}$ ist.

2.4. Vereinigungsmengenaxiom

Die zur Durchschnittsbildung "duale" Bildung ist die der Vereinigungsmenge. Daß diese möglich sein soll, fordert das nächste Axiom.

(M 4) **Vereinigungsmengenaxiom**

a) Sind A und B zwei Mengen, dann gibt es eine Menge, Vereinigungsmenge von A und B genannt und mit $A \cup B$ bezeichnet, die genau die Elemente enthält, die in A oder(und !) B enthalten sind:

$$A \cup B = \{ x \mid x \in A \vee x \in B \}$$

b) Sei $\mathfrak{A}$ eine Menge, deren Elemente selbst Mengen sind, dann gibt es eine Menge, Vereinigungsmenge von $\mathfrak{A}$ genannt und mit

$$\bigcup \mathfrak{A} = \bigcup_{A \in \mathfrak{A}} A$$

bezeichnet, die genau die Elemente enthält, die in mindestens einem $A \in \mathfrak{A}$ liegen:

$$\bigcup \mathfrak{A} = \{ x \mid \bigvee A \in \mathfrak{A} \, [x \in A] \}$$

Wir bemerken dazu zunächst, daß wir unter a) die Vereinigungsmenge $A \cup B$ gefordert haben, da diese einerseits vernünftigerweise existieren sollte, andererseits nicht sichergestellt ist, daß sie durch b) mitgeliefert wird. Dazu müßte es eine Menge $\mathfrak{A}$ geben, die genau die Elemente A und B besitzt.
Fordert man axiomatisch eine solche Menge $\mathfrak{A} = \{A,B\}$, dann kann man sich auf b) beschränken. Umgekehrt ergibt sich aus a) zusammen mit dem nachfolgenden Potenzmengenaxiom, daß die Menge $\mathfrak{A} = \{A,B\}$ existiert.

Durch Induktion über n ergibt sich ferner, daß zu endlich vielen Mengen $A_1,\dots,A_n$ auch die Vereinigungsmenge

$$A_1 \cup \dots \cup A_n = \{x \mid x \in A_1 \vee \dots \vee x \in A_n\}$$

existiert.

Während bei der Definition von $\bigcap \mathfrak{A}$ $\mathfrak{A} \neq \emptyset$ vorausgesetzt werden mußte (um das Teilmengenaxiom anwenden zu können), ist bei der Definition von $\bigcup \mathfrak{A}$ auch $\mathfrak{A} = \emptyset$ zugelassen und das Axiom liefert jetzt

$$\bigcup \emptyset = \emptyset \ .$$

Es folgen einige Rechenregeln, deren Beweis dem Leser zur Übung überlassen bleibt.

R e c h e n r e g e l n:

1) $A \cup B = B \cup A$
2) $(A \cup B) \cup C = A \cup (B \cup C)$
3) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$,
   $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.
4) Die de Morganschen Gesetze:
   $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$,
   $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$.

Bereits jetzt haben wir alle Begriffe, um einen topologischen Raum zu definieren. Darauf wird hier nicht weiter eingegangen, doch soll für interessierte Leser wenigstens die Definition angegeben werden.

D e f i n i t i o n:

Eine Menge M zusammen mit einer Menge $\mathfrak{T}$, deren Elemente Teilmengen von M sind, heißt topologischer Raum mit der Topologie $\mathfrak{T}$, wenn die folgenden Eigenschaften gelten:

1) $\bigwedge \mathcal{T} \subset \mathfrak{T} \; [\bigcup \mathcal{T} \in \mathfrak{T}]$

2) $\bigwedge T_1, T_2 \in \mathfrak{T} \; [T_1 \cap T_2 \in \mathfrak{T}]$

3) $M \in \mathfrak{T}$

Die Topologie ist die Theorie der Mathematik, die dem Studium der topologischen Räume und damit zusammenhängenden Fragen gewidmet ist. Sie nimmt einen bedeutenden und umfangreichen Platz im Rahmen der gesamten Mathematik ein.

2.5. P o t e n z m e n g e n

Zum Aufbau der Mengenlehre wird ein weiteres Axiom gebraucht, das einerseits sicherstellt, daß jede Menge auch Element(einer weiteren Menge) ist und andererseits zu einer gegebenen Menge die Konstruktion einer Menge mit einer "größeren" Elementezahl ermöglicht.

(M 5) P o t e n z m e n g e n a x i o m
Zu jeder Menge A gibt es eine Menge, Potenzmenge von A genannt und mit P(A) bezeichnet, die genau alle Teilmengen von A als Elemente enthält und für die

$$P(A) = \{ U \mid U \subset A \}$$

geschrieben wird.

Z.B. ergibt sich damit

$P(\emptyset) = \{ \emptyset \}$ Menge mit einem Element

$P(\{a\}) = \{\emptyset, \{a\}\}$ Menge mit zwei Elementen

$P(\{a,b\}) = \{\emptyset, \{a\}, \{b\}, \{a,b\}\}$ Menge mit vier Elementen (falls $a \neq b$)

Allgemein gilt die

B e h a u p t u n g:
Ist A eine Menge mit n Elementen, dann ist $P(A)$ eine Menge mit 2^n Elementen.

B e w e i s: Vollständige Induktion nach der Zahl n der Elemente.
Induktionsbeginn: $n = 0$, d.h. $A = \emptyset$.
Dann ist $P(\emptyset) = \{\emptyset\}$ eine Menge mit $1 = 2^0$ Elementen.
Induktionsannahme: Die Behauptung sei richtig für Mengen mit höchstens n Elementen.
Induktionsschluß: Sei $A = \{a_1, \ldots, a_n, a_{n+1}\}$ eine Menge mit $n+1$ Elementen. Wir unterscheiden zwei Fälle:
1.Fall: $U \subset A \wedge a_{n+1} \notin U$.
Dann ist $U \subset A_n := \{a_1, \ldots, a_n\}$. Die Menge A_n besitzt nach Induktionsannahme 2^n T eilmengen und jede ihrer Teilmengen ist auch Teilmenge von A. Also gibt es 2^n Teilmengen $U \subset A$ mit $a_{n+1} \notin U$.
2.Fall: $V \subset A \wedge a_{n+1} \in V$.
Wir überlegen jetzt, daß man genau alle solchen Teilmengen V in der Form

$$V = U \cup \{a_{n+1}\}$$

aus genau allen Teilmengen $U \subset A_n$ erhält. Zunächst ist klar, daß aus $U \subset A_n$ folgt $V := U \cup \{a_{n+1}\} \subset A \wedge a_{n+1} \in V$.
Gilt $U_1 \subset A \wedge U_2 \subset A \wedge U_1 \neq U_2$, dann folgt $U_1 \cup \{a_{n+1}\} \neq U_2 \cup \{a_{n+1}\}$. Sei umgekehrt $V \subset A \wedge a_{n+1} \in V$, dann folgt $V \setminus \{a_{n+1}\} \subset A_n \wedge (V \setminus \{a_{n+1}\}) \cup \{a_{n+1}\} = V$, also erhält man genau alle solchen V in der Form $V = U \cup \{a_{n+1}\}$ mit $U \subset A_n$. Da nach Induktionsannahme genau 2^n $U \subset A_n$ existieren, müssen folglich genau 2^n $V \subset A$ mit $a_{n+1} \in V$ existieren.

Da jede Teilmenge von A genau unter einem der beiden Fälle vorkommt, gibt es $2^n + 2^n = 2^{n+1}$ Teilmengen von A.

Bei unserem Aufbau war bisher nur die Existenz der leeren Menge $\emptyset$ gesichert. (M 5) zeigt, daß weitere Mengen wie $P(\emptyset)$, $P(P(\emptyset)) = P(\{\emptyset\})$, $P(P(P(\emptyset))) = P(\{\emptyset, \{\emptyset\}\})$, $P(P(P(P(\emptyset)))) = P(\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}, \ldots)$ mit 1, 2, 2^2, 2^4, ... Elementen und deren Teilmengen existieren. Damit erhält man insbesondere zu jeder natürlichen Zahl n eine Menge mit 2^n Elementen. Will man die Existenz von unendlichen Mengen, die man z.B. braucht, um die Menge $\mathbb{N}$ der natürlichen Zahlen einzuführen, dann bedarf es eines weiteren Axioms. Dieses wird hier jedoch nicht angegeben, denn es handelt sich ja hier nur darum, einige Grundbegriffe der Mengenlehre zu entwickeln und einen möglichen axiomatischen Aufbau anzudeuten.

Da $A \in P(A)$ für jede Menge A gilt, ist jede Menge auch Element. Darüber hinaus gilt folgendes: Sind $A_1, \ldots, A_n$ Mengen, dann gibt es eine Menge $\{A_1, \ldots, A_n\}$, die genau die Mengen $A_1, \ldots, A_n$ als Elemente enthält. Wie man sich leicht klar macht, gilt nämlich, wenn noch

$$M := (\ldots((A_1 \cup A_2) \cup A_3)\ldots) \cup A_n$$

gesetzt wird:

$$\{A_1, \ldots, A_n\} = \{X \mid X \in P(M) \wedge (X = A_1 \vee X = A_2 \vee \ldots \vee X = A_n)\} .$$

Für die Potenzmengenbildung gelten folgende Rechenregeln, deren Beweis dem Leser zur Übung überlassen wird.

R e c h e n r e g e l n:

1) $P(A) \cap P(B) = P(A \cap B)$
2) $P(A) \cup P(B) \subset P(A \cup B)$
3) $\bigcap P(A) = \emptyset$, $\bigcup P(A) = A$
4) $A \subset B \Longrightarrow P(A) \subset P(B)$

2.6. A u s b l i c k

Wir wollen zum Schluß dieses so weit angedeuteten axiomatischen Aufbaues der Mengenlehre noch auf drei Gesichtspunkte hinweisen, die für den weiteren Aufbau der Mengenlehre von Bedeutung sind.

1) E i n o r d n u n g d e s Z a h l b e g r i f f e s

Wir haben bei unseren Überlegungen - wenn auch in vermeidbarer Weise - vom Begriff der natürlichen Zahl Gebrauch gemacht und die Zahlenmenge $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ für Beispiele benutzt. Bei einem axiomatischen Aufbau der Mengenlehre kann man jedoch insbesondere die Menge $\mathbb{N}$ aufgrund von entsprechenden Axiomen im Rahmen der Mengenlehre gewinnen und ferner zeigen, daß $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ tatsächlich Mengen im Sinne dieser Mengenlehre sind. Da ein solcher systematischer, axiomatischer Aufbau sowohl in der Zielsetzung als auch im Umfang über den Rahmen dieser Ausarbeitung hinausgehen würde, entwickeln wir die Zahlbereiche $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ im letzten Kapitel dieser Ausarbeitung, ohne einen solchen systematischen, axiomatischen Aufbau streng einzuhalten.

2) A n t i n o m i e n d e r M e n g e n l e h r e , d e r K l a s s e n b e g r i f f

In der historischen Entwicklung der Mengenlehre hat man sich zunächst bei der Bildung von Mengen keine Beschränkungen auferlegt. Man glaubte, daß durch jede "Bedingung"(Aussageform) die"Erfüllungsmenge dieser Bedingung", d.h. die Menge aller Objekte, die dieser Bedingung genügen, definiert würde. Danach wäre es also z.B. sinnvoll, von der Menge aller Mengen zu sprechen. B.Russell (1872-1969) bemerkte als erster, daß dieses Verfahren zu Widersprüchen (Russellsche Antinomie) führt.

Wir wollen überlegen, daß zu jeder Menge A, deren Elemente selbst wieder Mengen sind, eine Menge B mit $B \notin A$ exi-

stiert, so daß es keine Menge geben kann, die jede Menge als Element enthält. Nach unserem Axiom (M 3) gibt es zu einer solchen Menge A die Teilmenge

$$B := \{a \mid a \in A \wedge a \notin a\} \quad ;$$

da nach Voraussetzung a eine Menge ist und jede Menge auch Element ist, hat die Beziehung $a \notin a$ einen Sinn.

B e h a u p t u n g: $B \notin A$.

B e w e i s: Angenommen $B \in A$, dann unterscheiden wir zwei Fälle.

1.Fall: $B \notin B$, dann folgte, (da $B \in A$) $B \in B$. Widerspruch!

2.Fall: Es bleibt also nur der Fall $B \in B$ übrig, dann folgte (da $B \in A$) $B \notin B$. Widerspruch!

Also führt die Annahme $B \in A$ in jedem Falle zum Widerspruch, d.h. es muß $B \notin A$ gelten.

Wir sind der hier aufgezeigten Gefahr entgangen, indem wir im Axiom (M 3) die "Erfüllungsmenge" zu einer Bedingung $\mathfrak{P}(x)$ auf die Elemente einer bereits vorhandenen Menge beschränkt haben.

Auf der anderen Seite besteht aber der Wunsch, so etwas wie die "Zusammenfassung" aller Mengen oder aller Gruppen oder aller topologischen Räume usw. mathematisch in den Griff zu bekommen. Dies ist in der Tat möglich und hat zu einer Theorie der Klassen geführt. Es gibt dann im Sinne dieser Theorie die Klasse aller Mengen, die Klasse aller Gruppen usw.. Die Axiome für die Klassen müssen notwendig von den Axiomen für die Mengen abweichen, da sonst "Klasse" nur ein anderer Ausdruck für "Menge" wäre. Kurz kann man sagen, daß man mit Klassen"nicht so viel machen darf" wie mit Mengen. In einer solchen Theorie der Klassen werden dann die Mengen als die Klassen ausgesondert, die (mindestens) in einer Klasse als Element enthalten sind.

3) K a r d i n a l z a h l e n u n d O r d i n a l z a h l e n

Das Hauptziel der Mengenlehre als selbständiger mathematischer Theorie besteht darin, unendliche Mengen zu untersuchen und zu klassifizieren. Dies kann gesehen werden unter dem Gesichtspunkt, den Begriff der natürlichen Zahl einerseits als Anzahl (= Kardinalzahl) andererseits versehen mit der Anordnung der natürlichen Zahlen(= Ordinalzahl) auf beliebige unendliche Mengen auszudehnen.

Um dies für intessierte Leser kurz anzudeuten, müssen wir allerdings Begriffe benutzen, die erst später in dieser Ausarbeitung bereitgestellt werden. Man nennt zwei Mengen gleichmächtig, wenn es eine umkehrbar eindeutige Abbildung zwischen diesen Mengen gibt. Eine Klasse(dies ist keine Menge!) aller untereinander gleichmächtigen Mengen kann man dann als eine Kardinalzahl definieren (es gibt noch bessere Definitionen für Kardinalzahlen, wo z.B. die Kardinalzahl eine gewisse wohlgeordnete Menge, aber keine Klasse von Mengen ist). Um zum Begriff der Ordinalzahl zu kommen, werden die beiden folgenden Eigenschaften der Menge der natürlichen Zahlen verallgemeinert:

a) $\mathbb{N}$ ist eine geordnete Menge, in der jede nichtleere Teilmenge ein kleinstes Element besitzt.
   Allgemein nennt man eine geordnete Menge mit dieser Eigenschaft eine wohlgeordnete Menge.

b) Die Anzahl der Elemente der Menge $\{0,1,2,\ldots,n-1\}$ ist gleich n .

Eine Ordinalzahl ist dann eine wohlgeordnete Menge, in der eine Verallgemeinerung von b) (die hier nicht formuliert werden kann) gültig ist.

Die Untersuchung der Kardinalzahlen und der Ordinalzahlen, ins-

besondere ihrer Arithmetik und weiterer damit zusammenhängender Fragen ist der Hauptgegenstand der Mengenlehre.

§ 3 Geordnete Paare und Produktmengen

3.1. Geordnete Paare

Seien a und b zwei Elemente. Wegen (M 1) gibt es dann eine Menge M mit $a \in M$ und eine Menge N mit $b \in N$. Folglich existieren die Mengen

$$\{a\} = \{m \mid m \in M \wedge m = a\} ,$$

$$\{a,b\} = \{x \mid x \in M \cup N \wedge (x = a \vee x = b)$$

Da $\{a\}$ und $\{a,b\}$ Mengen sind, existiert ferner die Menge $\{\{a\}, \{a,b\}\}$ wie schon in 2.5. gezeigt.

Definition:
Das geordnete Paar (a,b) der Elemente a und b ist die Menge, deren Elemente die Mengen $\{a\}$ und $\{a,b\}$ sind:

$$(a,b) := \{\{a\}, \{a,b\}\} ;$$

a heißt das erste Element des Paares (a,b),
b heißt das zweite Element des Paares (a,b).

Es mag zunächst etwas überraschend erscheinen, daß man den so anschaulich erscheinenden Begriff des geordneten Paares auf eine nicht ganz naheliegende mengentheoretische Definition stützt. Bei dieser Gelegenheit kann man die Frage stellen, welche Rolle die Anschauung denn überhaupt in der Mathematik spielt. Die Bedeutung der Anschauung liegt darin, daß sie uns zu Ideen, Begriffen, Sachverhalten und Beweisansätzen inspiriert, die dann jedoch unabhängig von der Anschauung mathematisch präzisiert werden müssen.

Die mathematische Präzisierung des Begriffes "geordnetes Paar" besteht in der vorhergehenden mengentheoretischen Definition,

die ihre Rechtfertigung durch die folgende Behauptung erhält.

B e h a u p t u n g:
Seien (a,b) und (x,y) geordnete Paare; dann gilt:

$$(a,b) = (x,y) \iff a = x \wedge b = y \ .$$

B e w e i s: $\Longleftarrow$: klar.

$\Longrightarrow$: Wir unterscheiden zwei Fälle.

1.Fall: $a = b \Longrightarrow (a,b) = (a,a) = \{\{a\}, \{a,a\}\} = \{\{a\}, \{a\}\} = \{\{a\}\}$.

Wegen $(x,y) = \{\{x\}, \{x,y\}\} = (a,b) = \{\{a\}\}$ folgt $\{x\} = \{a\}$ und $\{x,y\} = \{a\}$, also $x = a$ und $y = a = b$.

2.Fall: $a \neq b \Longrightarrow \{a,b\} = \{x,y\} \Longrightarrow x \neq y \Longrightarrow \{x\} = \{a\} \Longrightarrow a = x \Longrightarrow b = y$, wegen $\{a,b\} = \{x,y\}$.

3.2. Pr o d u k t m e n g e n

Seien jetzt zwei Mengen A und B gegeben und seien $a \in A$, $b \in B$. Dann ist $(a,b) = \{\{a\}, \{a,b\}\}$ offenbar ein Element der Menge $P(P(A \cup B))$, denn $\{a\} \in P(A \cup B)$, $\{a,b\} \in P(A \cup B)$ und folglich $(a,b) \in P(P(A \cup B))$.

D e f i n i t i o n:
Seien A und B Mengen.

$$A \times B := \{x \mid x \in P(P(A \cup B)) \wedge \forall a \in A, b \in B\ [x = (a,b)]\}$$
$$= \{(a,b) \mid a \in A \wedge b \in B\}$$

heißt das Produkt der Mengen A und B oder die Produktmenge von A und B .

Die erste der beiden rechts hingeschriebenen Mengen haben wir nur angegeben, damit nach dem Teilmengenaxiom unmittelbar klar

ist, daß AxB tatsächlich eine Menge ist. Wir werden die Produktmenge im folgenden stets in der zweiten Form schreiben.

F o l g e r u n g:
$A \times B = \emptyset \iff A = \emptyset \vee B = \emptyset$.

B e w e i s: $A \times B = \emptyset \iff$ es gibt kein geordnetes Paar (a,b) mit $a \in A \wedge b \in B \iff$ es gibt kein $a \in A$ oder kein $b \in B$ $\iff A = \emptyset \vee B = \emptyset$

Nachdem wir geordnete Paare definiert haben, können auch geordnete Tripel (a,b,c) durch

$$(a,b,c) := ((a,b),c)$$

definiert werden. Dann gilt analog zu geordneten Paaren:

$$(a,b,c) = (x,y,z) \iff a = x \wedge b = y \wedge c = z \quad .$$

B e w e i s: $((a,b),c) = ((x,y),z) \iff (a,b) = (x,y) \wedge c = z$ $\iff a = x \wedge b = y \wedge c = z$, wobei wir die entsprechende Behauptung für geordnete Paare benutzt haben.

Induktiv lassen sich dann auch geordnete n-Tupel durch

$$(a_1,\ldots,a_n) := ((a_1,\ldots,a_{n-1}), a_n)$$

definieren, die wiederum die entsprechende Eigenschaft wie die geordneten Paare und Tripel haben. Später, wenn wir Abbildungen zur Verfügung haben, können wir geordnete n-Tupel auch als "Familien" definieren.
Produktmengen spielen im folgenden Kapitel bei der Definition von Relationen eine grundlegende Rolle.

II. RELATIONEN, INSBESONDERE ABBILDUNGEN, ÄQUIVALENZRELATIONEN UND ORDNUNGEN

§1 Definition und allgemeine Eigenschaften

Die umgangssprachliche Bedeutung des Wortes Relation besagt, daß zwei Objekte, Personen, Begriffe, Ereignisse usw. miteinander in Beziehung stehen. Dieses "in Beziehung stehen" soll nun mathematisch gefaßt werden.

1.1. Definition:
Eine Relation

$$\varrho = (A,B,U)$$

ist ein geordnetes Tripel von Mengen A,B,U mit $U \subset A \times B$.

Die Elemente von U sind also geordnete Paare (a,b) mit $a \in A$ und $b \in B$. Man kann die Relation ϱ so interpretieren, daß ein Element $a \in A$ genau dann zu einem Element $b \in B$ in Relation steht, wenn (a,b) in U liegt.

Man nennt eine Relation $\varrho = (A,B,U)$ auch eine Relation von A in B oder nach B oder auch zwischen A und B. Ist $A = B$, dann heißt ϱ Relation von A.

1.2. Bezeichnungen:

Quelle von ϱ = $Qu(\varrho)$: = A

Ziel von ϱ = $Zi(\varrho)$: = B

Graph von ϱ = $Gr(\varrho)$: = U

Urbild von ϱ = $Ur(\varrho)$: = $\{a \mid a \in A \wedge \bigvee b \in B\ [(a,b) \in U]\}$

Bild von ϱ = $Bi(\varrho)$: = $\{b \mid b \in B \wedge \bigvee a \in A\ [(a,b) \in U]\}$

1.3. B e i s p i e l e:

1) $\varrho = (A,B,AxB)$ heißt die größte Relation zwischen A und B.

2) $\varrho = (A,B,\emptyset)$ heißt die kleinste oder leere Relation zwischen A und B.

3) $\varrho = (A,A,\{(a,a) \mid a \in A\})$ heißt die identische oder Gleichheitsrelation von A.

Ohne daß wir davon im allgemeinen Fall weiterhin Gebrauch machen, soll noch erwähnt werden, daß man für gewisse Relationen eine Produktrelation definieren kann. Allerdings wird bei unseren weiteren Überlegungen diese Produktbildung im Spezialfall von Abbildungen eine wichtige Rolle spielen.

1.4. D e f i n i t i o n:

Gegeben seien Relationen

$$\varrho = (A,B,U) \quad , \qquad \delta = (B,C,V) \quad .$$

Dann sei

$$\delta\varrho := (A,C,W)$$

mit $W := \{(a,c) \mid (a,c) \in AxC \wedge \bigvee b \in B\,[(a,b) \in U \wedge (b,c) \in V]\}$

Man beachte, daß hierbei $Zi(\varrho) = Qu(\delta)$ vorausgesetzt wurde.

Im folgenden werden drei Typen von Relationen eingehender betrachtet und zwar Abbildungen, Äquivalenzrelationen und Ordnungen.

§ 2 Abbildungen

2.1. Definition:

Eine Abbildung ist eine Relation

$$\varphi = (A,B,U)$$

derart, daß zu jedem $a \in A$ genau ein $b \in B$ mit $(a,b) \in U$ existiert.

Man beachte, daß die Formulierung "zu jedem $a \in A$ existiert genau ein $b \in B$ mit $(a,b) \in U$" auch wie folgt gefaßt werden kann: Zu jedem $a \in A$ existiert ein $b \in B$ mit $(a,b) \in U$ und falls für $b_1 \in B$ auch $(a,b_1) \in U$ gilt, so folgt $b = b_1$.

Bei Abbildungen benutzen wir die allgemein bei Relationen in 1.2. eingeführten Bezeichnungen. Da jetzt jedoch nach Definition der Abbildung $Ur(\varphi) = A = Du(\varphi)$ gilt, ist die Bezeichnung $Ur(\varphi)$ überflüssig.

Ferner führt man bei Abbildungen die folgende Schreibweise ein:

$$\varphi(a) := b \iff (a,b) \in Gr(\varphi)$$

oder

$$a \longmapsto b \quad :\iff (a,b) \in Gr(\varphi) .$$

Diese Schreibweise ist (eindeutig und daher) sinnvoll, da zu jedem $a \in A$ genau ein $b \in B$ mit $(a,b) \in U$ existiert.

Gilt $(a,b) \in Gr(\varphi)$, d.h. nach der neuen Schreibweise $\varphi(a) = b$ oder $a \longmapsto b$, dann heißt b das Bild von a bei φ und a heißt ein Urbild von b bei φ. Man sagt auch, daß bei φ a auf b abgebildet wird oder daß b a zugeordnet wird.

Mit diesen Bezeichnungen gilt offenbar

$$Bi(\varphi) = \{\varphi(a) \mid a \in Qu(\varphi)\}$$
$$Gr(\varphi) = \{(a, \varphi(a)) \mid a \in Qu(\varphi)\} \quad .$$

Liegen $Qu(\varphi)$ und $Zi(\varphi)$ fest, dann ist φ durch $Gr(\varphi)$ eindeutig bestimmt.

Die Abbildung φ wird auch durch die Schreibweisen

$$\varphi : A \longrightarrow B \quad , \quad A \xrightarrow{\varphi} B$$

angegeben. Nicht ganz korrekt, aber bequem, kann φ auch durch

$$\varphi : A \ni a \longmapsto b \in B$$

angegeben werden, wobei oft auch φ noch weggelassen wird.

2.2. D e f i n i t i o n:

1) Die Abbildung φ heißt surjektiv:
   $\Longleftrightarrow Bi(\varphi) = Zi(\varphi)$
   (d.h. φ ist Abbildung auf ganz $Zi(\varphi)$)
2) Die Abbildung φ heißt injektiv :
   $\Longleftrightarrow \wedge a_1, a_2 \in Qu(\varphi) \; [a_1 \neq a_2 \Longrightarrow \varphi(a_1) \neq \varphi(a_2)]$
   (d.h. φ ist eineindeutig)
3) Die Abbildung φ heißt bijektiv:
   $\Longleftrightarrow$ φ ist surjektiv und injektiv .

2.3. B e i s p i e l e:

1) Die identische Abbildung einer Menge A , bezeichnet mit 1_A
   $$1_A : A \ni a \longmapsto a \in A \; .$$
   Offenbar ist dies die identische Relation(siehe 1.3.), die jetzt als identische Abbildung bezeichnet wird.
2) $\mathbb{N} \ni n \longmapsto 2n \in \mathbb{N}$.
3) $\mathbb{N} \ni n \longmapsto 2n \in \{2,4,6,8,\ldots\}$
   Man beachte, daß die Abbildungen in 2) und 3) verschieden sind, da ihre Ziele verschieden sind. Die Abbildung in 2) ist injektiv, aber nicht surjektiv, während die Abbildung in 3) bijektiv ist.

4) $\mathbb{R} \ni r \longmapsto [r] \in \mathbb{Z}$;

dabei sei $[r]$ die größte ganze Zahl $\leq r$. Diese Abbildung ist surjektiv aber nicht injektiv .

5) $\mathbb{Q} \ni q \longmapsto q \in \mathbb{R}$,

Inklusionsabbildung der Teilmenge $\mathbb{Q} \subset \mathbb{R}$ in $\mathbb{R}$.

Diese Abbildung (die von $1_{\mathbb{Q}}$ verschieden ist!) ist injektiv aber nicht surjektiv.

6) $\mathbb{R} \ni r \longmapsto 2^r \in \mathbb{R}^+$,

wobei $\mathbb{R}^+ := \{r \mid r \in \mathbb{R} \wedge r > 0\}$.

Gegeben seien jetzt zwei Abbildungen

$$\alpha : A \longmapsto B \quad \text{und} \quad \beta : B \longmapsto C ,$$

wobei also $Zi(\alpha) = Qu(\beta)$ ist. Dann kann als Spezialfall von 1.4. das Produkt $\beta\alpha$ definiert werden.

2.4. D e f i n i t i o n:

Seien $\alpha : A \longmapsto B$, $\beta : B \longmapsto C$ Abbildungen. Dann sei

$$\beta\alpha := (A,C,W)$$

mit

$$W := \{(a, \beta(\alpha(a))) \mid a \in A\} ,$$

d.h. $(\beta\alpha)(a) = \beta(\alpha(a))$, $a \in A$.

$\beta\alpha$ heißt das Produkt oder die Hintereinanderausführung der Abbildungen α und β .

Offensichtlich ist die Relation $\beta\alpha = (A,C,W)$ wieder eine Abbildung, denn zu jedem $a \in A$ ist $\beta(\alpha(a))$ ein durch a (bei gegebenen festen α und β) eindeutig bestimmtes Element aus C , denn nach Voraussetzung sind $\alpha(a)$ durch a und $\beta(\alpha(a))$ durch $\alpha(a)$ eindeutig bestimmt.

Wir weisen noch einmal ausdrücklich darauf hin, daß $\beta\alpha$ nur unter der Voraussetzung $Bi(\alpha) = Qu(\beta)$ definiert ist und wollen, wenn die Schreibweise $\beta\alpha$ benutzt wird, dies voraussetzen.

2.5. "K a t e g o r i s c h e" E i g e n s c h a f t e n d e s P r o d u k t e s v o n A b b i l d u n g e n

a) Seien

$$\alpha : A \longmapsto B \quad \wedge \quad \beta : B \longmapsto C \quad \wedge \quad \gamma : C \longmapsto D$$

Abbildungen, dann gilt das assoziative Gesetz:

$$\gamma(\beta\alpha) = (\gamma\beta)\alpha$$

b) Für die schon eingeführte identische Abbildung 1_A bzw. 1_B gilt:

$$\alpha = \alpha 1_A = 1_B \alpha$$

B e w e i s:

a) Quelle (= A) und Ziel (= D) von $\gamma(\beta\alpha)$ und $(\gamma\beta)\alpha$ stimmen offensichtlich überein. Fragt sich nur, ob im Graphen beider Abbildungen zu $a \in A$ jeweils die gleiche zweite Komponente aus D gehört. Für $\gamma(\beta\alpha)$ ist diese nach Definition des Produktes gleich

$$\begin{aligned}(\gamma(\beta\alpha))(a) &= \gamma((\beta\alpha)(a)) \\ &= \gamma(\beta(\alpha(a)))\end{aligned}$$

und für $(\gamma\beta)\alpha$ gleich

$$\begin{aligned}((\gamma\beta)\alpha)(a) &= (\gamma\beta)(\alpha(a)) \\ &= \gamma(\beta(\alpha(a)))\end{aligned}$$

Folglich gilt a).

b) Quelle (= A) und Ziel (= B) von α, $\alpha 1_A$ und $1_B\alpha$ stimmen überein. Da auch

$$\alpha(a) = \alpha(1_A(a)) = 1_B(\alpha(a)),$$

folgt b).

Die Bezeichnung "kategorische Eigenschaften" soll hier nicht erläutert werden, doch soll erwähnt werden, daß die Klasse aller Mengen zusammen mit allen Abbildungen eine sogenannte Kategorie bildet, für die die Eigenschaften die definierenden Eigenschaften sind.

Mit Hilfe des Produktes kann man Surjektionen und Injektionen in folgender Weise kennzeichnen.

2.6. S a t z:

Sei $\alpha: A \longmapsto B$ eine Abbildung.

a) α ist dann und nur dann surjektiv, wenn für beliebige Abbildungen β_1, β_2 gilt:

$$\beta_1 \alpha = \beta_2 \alpha \implies \beta_1 = \beta_2 \quad .$$

b) α ist dann und nur dann injektiv, wenn für beliebige Abbildungen γ_1, γ_2 gilt:

$$\alpha \gamma_1 = \alpha \gamma_2 \implies \gamma_1 = \gamma_2 \quad .$$

B e w e i s:

a) Sei α surjektiv und gelte $\beta_1 \alpha = \beta_2 \alpha$, dann folgt zunächst $Zi(\beta_1) = Zi(\beta_1 \alpha) = Zi(\beta_2 \alpha) = Zi(\beta_2)$,

$B = Zi(\alpha) = Qu(\beta_1) = Qu(\beta_2)$.

Sei jetzt $b \in B$, dann gibt es, da α surjektiv ist, ein $a \in A$ mit $\alpha(a) = b$. Nach Voraussetzung folgt dann

$$\beta_1(b) = \beta_1(\alpha(a)) = (\beta_1 \alpha)(a)$$
$$= (\beta_2 \alpha)(a) = \beta_2(\alpha(a)) = \beta_2(b) ,$$

also gilt auch $Gr(\beta_1) = Gr(\beta_2)$ und folglich $\beta_1 = \beta_2$.

Um die Umkehrung zu beweisen, zeigen wir, daß, wenn α nicht surjektiv ist, die Bedingung in a) nicht erfüllt ist. Sei also α nicht surjektiv, d.h. es gebe ein Element $b_0 \in B$, $b_0 \notin Bi(\alpha)$. Dann definiere man Abbildungen

$$\beta_i : B \longrightarrow \{1,2\} \qquad ,(i=1,2)$$

mit

$$\beta_1(b) := 1 \qquad \text{für alle } b \in B$$

$$\beta_2(b) := \begin{cases} 1 & \text{für } b \in B \wedge b \neq b_0 \\ 2 & \text{für } b = b_0 \end{cases} .$$

Dann gilt $\beta_1 \neq \beta_2$; da andererseits b_0 nicht in $Bi(\alpha) = \{\alpha(a) \mid a \in A\}$ enthalten ist, gilt für alle $a \in A$

$$(\beta_1\alpha)(a) = \beta_1(\alpha(a)) = \beta_2(\alpha(a)) = (\beta_2\alpha)(a)$$

also $\beta_1\alpha = \beta_2\alpha$.

b) Sei α jetzt injektiv und gelte $\alpha\gamma_1 = \alpha\gamma_2$, dann folgt zunächst

$$Qu(\gamma_1) = Qu(\alpha\gamma_1) = Qu(\alpha\gamma_2) = Qu(\gamma_2) ,$$

$$A = Qu(\alpha) = Zi(\gamma_1) = Zi(\gamma_2) .$$

Für $c \in Qu(\gamma_1) = Qu(\gamma_2)$ gilt nach Voraussetzung

$$\alpha(\gamma_1(c)) = (\alpha\gamma_1)(c) = (\alpha\gamma_2)(c) = \alpha(\gamma_2(c))$$

und da α injektiv ist, folgt

$$\gamma_1(c) = \gamma_2(c) ,$$

woraus sich $Gr(\gamma_1) = Gr(\gamma_2)$ ergibt. Also gilt $\gamma_1 = \gamma_2$.
Um die Umkehrung zu zeigen, sei α nicht injektiv, d.h. es gebe Elemente $a_1, a_2 \in A$, $a_1 \neq a_2$ mit $\alpha(a_1) = \alpha(a_2)$.
Dann betrachte man die Abbildungen

$$\gamma_i : \{1\} \longrightarrow A \qquad , (i = 1,2)$$

mit

$$\gamma_1(1) := a_1 \qquad , \quad \gamma_2(1) := a_2 .$$

Dann gilt $\gamma_1 \neq \gamma_2$; andererseits folgt

$$(\alpha\gamma_1)(1) = \alpha(a_1) = \alpha(a_2) = \alpha\gamma_2(1) ,$$

also

$$\alpha\gamma_1 = \alpha\gamma_2 .$$

Damit ist auch b) bewiesen.

Für spätere Verwendung beweisen wir noch den folgenden Hilfssatz.

2.7. H i l f s s a t z:

Seien $\alpha : A \longrightarrow B$ und $\beta : B \longrightarrow C$ Abbildungen, dann gilt:

a) Surjektiv $\alpha \wedge$ surjektiv $\beta \Longrightarrow$ surjektiv $\beta\alpha$;
   injektiv $\alpha \wedge$ injektiv $\beta \Longrightarrow$ injektiv $\beta\alpha$

b) Surjektiv $\beta\alpha \Longrightarrow$ surjektiv β ;
   injektiv $\beta\alpha \Longrightarrow$ injektiv α .

B e w e i s:

a) Folgt sofort aus der Definition von surjektiv und injektiv.

b) Surjektiv $\beta\alpha \Longrightarrow Bi(\beta\alpha) = Zi(\beta\alpha) = Zi(\beta)$. Da
   $Bi(\beta\alpha) = \{\beta(\alpha(a)) \mid a \in A\} \subset Bi(\beta) = \{\beta(b) \mid b \in B\}$
   folgt $Bi(\beta) = Zi(\beta)$, d.h. β ist surjektiv.
   Seien $a_1, a_2 \in A$ und $a_1 \neq a_2$, dann folgt nach Voraussetzung $\beta(\alpha(a_1)) = (\beta\alpha)(a_1) \neq (\beta\alpha)(a_2) = \beta(\alpha(a_2))$
   also auch $\alpha(a_1) \neq \alpha(a_2)$, d.h. α ist injektiv.

Wir wollen jetzt noch Überlegen, daß es zu bijektiven Abbildungen (beidseitige) Umkehrabbildungen gibt.

2.8. H i l f s s a t z:

Für die Abbildung $\alpha : A \longrightarrow B$ gilt:

Bijektiv $\alpha \Longleftrightarrow$ es existiert eine Abbildung $\alpha' : B \longrightarrow A$
mit $\alpha'\alpha = 1_A \wedge \alpha\alpha' = 1_B$.

B e w e i s:

$\Longrightarrow$: Sei $\alpha' := (B, A, \{(b,a) \mid (a,b) \in Gr(\alpha)\})$, dann ist α' eine Abbildung, denn aus der Surjektivität von α folgt, daß zu jedem $b \in B$ mindestens ein Paar $(b,a) \in Gr(\alpha')$ existiert und aus der Injektivität von α folgt, daß zu festem $b \in B$ höchstens ein Paar $(b,a) \in Gr(\alpha')$ existiert; insgesamt gibt es also zu $b \in B$ genau ein Paar $(b,a) \in Gr(\alpha')$. Nach Definition von α' folgt sofort

$$\alpha'\alpha = 1_A \wedge \alpha\alpha' = 1_B .$$

$\Longleftarrow$: Da 1_A bzw. 1_B bijektiv ist, folgt nach 2.7., daß α injektiv bzw. surjektiv, insgesamt also bijektiv sein muß.

Ergänzend zu diesem Hilfssatz stellen wir noch fest, daß zu bijektivem α genau ein $\alpha' : B \longrightarrow A$ mit $\alpha'\alpha = 1_A \wedge \alpha\alpha' = 1_B$ existiert. Sei auch $\alpha''\alpha = 1_A \wedge \alpha\alpha'' = 1_B$, dann folgt

$$\alpha' = \alpha' 1_B = \alpha'(\alpha\alpha'') = (\alpha'\alpha)\alpha'' = 1_A\alpha'' = \alpha''$$

(wobei wir von α' nur $\alpha'\alpha = 1_A$ und von α'' nur $\alpha\alpha'' = 1_B$ benutzt haben).

2.9. D e f i n i t i o n:

Sei $\alpha : A \longrightarrow B$ bijektiv. Dann wird die zuvor mit α' bezeichnete Abbildung

$$(B, A, \{(b,a) \mid (a,b) \in Gr(\alpha)\})$$

die zu α inverse Abbildung genannt und mit α^{-1} bezeichnet.

2.10. F o l g e r u n g:

a) Bijektiv $\alpha \Longrightarrow$ bijektiv $\alpha^{-1} \wedge (\alpha^{-1})^{-1} = \alpha$

b) Bijektiv $\alpha \wedge$ bijektiv $\beta \Longrightarrow$ bijektiv $\beta\alpha \wedge (\beta\alpha)^{-1} = \alpha^{-1}\beta^{-1}$

B e w e i s:

a) Die rechte Seite von 2.8. ist bezüglich α und α' symmetrisch; also folgt daraus auch, daß $\alpha' = \alpha^{-1}$ bijektiv und α die eindeutig bestimmte inverse Abbildung zu α^{-1} ist, die nach 2.9. mit $(\alpha^{-1})^{-1}$ bezeichnet wird.

b) Es gilt

$$(\alpha^{-1}\beta^{-1})(\beta\alpha) = \alpha^{-1}(\beta^{-1}\beta)\alpha = \alpha^{-1} 1_B \alpha = \alpha^{-1}\alpha = 1_A ,$$

sowie $(\beta\alpha)(\alpha^{-1}\beta^{-1}) = 1_B$,

so daß wieder nach 2.8. die Behauptung folgt.

Man beachte in diesem Zusammenhang, daß für eine Abbildung

$\alpha : A \longrightarrow B$ aus der Existenz einer Abbildung $\beta : B \longrightarrow A$

mit $\beta\alpha = 1_A$ keineswegs $\alpha\beta = 1_B$, d.h. die Bijektivität

von α folgen muß. Sei z.B.

$$\alpha : \mathbb{N} \ni n \longmapsto 2n \in \mathbb{N}$$

und $\beta : \mathbb{N} \longrightarrow \mathbb{N}$

mit

$$\beta(2n) := n \quad , \quad n \in \mathbb{N}$$

$$\beta(2n-1) := 1 \quad , \quad n \in \mathbb{N} \quad ,$$

dann gilt offenbar

$$\beta\alpha = 1_A \quad ,$$

aber $\alpha\beta \neq 1_B$, denn

$$(\alpha\beta)(2n-1) = \alpha(1) = 2 \quad .$$

Zum Schluß dieses Abschnittes haben wir noch die Einschränkung einer Abbildung zu definieren.

2.11. D e f i n i t i o n:

Sei $\alpha : A \longrightarrow B$ und sei $A_0 \subset A$, dann heißt

$$\alpha|A_0 := (A_0, B, Gr(\alpha) \cap (A_0 \times B)) \quad ,$$

die Einschränkung von α auf A_0 .

Es ist sofort zu sehen, daß $\alpha|A_0$ wieder eine Abbildung ist.

Bei gewissen Überlegungen ist es üblich, eine Abbildung als Familie zu bezeichnen. Leider gibt es keine genaue Angabe darüber, wann man diesen Wechsel in der Bezeichnung vorzunehmen hat. Recht vage kann man sagen, daß man eine Abbildung dann eine Familie nennt, wenn es einem nicht so sehr auf die Abbildung "an sich" ankommt, sondern vielmehr auf die Bilder bei dieser Abbildung. Bezeichnet man eine Abbildung

$$f : \mathfrak{I} \longrightarrow M$$

als Familie, dann nennt man die Quelle $\mathfrak{I}$ von f auch die Indexmenge der Familie f. Für f wird dann meist eine der folgenden Schreibweisen benutzt:

$$f = (f(i) \mid i \in \mathfrak{I}) = (f(i)) =$$
$$= (f_i \mid i \in \mathfrak{I}) = (f_i) = (m_i) \quad (\text{mit } m_i = f(i))$$

Ist $\mathfrak{I}$ endlich, etwa $\mathfrak{I} = \{1,2,\ldots,n\}$, dann wird auch

$$f = (f_1, \ldots, f_n)$$

geschrieben. Für $\mathfrak{I} = \mathbb{N}$ benutzt man die Bezeichnung

$$f = (f_1, f_2, \ldots) = (f_i) .$$

Wir hatten früher die Produktmenge

$$A \times B = \{(a,b) \mid a \in A \wedge b \in B\}$$

definiert. Es soll jetzt eine Menge von Familien angegeben werden, die zu $A \times B$ bijektiv ist, so daß wir damit - bis auf eine Bijektion - eine neue Definition für $A \times B$ erhalten.

Sei $f: \{1,2\} \longrightarrow A \cup B$

mit $f(1) \in A \wedge f(2) \in B$.

Für f schreiben wir zunächst $f = \langle f_1, f_2 \rangle$,

wobei $f_1 := f(1)$, $f_2 := f(2)$ sei .

Sei $A \underline{\times} B$ die Menge aller solchen Abbildungen $f: \{1,2\} \longrightarrow A \cup B$ mit $f_1 \in A \wedge f_2 \in B$.

B e h a u p t u n g:

$\overline{\varphi} : A \underline{\times} B \ni \langle f_1, f_2 \rangle \longmapsto (f_1, f_2) \in A \times B$ ist eine Bijektion.

B e w e i s: Offensichtlich ist $\overline{\varphi}$ eine surjektive Abbildung, denn gilt $a \in A$, $b \in B$, dann ist $f: \{1,2\} \longrightarrow A \cup B$ mit $f(1) := a$, $f(2) := b$ eine Abbildung mit $\overline{\varphi}(f) = \overline{\varphi}(\langle a,b \rangle) = (a,b)$. Aus $(f_1, f_2) = (g_1, g_2)$ folgt $f_1 = g_1 \wedge f_2 = g_2$, also $f = g$, d.h. $\langle f_1, f_2 \rangle = \langle g_1, g_2 \rangle$. Demnach ist $\overline{\varphi}$ auch injektiv.

Nachdem man damit weiß, daß $\bar{\underline{\phi}}$ eine Bijektion ist, läßt man den Unterschied in der Schreibweise $A \underline{x} B$ und $\langle f_1 , f_2 \rangle$ bzw. AxB und (f_1 , f_2) weg und schreibt in beiden Fällen AxB und (f_1 , f_2). Welche Definition dafür zugrunde gelegt wird, kann dem jeweiligen Zweck überlassen bleiben.

Entsprechend kann man auch

$$A_1 xA_2 x...xA_n$$

im Sinne der ursprünglichen mengentheoretischen Definition

$$A_1 x...xA_n := (...((A_1 xA_2)xA_3)x...A_{n-1})xA_n$$

auffassen oder als Menge aller Familien

$$f: \{1,2,...,n\} \longrightarrow A_1 \cup A_2 \cup ... \cup A_n$$

mit $\quad f(i) \in A; \quad (i = 1,...,n)$,

d.h. mit der Schreibweise $f_i = f(i)$ als die Menge

$$\{(f_1 ,...,f_n) \mid f_i \in A_i\} \quad .$$

Die neue Auffassung trägt allerdings weiter, da man jetzt nicht auf endliche Indexmengen $\mathfrak{I}$ beschränkt ist. Sind z.B. die Mengen $\{A_i \mid i \in \mathbb{N}\}$ gegeben, dann sei

$$\prod_{i \in \mathbb{N}} A_i = A_1 xA_2 xA_3 x...$$
$$:= \{(f_1 , f_2 , f_3 , ...) \mid f_i \in A_i\}$$

d.h. die Menge aller Familien

$$f: \mathbb{N} \longrightarrow \bigcup_{i \in \mathbb{N}} A_i$$

mit $\quad f(i) = f_i \in A_i \quad (i \in \mathbb{N})$.

§ 3 Äquivalenzrelationen

3.1. Definition:

Eine Äquivalenzrelation einer Menge A ist eine Relation $\varrho = (A,A,U)$, die folgende Eigenschaften erfüllt:

(1) Reflexivität: $\bigwedge a \in A\ [(a,a) \in U]$

(2) Transitivität:

$\bigwedge a,b,c \in A\ [(a,b) \in U \wedge (b,c) \in U \implies (a,c) \in U]$

(3) Symmetrie: $\bigwedge a,b \in A\ [(a,b) \in U \implies (b,a) \in U]$

Schreibt man für $a,b \in A$:

$$a \sim b :\Longleftrightarrow (a,b) \in U\ ,$$

dann nehmen (1), (2), (3) die folgende übliche Form an:

(1) $\bigwedge a \in A\ [a \sim a]$

(2) $\bigwedge a,b,c \in A\ [a \sim b \wedge b \sim c \implies a \sim c]$

(3) $\bigwedge a,b \in A\ [a \sim b \implies b \sim a]$

Für die Äquivalenzrelation $\varrho = (A,A,U)$ wird dann auch $(A, \sim)$ oder, falls keine Verwechslung möglich ist, auch nur $\sim$ geschrieben.

3.2. Beispiele:

1) Die identische Relation $1_A = (A,A, \{(a,a) \mid a \in A\})$, die, wie schon festgestellt, eine Abbildung ist, ist auch eine Äquivalenzrelation. Für sie gilt: $a \sim b \Longleftrightarrow a = b$, d.h. die Gleichheit von Elementen in A ist eine Äquivalenzrelation. Unter Berücksichtigung von (1) "stehen hier so wenig wie möglich Elemente zueinander in Relation", d.h. 1_A ist die Äquivalenzrelation, deren Graph als Teilmenge im Graphen einer jeden anderen Äquivalenzrelation von A enthalten ist.

2) Die Relation (A,A,AxA) ist offensichtlich auch eine Äqui-

valenzrelation von A, deren Graph im Gegensatz zu dem von 1_A die Graphen aller Äquivalenzrelationen von A enthält.

3) Zu jeder Abbildung

$$\varphi : A \longrightarrow M$$

gehört eine Äquivalenzrelation von A: Sei für $a,b \in A$

$$a \sim b :\Longleftrightarrow \varphi(a) = \varphi(b) ,$$

dann ist sofort zu bestätigen, daß (1), (2), (3) erfüllt sind. Offensichtlich ist dies genau dann die identische Relation von A, wenn φ injektiv ist.

4) Äquivalenzrelationen in der Menge $\mathbb{Z}$ der ganzen Zahlen erhält man auf folgende Weise:
Sei $n \in \mathbb{Z}$, $n \neq 0$, dann wird für $a,b \in \mathbb{Z}$

$$a \sim b :\Longleftrightarrow n/a-b$$

definiert. Dabei bedeutet $n/a-b$, daß n Teiler von $a-b$ ist, d.h. daß ein $q \in \mathbb{Z}$ mit $a-b = qn$ existiert. Statt $a \sim b$ schreibt man jetzt meist

$$a \equiv b \ (\mathrm{mod}\ n) ,$$

in Worten: a kongruent b modulo n. Wir weisen noch darauf hin, daß $a \equiv b (\mathrm{mod}\ n)$, d.h. $n/a-b$ genau dann gilt, wenn a und b bei Division durch n mit Rest (ist $a = qn+r$ mit $0 \leq r < |n|$, dann ist r der Rest) den gleichen Rest besitzen.

3.3. D e f i n i t i o n:
Sei $(A, \sim)$ eine Äquivalenzrelation.
1) Für $a \in A$ heißt

$$\bar{a} := \{x \mid x \in A \wedge x \sim a\}$$

die durch a erzeugte Äquivalenzklasse zur Äquivalenzrelation $(A, \sim)$.

2) $\bar{A} = A/\sim \; := \{\bar{a} \mid a \in A\}$

heißt die Menge der Äquivalenzklassen zur Äquivalenzrelation $(A, \sim)$.

3) Gilt $b \in \bar{a}$, dann heißt b ein Repräsentant der Äquivalenzklasse $\bar{a}$.

3.4. H i l f s s a t z:

Sei $(A, \sim)$ eine Äquivalenzrelation, dann gilt:

1) $b \in \bar{a} \iff \bar{a} = \bar{b}$

(genau alle Repräsentanten einer Äquivalenzklasse erzeugen die Äquivalenzklasse).

2) $\wedge\, a,b \in A \left[\bar{a} \neq \bar{b} \Longrightarrow \bar{a} \cap \bar{b} = \emptyset\right]$

(Äquivalenzklassen, die nicht gleich sind, sind disjunkt).

3) $\bigcup\limits_{a \in A} \bar{a} = A$

(Die Vereinigungsmenge über alle Äquivalenzklassen von $(A, \sim)$ ist A).

B e w e i s:

1) $\Longrightarrow$: $b \in \bar{a} \Longrightarrow b \sim a \Longrightarrow a \sim b$.

Gilt $x \sim a \Longrightarrow x \sim b \Longrightarrow \bar{a} \subset \bar{b}$

Gilt $y \sim b \Longrightarrow y \sim a \Longrightarrow \bar{b} \subset \bar{a}$

also $\bar{a} = \bar{b}$.

$\Longleftarrow$: $\bar{a} = \bar{b} \Longrightarrow b \in \bar{b} = \bar{a}$

2) Sei $\bar{a} \cap \bar{b} \neq \emptyset$ und sei $c \in \bar{a} \cap \bar{b} \Longrightarrow (c \in \bar{a} \Longrightarrow \bar{c} = \bar{a}) \wedge (c \in \bar{b} \Longrightarrow \bar{c} = \bar{b}) \Longrightarrow \bar{c} = \bar{a} = \bar{b}$.

3) Da $a \in \bar{a} \Longrightarrow \bigcup\limits_{a \in A} \bar{a} = A$.

Die Bedingungen 2) und 3) dieses Hilfssatzes besagen, daß $\bar{A} = A/\sim$ eine sogenannte Partition von A ist.

3.5. D e f i n i t i o n:

Eine Partition $\mathfrak{P}$ einer Menge A ist eine Menge von nichtleeren, paarweise disjunkten Teilmengen von A, deren Vereinigung gleich A ist. In Zeichen:

Partition $\mathfrak{P}$ von A : $\Longleftrightarrow$

$$\mathfrak{P} \subset P(A) \setminus \{\emptyset\} \quad \wedge \quad \bigwedge X,Y \in \mathfrak{P} \quad [X \neq Y \Longrightarrow X \cap Y = \emptyset]$$

$$\wedge \bigcup \mathfrak{P} = \bigcup_{X \in \mathfrak{P}} X = A \,.$$

Wie Hilfssatz 3.4. zeigt, ist in der Tat zu jeder Äquivalenzrelation $(A, \sim)$ $A/\sim \; = \{\bar{a} \mid a \in A\}$ eine Partition von A.

Bemerkenswert ist nun, daß umgekehrt zu jeder Partition $\mathfrak{P}$ von A eine Äquivalenzrelation $(A, \sim)$ gehört, für die

$$\mathfrak{P} = A/\sim$$

gilt. Man definiert dazu für $a,b \in A$:

$$a \sim b : \Longleftrightarrow \bigvee X \in \mathfrak{P} \; [a \in X \wedge b \in X] \,,$$

d.h. es seien genau dann zwei Elemente äquivalent, wenn sie beide in einer der Mengen aus $\mathfrak{P}$ liegen. Wir prüfen die Bedingungen für eine Äquivalenzrelation nach:

Reflexivität: Wegen $\bigcup \mathfrak{P} = A$ liegt jedes a in einem $X \in \mathfrak{P}$, also folgt $a \sim a$.

Transitivität: Seien $a \sim b$, d.h. $a,b \in X \in \mathfrak{P}$ und $b \sim c$, d.h. $b,c \in Y \in \mathfrak{P} \Longrightarrow c \in X \cap Y$, wegen der paarweisen Disjunktheit folgt $X = Y \Longrightarrow a,c \in X \Longrightarrow a \sim c$.

Symmetrie: $a \sim b$, d.h. $a,b \in X \in \mathfrak{P} \Longrightarrow b,a \in X \Longrightarrow b \sim a$.

Nach Defintion von $\bar{a}$ und $A/\sim$ gilt dann offensichtlich

$$\mathfrak{P} = A/\sim \,.$$

In 3.2. Beispiel 3 wurde festgestellt, daß zu jeder Abbildung $\varphi : A \longrightarrow M$ eine Äquivalenzrelation gehört, die durch

3.6. $\quad a \sim b \; : \Longleftrightarrow \; \varphi(a) = \varphi(b)$

definiert wird. Wir wollen jetzt überlegen, daß man φ über $A/\sim$ "faktorisieren" kann.

Dazu betrachten wir, wenn zunächst $(A, \sim)$ eine beliebige Aquivalenzrelation ist, die surjektive Abbildung:

$$\nu : A \ni a \longmapsto \bar{a} \in \bar{A} = A/\sim \quad ,$$

die also jedes Element $a \in A$ auf die durch a erzeugte Aquivalenzklasse $\bar{a} = \{x \mid x \in A \wedge x \sim a\}$ abbildet. Man nennt ν die zu $(A, \sim)$ gehörende natürliche Surjektion.

Sei jetzt wieder $(A, \sim)$ die im Sinne von 3.6. zu $\varphi : A \longrightarrow M$ gehörende Aquivalenzrelation mit der zugehörigen Menge der Aquivalenzklassen $\bar{A} = A/\sim$. Dann kann eine injektive Abbildung

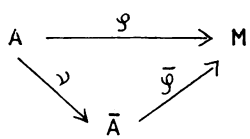
$$\bar{\varphi} : \bar{A} \longrightarrow M$$

so definiert werden, daß

$$\varphi = \bar{\varphi}\,\nu$$

gilt. Man hat damit φ als Produkt der Injektion $\bar{\varphi}$ und der Surjektion ν dargestellt. Das Bestehen der Gleichung $\varphi = \bar{\varphi}\,\nu$ drückt man auch dadurch aus, daß man sagt, das Diagramm

3.7.



ist kommutativ.

3.8. D e f i n i t i o n v o n $\bar{\varphi}$:

$$\bar{\varphi} : \bar{A} \ni \bar{a} \longmapsto \varphi(a) \in M \quad .$$

Um zu sehen, daß dies tatsächlich eine Abbildung ist, muß festgestellt werden, daß es zu $\bar{a}$ nur ein Paar $(\bar{a}, \varphi(a)) \in Gr(\bar{\varphi})$ gibt, d.h. daß $\varphi(a)$ nicht von der Wahl des Repräsentanten a von $\bar{a}$ abhängt. Sei $\bar{a} = \bar{b}$, dann folgt $a \sim b$, also nach 3.6.

$\varphi(a) = \varphi(b)$, womit das Gewünschte bewiesen ist. Sei nun $a \in A$, dann gilt $(\bar{\varphi}\,\nu)(a) = \bar{\varphi}(\nu(a)) = \bar{\varphi}(\bar{a}) = \varphi(a)$, also $\bar{\varphi}\,\nu = \varphi$.

Der soeben geschilderte Sachverhalt kann noch verallgemeinert werden, indem anstelle der zu φ gehörenden Äquivalenzrelation

$$a \sim b \iff \varphi(a) = \varphi(b)$$

eine beliebige "kleinere" ("kleinere" bezieht sich auf die Inklusion der zugehörigen Graphen) Äquivalenzrelation tritt.

3.9. S a t z:
Sei $\varphi : A \longrightarrow M$ eine Abbildung und sei $\sim$ eine Äquivalenzrelation von A mit der Eigenschaft

$$\bigwedge a,b \in A \left[a \sim b \implies \varphi(a) = \varphi(b)\right] .$$

Dann sind

$$\nu : A \ni a \longmapsto \bar{a} \in A/\sim$$

und

$$\bar{\varphi} : A/\sim \ni \bar{a} \longmapsto \varphi(a) \in M$$

Abbildungen mit

$$\varphi = \bar{\varphi}\,\nu .$$

und $\bar{\varphi}$ ist durch die Gleichung $\varphi = \bar{\varphi}\,\nu$ eindeutig bestimmt.
B e w e i s: Die surjektive Abbildung ν hatten wir bereits zuvor betrachtet und als die zu $\sim$ gehörende natürliche Surjektion bezeichnet. Um nun festzustellen, daß $\bar{\varphi}$ eine Abbildung ist, muß überlegt werden, daß $\bar{\varphi}(\bar{a}) = \varphi(a)$ unabhängig von der Wahl des Repräsentanten a von $\bar{a}$ ist. Sei $\bar{a} = \bar{b}$, dann folgt $a \sim b$, also nach Voraussetzung $\varphi(a) = \varphi(b)$.
Folglich ist $\bar{\varphi}$ eine Abbildung. Ferner gilt für $a \in A$:

$$(\bar{\varphi}\,\nu)(a) = \bar{\varphi}(\bar{a}) = \varphi(a) ,$$

also $\varphi = \bar{\varphi}\,\nu$. Sei auch $\varphi = \alpha\,\nu$ mit einer Abbildung

$\alpha : A/\sim \longrightarrow M$, dann folgt $\varphi(a) = (\alpha \nu)(a) = \alpha(\bar{a}) = \bar{\varphi}(\bar{a})$, also $\alpha = \bar{\varphi}$.

Dieser Satz kann auf endlich viele Äquivalenzrelationen ausgedehnt werden.

3.10. S a t z:

Sei $\varphi : A_1 x \ldots x A_n \longrightarrow M$

eine Abbildung und seien

$$(A_1 , \sim_1), \ldots, (A_n , \sim_n)$$

Aquivalenzrelationen mit der Eigenschaft

$\bigwedge (a_1 , \ldots a_n), (b_1 , \ldots, b_n) \in A_1 x \ldots x A_n$

$$\left[a_i \sim_i b_i \quad \text{für} \quad i = 1,..,n \Longrightarrow \varphi(a_1 , \ldots, a_n) = \varphi(b_1 , .. b_n)\right]$$

Dann sind

$\mu : A_1 x \ldots x A_n \ni (a_1 , \ldots, a_n) \longmapsto (\bar{a}_1 , \ldots, \bar{a}_n) \in (A_1 / \sim_1) x .. x (A_n / \sim_n)$

und

$\hat{\varphi} : (A_1 / \sim_1) x \ldots x (A_n / \sim_n) \ni (\bar{a}_1 , \ldots, \bar{a}_n) \longmapsto (a_1 , \ldots, a_n) \in M$

Abbildungen mit $\varphi = \hat{\varphi} \mu$ und $\hat{\varphi}$ ist durch die Gleichung $\varphi = \hat{\varphi} \mu$ eindeutig bestimmt.

B e w e i s: Wie im Beweis von 3.9. sind die Behauptungen sofort zu bestätigen, wobei jetzt die "Verträglichkeitsvoraussetzung" $\left[a_i \sim_i b_i \quad \text{für } i = 1,\ldots,n \Longrightarrow \varphi(a_1 , \ldots, a_n) = \varphi(b_1 , \ldots, b_n)\right]$ impliziert, daß $\hat{\varphi}$ eine Abbildung ist.

§ 4 Ordnungen

4.1. Definition:

Eine Ordnung (oder Anordnung) einer Menge A ist eine Relation $\varphi = (A,A,U)$, die folgende Eigenschaften erfüllt:

(1) Reflexivität: $\bigwedge a \in A \ [(a,a) \in U]$

(2) Transitivität: $\bigwedge a,b,c \in A \ [(a,b) \in U \wedge (b,c) \in U \Longrightarrow (a,c) \in U]$

(3) Antisymmetrie: $\bigwedge a,b \in A \ [(a,b) \in U \wedge (b,a) \in U \Longrightarrow a = b]$

4.2. Bezeichnungen:

Für $a,b \in A$ setze man

$$a \leq b :\Longleftrightarrow (a,b) \in U$$

$$a \not\leq b :\Longleftrightarrow (a,b) \notin U .$$

Für die Ordnung φ von A schreibt man auch $\varphi = (A, \leq)$ oder nur kurz $\leq$, und man nennt A eine geordnete Menge mit der Ordnung $\leq$.

Mit der hier eingeführten Schreibweise nehmen die Bedingungen (1), (2), (3) die folgende übliche Form an:

(1) $\bigwedge a \in A \ [a \leq a]$

(2) $\bigwedge a,b,c \in A \ [a \leq b \wedge b \leq c \Longrightarrow a \leq c]$

(3) $\bigwedge a,b \in A \ [a \leq b \wedge b \leq a \Longrightarrow a = b]$

Ist $\varphi = (A,A,U)$ eine Ordnung von A und ist B eine Teilmenge von A, dann ist die Einschränkung der Ordnung φ auf B,

$$\varphi|B := (B,B, U \cap (B \times B)),$$

offensichtlich eine Ordnung von B.

Sprechen wir von Teilmengen einer geordneten Menge, dann verstehen wir darunter stets geordnete Teilmengen in diesem Sinne.

Wie unmittelbar klar, ist die Gleichheitsrelation in einer Menge A eine Ordnung für A, für die gilt:

$$a \leq b \Longleftrightarrow a = b .$$

Betrachtet man eine solche Ordnung als trivial, so kann man Ordnungen, wie wir sie jetzt definieren, als das "Gegenteil" der trivialen Ordnung ansehen.

4.3. D e f i n i t i o n:

Eine Ordnung $\leq$ von A heißt totale Ordnung von A : $\Leftrightarrow$
$\bigwedge a,b \in A \; [a \leq b \vee b \leq a]$.
Ist $\leq$ eine totale Ordnung von A, dann heißt A (bei $\leq$) total geordnet oder auch eine Kette.

Offenbar sind Teilmengen von total geordneten Mengen wieder total geordnet. Die übliche Ordnung der reellen Zahlen ist eine totale Ordnung.

Um ein nichttriviales Beispiel für eine Ordnung zu erhalten, die keine totale Ordnung ist, betrachten wir zu einer Menge M die Potenzmenge P (M) . Diese ist mit der Inklusion $\subset$ von Teilmengen von M als Ordnungsrelation eine geordnete Menge:

(1) $\bigwedge A \in P(M) \; [A \subset A]$

(2) $\bigwedge A,B,C \in P(M) \; [A \subset B \wedge B \subset C \Longrightarrow A \subset C]$

(3) $\bigwedge A,B \in P(M) \; [A \subset B \wedge B \subset A \Longrightarrow A = B]$

Wie leicht zu sehen, ist P (M) mit dieser Ordnung dann und nur dann total geordnet, wenn $M = \emptyset$ oder M genau ein Element besitzt. Besitzt also M mindestens zwei Elemente, so ist P (M) nicht total geordnet.

Später werden wir oft von der folgenden Eigenschaft einer total geordneten Menge Gebrauch machen.

4.4. L e m m a:

Ist A eine total geordnete Menge, dann können je endlich viele Elemente aus A stets so numeriert werden, daß gilt:

$$a_1 \leq a_2 \leq \ldots \leq a_n \; .$$

B e w e i s: Beweis durch Induktion, wobei der Induktionsbeginn $n = 1$ klar ist. Seien jetzt $a_1, \ldots, a_n$ gegeben und gelte schon (Induktionsvoraussetzung)

$$a_1 \leq a_2 \leq \ldots \leq a_{n-1} .$$

Entweder ist $a_{n-1} \leq a_n$, dann ist man fertig, oder es gilt $a_n \leq a_{n-1}$. Dann können $a_1, \ldots, a_{n-2}, a_n$ nach Voraussetzung in der gewünschten Weise numeriert werden, seien dies etwa

$$b_1 \leq b_2 \leq \ldots \leq b_{n-1} .$$

Für $b_n := a_{n-1}$ erhält man dann wie gewünscht $b_1 \leq b_2 \leq \ldots \leq b_n$.

Kehren wir zu einer beliebigen, geordneten Menge $(A, \leq)$ zurück.

4.5. D e f i n i t i o n:

Sei $(A, \leq)$ eine geordnete Menge.

1) $a_0 \in A$ heißt ein maximales bzw. minimales Element in A:

$$\bigwedge a \in A \; [a_0 \leq a \Rightarrow a_0 = a] \quad \text{bzw.}$$

$$\bigwedge a \in A \; [a \leq a_0 \Rightarrow a = a_0]$$

2) $a_0 \in A$ heißt größtes oder kleinstes Element in A:

$$\bigwedge a \in A \; [a \leq a_0] \quad \text{bzw.}$$

$$\bigwedge a \in A \; [a_0 \leq a]$$

3) Ein Element $a_0 \in A$ heißt eine obere bzw. untere Schranke einer Teilmenge $B \subset A$:

$$\bigwedge b \in B \; [b \leq a_0] \quad \text{bzw.}$$

$$\bigwedge b \in B \; [a_0 \leq b]$$

4) Sei $B \subset A$. Besitzt die Menge der oberen Schranken von B in A ein kleinstes Element, so heißt dieses Supremum von B in A, in Zeichen sup(B) (wobei vorausgesetzt wird, daß es klar ist, um welche Menge A und Ordnung $\leq$ von A es sich handelt). Besitzt die Menge der unteren Schranken von B in A ein größtes Element, so heißt dieses Infimum von B in A, in Zeichen inf(B).

Eine geordnete Menge braucht weder größte noch kleinste, weder maximale noch minimale Elemente zu besitzen, wie die Menge der reellen Zahlen zeigt. Sie kann auch mehrere maximale oder minimale Elemente besitzen. Z.B. ist in der Gleichheitsrelation einer Menge (als Ordnung) jedes Element maximales und minimales Element und, falls die Menge mehr als ein Element besitzt, gibt es kein größtes und kein kleinstes Element.
Falls in einer geordneten Menge ein größtes bzw. kleinstes Element existiert, ist es aber, wie sofort aus der Definition folgt, eindeutig bestimmt.

4.6. D e f i n i t i o n:
Eine Ordnung einer Menge A heißt eine Wohlordnung, wenn jede nichtleere Teilmenge von A ein kleinstes Element besitzt.

Z.B. ist die Menge $\mathbb{N}$ der natürlichen Zahlen bei der natürlichen Ordnung wohlgeordnet. Hingegen ist $\mathbb{R}$ nicht wohlgeordnet und auch kein Intervall in $\mathbb{R}$.

Es ist klar, daß jede Wohlordnung einer Menge A eine totale Ordnung ist; hat man nämlich zwei Elemente $a,b \in A$, so muß die Menge $\{a,b\}$ ein kleinstes Element besitzen, d.h. es gilt entweder $a \leq b$ oder $b \leq a$.

Bei vielen Überlegungen in der Mathematik werden transfinite Hilfsmittel gebraucht; das sind Hilfsmittel, die es erlauben Schwierigkeiten zu bewältigen, die durch unendliche Mengen, Strukturen, Prozesse und dergleichen bedingt sind.
Unter"transfiniten Hilfsmitteln" verstehen wir die folgenden äquivalenten Aussagen:
(1) Auswahlaxiom
(2) Wohlordnungssatz:Jede Menge kann wohlgeordnet werden
(d.h. besitzt eine Wohlordnung)

(3) Zornsches Lemma

(4) Transfinite Induktion

Diese äquivalenten Aussagen sind selbst nicht beweisbar. Welche man davon als Axiom und welche man entsprechend als Sätze betrachtet, ist vom logischen Standpunkt aus willkürlich. Historisch ist man vom Auswahlaxiom als Axiom ausgegangen.

Wir wollen hier das Zornsche Lemma als Axiom betrachten und davon uneingeschränkt Gebrauch machen.

4.7. Z o r n s c h e s L e m m a:
Sei A eine geordnete Menge.
Besitzt jede total geordnete Teilmenge von A eine obere Schranke, dann besitzt A ein maximales Element.

Zum Schluß dieses Abschnittes sollen noch einige verbandstheoretische Begriffe zusammengestellt werden.

4.8. D e f i n i t i o n:

1) Ein Verband ist eine geordnete Menge, in der jede zweielementige Teilmenge ein Supremum und ein Infimum besitzt.
2) Ein Verband heißt vollständig, wenn jede Teilmenge ein Supremum und ein Infimum besitzt.

Durch Induktion ist leicht zu zeigen, daß in einem Verband jede nichtleere endliche Teilmenge ein Supremum und ein Infimum besitzt.

Ein vollständiger Verband enthält offenbar ein größtes Element
(= Supremum der ganzen Menge = Infimum der leeren Teilmenge)
und ein kleinstes Element
(= Infimum der ganzen Menge = Supremum der leeren Teilmenge)

Setzt man in einem Verband A:

$$a \cup b := \sup\{a,b\}$$
$$a \cap b := \inf\{a,b\}, \qquad a,b \in A$$

dann lassen sich die folgenden Begriffe, die Vertauschbarkeitsbedingungen für Supremum und Infimum enthalten, kurz formulieren.

4.9. D e f i n i t i o n:

1) Ein Verband $(A, \leq)$ heißt modular :

$$\Longleftrightarrow \quad \bigwedge a,b,c \in A \; [a = a \cap c \Longrightarrow (a \cup b) \cap c = a \cup (b \cap c)]$$

2) Ein Verband $(A, \leq)$ heißt distributiv:

$$\Longleftrightarrow \quad \bigwedge a,b,c \in A \; [(a \cup b) \cap c = (a \cap c) \cup (b \cap c)]$$

Dabei ist bemerkenswert, daß die einen distributiven Verband definierende Bedingung

$$(a \cup b) \cap c = (a \cap c) \cup (b \cap c) \qquad , a,b,c \in A$$

mit der Bedingung

$$(a \cap b) \cup c = (a \cup c) \cap (b \cup c) \qquad , a,b,c \in A$$

äquivalent ist.

Gewisse distributive Verbände spielen eine besondere Rolle, die sogenannten Boolschen Verbände.

4.10. D e f i n i t i o n:

Ein Verband $(A, \leq)$ heißt Boolscher Verband : $\Longleftrightarrow$

1) A ist distributiv
2) A enthält ein größtes Element e und ein kleinstes Element o.
3) $\bigwedge a \in A \; \bigvee \bar{a} \in A \; [a \cup \bar{a} = e \wedge a \cap \bar{a} = o]$.

Z.B. ist für eine Menge M die Potenzmenge P(M) mit der Inklusion $\subset$ als Ordnungsrelation ein Boolscher Verband. In diesem Falle ist $e = M$, $o = \emptyset$ und für jedes $A \in P(M)$ $\bar{A} = M \setminus A$ zu setzen. Die Symbole $\cap$ und $\cup$ im Boolschen

Verband stimmen jetzt mit Durchschnitt und Vereinigung überein.

Man kann übrigens zeigen, daß jeder endliche Boolsche Verband zu einem Verband $(P(M), \subset)$ isomorph ist (Satz von Stone).

Als Abschwächung des Verbandsbegriffes spielt der Begriff der filtrierten (oder gefilterten) Menge eine wichtige Rolle für die Definition von Limites.

4.11. D e f i n i t i o n:
Eine geordnete Menge A heißt nach links (oder unten) bzw. nach rechts (oder oben) filtriert :
jede zweielementige Teilmenge von A hat eine untere bzw. obere Schranke.

III. ALGEBRAISCHE GRUNDSTRUKTUREN

§1 Allgemeine Operationen und Monoide

Sei G eine Menge.

1.1. Definition:
Eine (binäre) Operation in G ist eine Abbildung

$$\gamma : G \times G \longrightarrow G$$

Für das Bild $\gamma((a,b))$ von $(a,b) \in G \times G$ bei γ werden verschiedene Bezeichnungen verwendet, die von weiteren Eigenschaften von γ und dem Zusammenhang, in dem γ auftritt, abhängen. Z.B. kommen für $\gamma((a,b))$ folgende Bezeichnungen vor:
$a+b$, $a \cdot b$, ab , $a \circ b$, $a \cap b$, $a \cup b$.
Wir schreiben $\gamma(a,b) := \gamma((a,b))$
und wollen jetzt einige wichtige Bedingungen für γ formulieren.

1.2. Definition:
(1) Assoziatives Gesetz:
$\bigwedge a,b,c \in G \left[\gamma(a, \gamma(b,c)) = \gamma(\gamma(a,b),c)\right]$
(2) Existenz eines neutralen Elementes e:
$\bigvee e \in G \ \bigwedge a \in G \left[\gamma(a,e) = \gamma(e,a) = a\right]$
(3) Existenz eines inversen Elementes (falls ein neutrales Element e existiert):
$\bigwedge a \in G \ \bigvee a^* \in G \left[\gamma(a,a^*) = \gamma(a^*,a) = e\right]$
(4) Kommutatives Gesetz:
$\bigwedge a,b \in G \left[\gamma(a,b) = \gamma(b,a)\right]$.

Im Fall $ab := \gamma(a,b)$ bzw. $a+b := \gamma(a,b)$ nehmen diese Bedingungen die folgende Form an .

(1)	$a(bc) = (ab)c$	$a+(b+c) = (a+b)+c$
(2)	$ae = ea = a$	$a+e = e+a = a$
(3)	$aa^* = a^*a = e$	$a+a^* = a^*+a = e$
(4)	$ab = ba$	$a+b = b+a$

Gewisse Kombinationen dieser Bedingungen ergeben bekannte Operationen.

1.3. D e f i n i t i o n:

Sei γ eine Operation der Menge $G \neq \emptyset$. Dann heißt (G, γ) eine

1) Halbgruppe $:\Longleftrightarrow$ (1) gilt
2) Monoid $:\Longleftrightarrow$ (1) $\wedge$ (2) gelten
3) Gruppe $:\Longleftrightarrow$ (1) $\wedge$ (2) $\wedge$ (3) gelten
4) Kommutative oder Abelsche Gruppe :
$\Longleftrightarrow$ (1) $\wedge$ (2) $\wedge$ (3) $\wedge$ (4) gelten.

1.4. B e i s p i e l e:

1) $\mathbb{N}$ ist mit der Addition als Operation eine Halbgruppe, aber kein Monoid.
2) $\mathbb{N}$ ist mit der Multiplikation als Operation ein Monoid mit dem neutralen Element 1 , aber keine Gruppe.
3) Die Menge aller Abbildungen einer Menge $M \neq \emptyset$ nach M ist mit dem Produkt (= Hintereinanderausführung) von Abbildungen als Operation ein Monoid mit der identischen Abbildung als neutralem Element.

Es sollen jetzt einige Eigenschaften für ein Monoid G bewiesen werden, die wir später in verschiedenen Fällen brauchen. Dazu wird die Operation von G in der Form ab geschrieben, also als Multiplikation; dennoch werden die Resultate später auch für Monoide mit additiv geschriebener Operation benutzt.

Sei also G im folgenden ein Monoid.

1.5. B e h a u p t u n g:
In einem Monoid G ist das neutrale Element eindeutig bestimmt.

B e w e i s: Seien e und e' neutrale Elemente von G, dann folgt

$$e' = ee' = e .$$

Hierbei wird nur benutzt, daß e „Linksidentität" von e' und e' „Rechtsidentität" von e ist.

1.6. D e f i n i t i o n:
Seien $a,a',a'',a^* \in G$. Dann heißt a' Rechtsinverses bzw. a'' Linksinverses bzw. a^* Inverses von a :$\Leftrightarrow$
$aa' = e$ bzw. $a''a = e$ bzw. $aa^* = a^*a = e$.
Existiert ein Rechtsinverses bzw. ein Linksinverses bzw. ein Inverses von a , dann heißt a rechtsinvertierbar oder Rechtseinheit bzw. linksinvertierbar oder Linkseinheit bzw. invertierbar oder Einheit.

1.7. B e h a u p t u n g:
Aus $aa' = e \quad \wedge \quad a''a = e$
folgt $a' = a''$.
Folglich ist dann $a' = a''$ ein Inverses von a und falls a ein Inverses besitzt, so ist dieses eindeutig bestimmt.

B e w e i s: $a' = ea' = (a''a)a' = a''(aa') = a''e = a''$.

Wird die Operation des Monoids G multiplikativ geschrieben und ist $a \in G$ invertierbar, dann wird mit a^{-1} das Inverse von a bezeichnet. Wird die Operation von G als Addition geschrieben, dann bezeichne $-a$ das Inverse von a und es wird $b-a := b+(-a)$ gesetzt.

1.8. B e h a u p t u n g:
Ist a invertierbar, dann auch a^{-1}, und es gilt

$$(a^{-1})^{-1} = a .$$

Sind a und b invertierbar, dann auch ab und es gilt

$$(ab)^{-1} = b^{-1} a^{-1} .$$

B e w e i s: Wegen $aa^{-1} = a^{-1} a = e$ ist a^{-1} invertierbar und es gilt $(a^{-1})^{-1} = a$, da das Inverse eindeutig bestimmt ist und a ein Inverses von a^{-1} ist.
Wegen $(ab)(b^{-1} a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$
und $(b^{-1} a^{-1})(ab) = b^{-1}(a^{-1} a)b = b^{-1} eb = b^{-1} b = e$
ist ab invertierbar mit dem Inversen $b^{-1} a^{-1}$, also gilt $(ab)^{-1} = b^{-1} a^{-1}$.

1.9. B e h a u p t u n g:
Die invertierbaren Elemente in einem Monoid G bilden bei der Operation von G eine Gruppe mit der gleichen Identität wie G.

B e w e i s: Folgt sofort aus der vorhergehenden Behauptung.

1.10. F o l g e r u n g:
Die invertierbaren Abbildungen (= Bijektionen, wie früher festgestellt) einer Menge M auf sich bilden bei der Hintereinanderausführung als Verknüpfung eine Gruppe.

1.11. D e f i n i t i o n:
Ist M eine endliche Menge mit der Elementezahl n, dann heißen die Bijektionen von M auf sich Permutationen und die Gruppe aller Permutationen heißt die symmetrische Gruppe von n Elementen, in Zeichen S_n.

B e m e r k u n g: Welche Menge M mit n Elementen man zugrunde legt, geht in die Bezeichnung S_n nicht ein, da dies unwesentlich ist. Als Menge M mit n Elementen wird daher meist die Menge $\{1,2,\ldots,n\}$ zugrunde gelegt.

Für eine Permutation π der Menge $\{1,2,\ldots,n\}$ wird auch die folgende Schreibweise benutzt:

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ a_1 & a_2 & \ldots & a_n \end{pmatrix} := \pi \quad ,$$

wenn $\pi : \{1,\ldots,n\} \longrightarrow \{1,\ldots,n\}$
die Permutation mit $\pi(i) = a_i$, $i = 1,\ldots,n$ ist, d.h. man schreibe in dem Schema

$$\begin{pmatrix} 1 & \ldots & n \\ \pi(1) & \ldots & \pi(n) \end{pmatrix}$$

das Bild jeweils unter das Urbild.

Das assoziative Gesetz besagt für eine multiplikativ geschriebene Halbgruppe, daß es bei einem Produkt von drei Faktoren nicht auf die Reihenfolge ankommt, so daß man Klammern weglassen kann. Diese Eigenschaft überträgt sich induktiv auf Produkte von mehr als drei Faktoren, wovon wir bereits gebrauch gemacht haben.

Für die Elemente einer multiplikativ geschriebenen Halbgruppe G benutzen wir die (übliche) Potenzschreibweise.
Sei $a \in G$, $n \in \mathbb{N}$, dann sei

$$a^n := \underbrace{aa\ldots a}_{n \text{ Faktoren}}$$

Für $m,n \in \mathbb{N}$ gilt dann $a^m a^n = a^{m+n}$.
Ist G sogar ein Monoid, dann sei $a^0 := e$. Für ein invertierbares Element a setzt man

$$a^{-n} := \underbrace{a^{-1}a^{-1}\ldots a^{-1}}_{n \text{ Faktoren}} = (a^n)^{-1} \quad .$$

In additiver Schreibweise hat man entsprechend, wenn das neutrale Element des Monoids G mit 0 bezeichnet wird:

$$na := \underbrace{a+a+\ldots+a}_{n \text{ Summanden}} \quad , n \in \mathbb{N} \quad \wedge \quad 0a := 0$$

Beachte dabei, daß in $0a = 0$ die erste 0 in $\mathbb{Z}$ und die zweite 0 in G liegt. Für invertierbares a gilt entsprechend für $n \in \mathbb{N}$

$$\begin{aligned}(-n)a &:= (-a)+(-a)+\ldots+(-a) \\ &= \underbrace{-a-a-\ldots-a}_{n \text{ Summanden}} = -(na)\end{aligned}$$

§ 2 Gruppen

Es sollen jetzt Eigenschaften von Gruppen angegeben werden, wobei die Gruppenoperation als Multiplikation geschrieben wird. Im folgenden sei also G eine muliplikative Gruppe mit dem neutralen Element e.

2.1. Behauptung:
$\bigwedge a \in G \, [a^2 = a \iff a = e]$

Beweis: $\Longrightarrow$: $a^2 = a \Longrightarrow a^2 a^{-1} = a = a a^{-1} = e$.
$\Longleftarrow$: $e^2 = e$, da e das neutrale Element ist.

2.2. Behauptung:
Für $a \in G$ sind die folgenden Abbildungen Bijektionen:
$a^{(\ell)} : G \ni x \longmapsto ax \in G$, $a^{(r)} : G \ni x \longmapsto xa \in G$
$\tau_a : G \ni x \longmapsto a^{-1} x a \in G$

Beweis:
$a^{(\ell)}$: Da ax eindeutig bestimmt ist, ist $a^{(\ell)}$ eine Abbildung. Aus $ax = ay$ folgt $a^{-1}ax = x = a^{-1}ay = y$, also ist $a^{(\ell)}$ injektiv. Sei $y \in G$, dann folgt $a(a^{-1}y) = y$, d.h. y ist Bild bei $a^{(\ell)}$, also ist $a^{(\ell)}$ surjektiv.
Analog für $a^{(r)}$.
τ_a : $\tau_a = a^{(r)}(a^{-1})^{(\ell)}$ = Hintereinanderausführung von $(a^{-1})^{(\ell)}$ und $a^{(r)}$.

Untergruppen

Ist eine algebraische (oder sonstige) Struktur G gegeben, dann sind "Unterstrukturen" von G von Interesse, das sind Teilmengen H von G, die bei "Einschränkung" der Struktur von G auf H selbst wieder eine solche (oder damit zusammenhängende) Struktur darstellen.

2.3. D e f i n i t i o n:

1) Eine Teilmenge H von G heißt Untergruppe von G, wenn H bei der Einschränkung der Gruppenoperation von G auf H, d.h. also bei

$$H \times H \ni (h_1, h_2) \longmapsto h_1 h_2 \in H$$

eine Gruppe ist.

Ist H Untergruppe von G, dann wird $H \leq G$ geschrieben.

2) Eine Untergruppe H von G heißt Normalteiler von G:

$$\bigwedge a \in G \left[a^{-1}Ha := \{a^{-1}ha \mid h \in H\} = H\right] .$$

Wir weisen zunächst darauf hin, daß die Definition der Untergruppe die Forderung einschließt, daß für $h_1, h_2 \in H$ auch $h_1 h_2 \in H$ gilt. Sei $H \leq G$ und sei e' das neutrale Element von H, dann gilt $e'e' = e'$; nach 2.1. genügt aber nur das neutrale Element e von G dieser Gleichung, so daß $e' = e$ folgt. Dann folgt nach 1.7., daß das inverse Element von $h \in H$ in H mit dem inversen Element h^{-1} von h in G übereinstimmt. In der Untergruppe H von G stimmt also nicht nur die Operation mit der von G überein, sondern auch das neutrale Element und die Inversenbildung.

2.4. U n t e r g r u p p e n k r i t e r i u m:

Sei G eine Gruppe und H eine nichtleere Teilmenge von G, dann gilt:

(1) **H ist Untergruppe von G** $\Longleftrightarrow$

$$\bigwedge a,b \in H \left[ab^{-1} \in H\right] .$$

(2) **Ist H endlich, dann gilt:**

H ist Untergruppe von G $\Longleftrightarrow$

$$\bigwedge a,b \in G \left[ab \in H\right] .$$

B e w e i s:

(1) $\Longrightarrow$: klar nach Definition einer Untergruppe.

(1) $\Longleftarrow$: $a \in H \Longrightarrow$ (für $b=a$) $aa^{-1} = e \in H$. Da $e \in H \Longrightarrow$ ($a \in H \Longrightarrow ea^{-1} = a^{-1} \in H$) . Dann folgt aus $a,b \in H$ auch $a,b^{-1} \in H \Longrightarrow a(b^{-1})^{-1} = ab \in H$.

Damit ist festgestellt, daß die Einschränkung der Gruppenoperation von G auf H eine Operation in H ist. Da das assoziative Gesetz in ganz G gilt, gilt es auch für die Elemente aus H . Da ferner, wie schon festgestellt, $e \in H$ und für $a \in H$ auch $a^{-1} \in H$, ist H eine Gruppe .

(2) $\Longrightarrow$: klar.

(2) $\Longleftarrow$: Nach Voraussetzung existiert für jedes $a \in H$ die Abbildung $H \ni h \longmapsto ah \in H$,

die nach 2.2. injektiv ist. Eine injektive Abbildung einer endlichen Menge ist aber surjektiv, denn wegen der Injektivität muß es ebenso viele verschiedene Bilder wie Urbilder geben.Da mit $a \in H$ nach Voraussetzung auch $aa = a^2 \in H$, ist auch

$$H \ni h \longmapsto a^2 h \in H$$

surjektiv. Daher gibt es ein $h_0 \in H$ mit $a^2 h_0 = a$, folglich gilt

$$a^{-2}(a^2 h_0) = h_0 = a^{-2}a = a^{-1} \in H .$$

Aus $a,b \in H \Longrightarrow a,b^{-1} \in H \Longrightarrow ab^{-1} \in H$, also ist die Bedingung in (1) erfüllt und nach (1) folgt die Behauptung.

2.5. D e f i n i t i o n:

Seien $H \subsetneq G$ und $a \in G$, dann heißt

$$aH := \{ah \mid h \in H\}$$

bzw.

$$Ha := \{ha \mid h \in H\}$$

die durch a erzeugte Rechts- bzw. Linksrestklasse von G modulo H oder auch von G nach H .

Wir beschränken uns im folgenden auf die Betrachtung von Rechtsrestklassen, da die entsprechenden Überlegungen für Linksrestklassen völlig analog verlaufen.

2.6. H i l f s s a t z:
Seien $H \subsetneq G$ und $a,b \in G$, dann gilt:
(1) $aH = bH \iff b \in aH \iff a^{-1}b \in H$
(2) $\{aH \mid a \in G\}$ ist eine Partition von G
(Definition einer Partition siehe II 3.5.)

B e w e i s:
(1): $aH = bH \Longrightarrow be = b \in aH$ (da $e \in H$).
Umgekehrt besagt $b \in aH$, daß ein $h_0 \in H$ mit $b = ah_0$ existiert $\Longrightarrow bH = (ah_0)H = a(h_0 H) = aH$, also gilt $aH = bH \iff b \in aH$. Aus $b \in aH \Longrightarrow b = ah_0$, $h_0 \in H$ $\Longrightarrow a^{-1}b = h_0 \in H$. Aus $a^{-1}b \in H \Longrightarrow a^{-1}b = h_0 \in H$ $\Longrightarrow b = ah_0 \Longrightarrow b \in aH$. Damit ist (1) gezeigt.
(2): Wegen $a \in aH \Longrightarrow aH \neq \emptyset \quad \wedge \bigcup_{a \in G} aH = G$.
Sei $b \in aH \cap cH$ mit $a,b,c \in G \Longrightarrow$ nach (1)
$aH = bH = cH$,
also sind verschiedene Restklassen disjunkt. Insgesamt ist gezeigt, daß $\{aH \mid a \in G\}$ eine Partition ist.

Wir bemerken noch, daß der erste Teil von (1) besagt, daß genau die Repräsentanten einer Restklasse die Restklasse erzeugen.

Der Beweis dieses Hilfssatzes kann auch so geführt werden, daß man durch $a \sim b :\iff a^{-1}b \in H$ eine Äquivalenzrelation in G definiert, für die die durch a erzeugte Restklasse gleich aH ist. Die Behauptung folgt dann aus II 3.4. .

Man beachte bei allen Überlegungen, wie sich die Schreibweise ändert, wenn die Gruppenoperation als Addition geschrieben wird.

2.7. B e i s p i e l e:

1) Sei jetzt $G = \mathbb{Z}$ mit der Addition als Gruppenoperation.
Für $n \in \mathbb{N}$ sei $n\mathbb{Z} := \{nz \mid z \in \mathbb{Z}\}$, dann gilt $n\mathbb{Z} \subsetneq \mathbb{Z}$.
Es gibt jetzt genau die Restklassen
$0+n\mathbb{Z}, 1+n\mathbb{Z}, \ldots, n-1+n\mathbb{Z}$,
denn jede ganze Zahl z besitzt bei Teilung durch n mit Rest genau eine der Zahlen $0,1,\ldots,n-1$ als Rest:
Sei etwa
$$z = nq+r \quad \text{mit} \quad 0 \leq r < n,$$
dann gilt offenbar
$$z \in r+n\mathbb{Z}.$$

2) Sei jetzt $G = \mathbb{R}$ mit der Addition als Gruppenoperation und $\mathbb{Z}$ als Untergruppe. Überlege, daß man dann genau alle Restklassen $\varrho+\mathbb{Z}$, $\varrho \in \mathbb{R}$ in der Form
$$\varrho+\mathbb{Z} \quad \text{mit} \quad 0 \leq \varrho < 1$$
erhält.

2.8. D e f i n i t i o n:
Die Ordnung einer Gruppe G, in Zeichen $\mathrm{Ord}(G)$, sei die Elementezahl von G, falls G nur endlich viele Elemente enthält, und sonst das Symbol ∞.

2.9. S a t z:
Sei G eine Gruppe mit $\mathrm{Ord}(G) = n$ $(\in \mathbb{N})$ und sei $H \subsetneq G$.
Dann ist $\mathrm{Ord}(H)$ ein Teiler von $\mathrm{Ord}(G)$.

B e w e i s: Da $\{aH \mid a \in G\}$ eine Partition ist, kann man alle Elemente aus G dadurch zählen, daß man die Summen der Elemente in den verschiedenen aH bildet. Da , wie früher festgestellt,

$$G \ni x \longmapsto ax \in G$$

eine Injektion ist, enthält aH genau so viele Elemente wie H . Ist die Zahl der verschiedenen Restklassen aH gleich m, dann folgt $\mathrm{Ord}(G) = m\ \mathrm{Ord}(H)$.

Die Anzahl m der verschiedenen Restklassen von G nach H nennt man auch den Index von G nach H .

Aus diesem Resultat erhält man z.B. die

2.10. F o l g e r u n g:

Ist G eine Gruppe mit $\mathrm{Ord}(G) = p$ =Primzahl, dann besitzt G nur die "trivialen Untergruppen " $\{e\}$ und G .

B e w e i s: Teiler von p sind nur 1 und p .

N o r m a l t e i l e r u n d F a k t o r g r u p p e n

Eine Untergruppe H von G mit der Eigenschaft

$$\bigwedge a \in G\ [a^{-1}Ha = H]$$

hatten wir in 2.3. Normalteiler von G genannt. Wir stellen zunächst fest:

$$a^{-1}Ha = H \iff Ha = aH\ .$$

Zum Beweis multipliziere man $a^{-1}Ha = H$ von links mit a bzw. $Ha = aH$ von links mit a^{-1} .

Bei einem Normalteiler stimmen also die Rechtsrestklassen von G nach H mit den Linksrestklassen überein. Aufgrund dieser Voraussetzung ist es nun möglich, die Menge

$$\{aH \mid a \in G\} = \{Ha \mid a \in G\}$$

selbst wieder zu einer Gruppe, der sogenannten Faktorgruppe von G nach H, in Zeichen G/H, zu machen. Sei zunächst

$$G/H := \{aH \mid a \in G\} .$$

2.11. B e h a u p t u n g:

$\bar{\gamma} : G/H \times G/H \ni (aH, bH) \longmapsto abH \in G/H$

ist eine Gruppenoperation.

B e w e i s: Der wesentliche Punkt beim Beweis, bei dem die Normalteilereigenschaft von H eingeht, ist der zu zeigen, daß $\bar{\gamma}$ eine Abbildung ist. Zunächst wäre es ja möglich, daß, wenn man aH und bH durch andere Repräsentanten erzeugt, etwa $aH = a'H$, $bH = b'H$, man ein von abH verschiedenes Element $a'b'H$ erhalten würde. Aus $aH = a'H$, $bH = b'H$ folgt $a' = ah_1$, $b' = bh_2$ $(h_1, h_2 \in H)$, also gilt

$$a'b'H = ah_1 bh_2 H$$

Wegen $Hb = bH$ gibt es ein $h_1' \in H$ mit $h_1 b = bh_1'$; damit folgt $ah_1 bh_2 H = abh_1' h_2 H = abH$, was zu zeigen war. Um die weiteren Gruppeneigenschaften zu prüfen, setzen wir

$$aHbH := \bar{\gamma}(aH, bH) = abH .$$

Assoziatives Gesetz:

$(aHbH)cH = abHcH = (ab)cH = a(bc)H = aHbcH = aH(bHcH)$.

Neutrales Element:

Dies ist eH, denn $eHaH = eaH = aH = aeH = aHeH$.

Inverses Element:

Das inverse Element von aH ist $a^{-1}H$:

$aHa^{-1}H = aa^{-1}H = eH = a^{-1}aH = a^{-1}H\,aH$.

Damit ist 2.11. bewiesen.

2.12. D e f i n i t i o n:

Die durch 2.11. definierte Gruppe G/H mit der Gruppenoperation

$$aHbH := abH$$

heißt die Restklassen oder Faktorgruppe von G modulo H oder von G nach H.

G r u p p e n h o m o m o r p h i s m e n

Zu jeder algebraischen (oder sonstigen) Struktur gehören die strukturerhaltenden Abbildungen. Diese sind in zweifacher Hinsicht von großer Bedeutung. Einerseits treten sie als Hilfsmittel auf, um Ergebnisse von einer Struktur in andere Strukturen der gleichen Art zu übertragen. Andererseits bilden gewisse Mengen von strukturerhaltenden Abbildungen selbst wieder eine Struktur, die dann zum Gegenstand der Untersuchung gemacht werden kann.

2.13. D e f i n i t i o n:

Seien G eine Gruppe mit multiplikativ geschriebener Gruppenoperation und G' eine Gruppe mit der Gruppenoperation $\circ$.

a) Eine Abbildung

$$\varphi : G \longrightarrow G'$$

heißt ein Gruppenhomomorphismus (oder kurz Homomorphismus) von G nach G':

$$\wedge\, a,b \in G \quad [\varphi(ab) = \varphi(a) \circ \varphi(b)] \quad .$$

b) Sei $\varphi : G \longrightarrow G'$ ein Gruppenhomomorphismus und sei e' das neutrale Element von G', dann heißt

$$\underline{Ke(\varphi) := \{a \mid a \in G \wedge \varphi(a) = e'\}}$$

der Kern von φ.

2.14. F o l g e r u n g:

Sei $\varphi : G \longrightarrow G'$ ein Gruppenhomomorphismus.

1) Sei e das neutrale Element der Gruppe G, dann gilt $e \in Ke(\varphi)$.

2) $Ke(\varphi)$ ist ein Normalteiler von G.

B e w e i s:

1) $\varphi(e) = \varphi(ee) = \varphi(e) \circ \varphi(e) \Longrightarrow \varphi(e)$ ist das neutrale Element e' von G' (nach 2.1.)

2) Seien $a \in G$, $k \in Ke(\varphi) \Longrightarrow$

$$\varphi(a^{-1}ka) = \varphi(a^{-1}) \circ \varphi(k) \circ \varphi(a) = \varphi(a^{-1}) \circ e' \circ \varphi(a)$$
$$= \varphi(a^{-1}) \circ \varphi(a) = \varphi(a^{-1}a) = \varphi(e) \in Ke(\varphi)$$

nach 1) $\Longrightarrow a^{-1}Ke(\varphi)a \subset Ke(\varphi)$. Da dies für jedes $a \in G$ gilt, also auch für a^{-1} anstelle von a, folgt $Ke(\varphi) = a^{-1}(aKe(\varphi)a^{-1})a \subset a^{-1}Ke(\varphi)a$.

Folglich gilt $a^{-1}Ke(\varphi)a = Ke(\varphi)$, was zu zeigen war.

2.15. H o m o m o r p h i e s a t z:

Sei $\varphi : G \longrightarrow G'$

ein Gruppenhomomorphismus. Dann sind

$$\nu : G \ni a \longmapsto aKe(\varphi) \in G/Ke(\varphi)$$

ein surjektiver und

$$\bar{\varphi} : G/Ke(\varphi) \ni aKe(\varphi) \longrightarrow \varphi(a) \in G'$$

ein injektiver Gruppenhomomorphismus und es gilt

$$\varphi = \bar{\varphi}\,\nu \quad .$$

B e w e i s: Zur Abkürzung schreiben wir im Beweis $H := Ke(\varphi)$. Nach 2.14. wissen wir, daß dies ein Normalteiler ist, so daß die Faktorgruppe $G/Ke(\varphi)$ existiert. Zunächst ist klar, daß ν eine surjektive Abbildung ist. Wegen

$$\nu(ab) = abH = aHbH = \nu(a)\,\nu(b)$$

ist ν auch Homomorphismus. Für $\bar{\varphi}$ muß zunächst festgestellt

werden, daß es eine Abbildung ist, denn die Definition von $\bar{\varphi}(aH) = \varphi(a)$ hängt von der Wahl des Repräsentanten a von , aH ab. Sei $aH = bH$, also $b = ah$, $h \in H$, dann folgt

$$\varphi(b) = \varphi(ah_0) = \varphi(a)\circ\varphi(h_0) = \varphi(a)e' = \varphi(a) ,$$

so daß aus $aH = bH$ folgt

$$\bar{\varphi}(aH) = \varphi(a) = \varphi(b) = \bar{\varphi}(bH) .$$

Somit ist $\bar{\varphi}(aH)$ unabhängig von der Wahl von a durch aH eindeutig bestimmt, d.h. $\bar{\varphi}$ ist eine Abbildung. Dafür gilt

$$\bar{\varphi}(aHbH) = \bar{\varphi}(abH) = \varphi(ab)$$
$$= \varphi(a)\,\varphi(b) = \bar{\varphi}(aH)\,\bar{\varphi}(bH) ,$$

also ist $\bar{\varphi}$ ein Homomorphismus .

Sei jetzt

$$\bar{\varphi}(aH) = \varphi(a) = \varphi(b) = \bar{\varphi}(bH) ,$$

dann folgt

$$e' = \varphi(a)^{-1}\,\varphi(b) = \varphi(a^{-1})\,\varphi(b) = \varphi(a^{-1}b)$$

also $a^{-1}b = k \in H = Ke(\varphi)$, woraus $aH = bH$ folgt. Also ist $\bar{\varphi}$ injektiv.

Schließlich gilt

$$(\bar{\varphi}\,\nu)(a) = \bar{\varphi}(\nu(a)) = \bar{\varphi}(aH) = \varphi(a) ,$$

woraus $\varphi = \bar{\varphi}\,\nu$ folgt. Damit ist der Homomorphiesatz bewiesen.

Die Bedeutung dieses Satzes, der in ähnlicher Form in vielen algebraischen Strukturen auftritt, liegt darin, daß danach jeder Homomorphismus ein Produkt eines injektiven und eines surjektiven Homomorphismus ist, wobei der surjektive Homomorphismus ν nur von $Ke(\varphi)$ abhängt und für alle Normalteiler H von G in der gleichen Weise durch

$$G \ni a \longmapsto aH \in G/H$$

definiert wird. Ferner gilt offensichtlich, daß, wenn φ selbst surjektiv bzw. injekitv ist, $\bar{\varphi}$ bzw. ν sogar bijektiv sein muß.

§ 3 Ringe und Körper

Allgemeine Eigenschaften

Die bisher betrachteten algebraischen Strukturen wie Halbgruppen, Monoide und Gruppen sind durch eine (binäre) Operation, die gewisse Bedingungen erfüllen muß, definiert. In den Ringen und Körpern lernen wir algebraische Strukturen kennen, die durch zwei Operationen - eine Addition und eine Multiplikation - definiert werden.

3.1. Definition:
Ein Ring ist ein Tripel $(R,+,\cdot)$ mit folgenden Eigenschaften:

(1) $(R,+)$ ist eine kommutative Gruppe

(2) $(R,\cdot)$ ist eine Halbgruppe

(3) Es gelten die distributiven Gesetze:
$\bigwedge a,b,c \in R \; [(a+b)c = ac+bc \;\wedge\; a(b+c) = ab+ac]$

(4) $(R,+,\cdot)$ heißt ein Ring mit 1-Element, falls $(R,\cdot)$ ein Monoid ist.

(5) $(R,+,\cdot)$ heißt ein kommutativer Ring, falls $(R,\cdot)$ kommutativ ist.

Wir geben jetzt eine Reihe von Bezeichnungen, Bemerkungen und Folgerungen an, die wir später meist ohne besonderen Hinweis benutzen werden.
Die Operation $+$ wird Addition genannt, $a+b$ heißt Summe von a und b und wird auch als "a plus b" gelesen. Das neutrale Element bei der Addition, das, wie früher festgestellt, eindeutig bestimmt ist, wird Nullelement oder kurz Null genannt und mit 0 bezeichnet. Die Operation $\cdot$ wird Multiplikation genannt, $a\cdot b$ oder ab heißt Produkt von a und b und wird auch als "a mal b" gelesen. Hat $(R,\cdot)$ ein neutrales Element,

das ebenfalls eindeutig bestimmt ist, so wird dieses Einselement oder kurz Eins genannt und mit 1 bezeichnet. Bei diesen Bezeichnungen beachte man aber, daß im allgemeinen 0 und 1 keine Zahlen sind(es sei denn, R ist ein Zahlring) .

Wir geben jetzt eine Reihe von einfachen Folgerungen aus der Definition an.

3.2. B e h a u p t u n g:
$\bigwedge r \in R \; [r0 = 0r = 0]$

B e w e i s: Aus $0 = 0+0$ folgt
$r0 = r(0+0) = r0+r0 \implies$
$0 = r0-r0 = r0+(r0-r0) = r0+0 = r0.$
Analog für die andere Seite.

Sei jetzt 0 ein Symbol und setzt man $0+0 := 0$, $00 := 0$, dann wird dadurch ein Ring mit genau einem Element, nämlich 0 ,definiert. Ist andererseits R ein Ring mit genau einem Element, so muß dieses das Nullelement 0 der Addition sein, da dieses nach Voraussetzung ($(R,+)$ ist Gruppe) existieren muß. Es gilt dann ebenfalls $0+0 = 0$, $00 = 0$. Es gibt also (bei unserer Bezeichnung) genau einen Ring mit genau einem Element, dieser wird als Nullring bezeichnet. Beachte:Der Nullring ist ein Ring mit Einselement ($= 0$).

3.3. B e h a u p t u n g:
In einem Ring R mit Einselement, der mindestens zwei Elemente besitzt, gilt $1 \neq 0$.

B e w e i s: Sei $r \in R$, $r \neq 0$. Angenommen $1 = 0$, dann folgt nach 3.2. : $r = r1 = r0 = 0$
Widerspruch!

3.4. B e h a u p t u n g:

$\bigwedge r,s \in R\ [r(-s) = (-r)s = -(rs)]$

B e w e i s: $rs+r(-s) = r(s+(-s)) = r0 = 0$.

Wegen der Eindeutigkeit des inversen Elementes in einer Gruppe folgt: $r(-s) = -(rs)$. Analog für $(-r)s$.

H o m o m o r p h i s m e n u n d I d e a l e

Abbildungen von Ringen, die die Struktur des Ringes "erhalten", heißen Homomorphismen. Genauer gilt:

3.5. D e f i n i t i o n:

1) Seien R und S Ringe. Eine Abbildung

$$\varphi : R \longrightarrow S$$

heißt (Ring-)Homomorphismus von R nach S : $\Longleftrightarrow$

① φ ist ein Homomorphismus der additiven Gruppe von R in die von S, d.h.

$\bigwedge r_1, r_2 \in R\ [\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2)]$,

② $\bigwedge r_1, r_2 \in R\ [\varphi(r_1 r_2) = \varphi(r_1)\,\varphi(r_2)]$.

2) Ein Ringhomomorphismus $\varphi : R \longrightarrow S$ heißt unitär : $\Longleftrightarrow$

R und S sind Ringe mit Einselement 1 bzw. $1'$ und es gilt $\varphi(1) = 1'$.

3) Sei $\varphi : R \longrightarrow S$ ein Ringhomomorphismus.

Dann heißt

$$Ke(\varphi) := \{k \mid k \in R \wedge \varphi(k) = 0 \in S\}$$

der Kern von φ .

4) Eine Teilmenge C eines Ringes R heißt Linksideal bzw. Rechtsideal bzw. zweiseitiges Ideal von R : $\Longleftrightarrow$

① C ist Untergruppe der additiven Gruppe von R .

② $\bigwedge c \in C\ \bigwedge r \in R\ [rc \in C$ bzw. $cr \in C$ bzw. $cr \in C \wedge rc \in C]$.

Die weiteren Überlegungen sollen zeigen, daß der Kern eines Ringhomomorphismus ein zweiseitiges Ideal ist und daß umgekehrt zu jedem zweiseitigen Ideal C ein Ringhomomorphismus angegeben werden kann, dessen Kern gleich C ist.

3.6. B e h a u p t u n g:
Ist $\varphi : R \longrightarrow S$ ein Ringhomomorphismus, dann gilt:
a) Ist 0 bzw. $0'$ die Null in R bzw. in S, dann folgt

$$\varphi(0) = 0'$$

b) $\bigwedge r \in R \; [\varphi(-r) = -\varphi(r)]$.

B e w e i s:
a) $\varphi(0)+\varphi(0) = \varphi(0+0) = \varphi(0) \Longrightarrow \varphi(0) = 0'$
b) $\varphi(r)+\varphi(-r) = \varphi(r-r) = \varphi(0) = 0' \Longrightarrow \varphi(-r) = -\varphi(r)$

3.7. B e h a u p t u n g:
Sei $\varphi : R \longrightarrow S$ ein Ringhomomorphismus, dann ist $Ke(\varphi)$ ein zweiseitiges Ideal von R .

B e w e i s: Wegen 3.6. gilt $0 \in Ke(\varphi)$, also $Ke(\varphi) \neq \emptyset$.
Ferner folgt aus 3.6. für beliebige $k_1, k_2 \in Ke(\varphi)$:

$$\begin{aligned}\varphi(k_1 - k_2) &= \varphi(k_1) - \varphi(k_2) \\ &= 0' - 0' = 0' \in S ,\end{aligned}$$

also $k_1 - k_2 \in Ke(\varphi)$. Nach dem Untergruppenkriterium ist folglich $Ke(\varphi)$ eine Untergruppe von $(R,+)$.
Seien jetzt $k \in Ke(\varphi)$, $r \in R$, dann gilt

$$\varphi(kr) = \varphi(k)\varphi(r) = 0'\varphi(r) = 0' \quad ,$$
$$\varphi(rk) = \varphi(r)\varphi(k) = \varphi(r)0' = 0' \quad .$$

Damit ist der Beweis vollständig.

Restklassenringe

Um nun zu zeigen, daß jedes zweiseitige Ideal Kern eines Homomorphismus ist, konstruieren wir den Restklassen- oder Faktorring nach einem zweiseitigen Ideal. Sei also C zweiseitiges Ideal des Ringes R, dann existiert zunächst die additive Faktorgruppe R/C (im Sinne von 2.12), bei der die Addition durch

$$(r_1+C)+(r_2+C) := (r_1+r_2)+C$$

definiert ist.

Behauptung:

Definiert man in R/C eine Multiplikation durch

$$(r_1+C)(r_2+C) := r_1 r_2 + C \quad ,$$

dann wird R/C zu einem Ring.

Stellen wir dazu zuerst fest, daß

$$R/C \times R/C \ni (r_1+C, r_2+C) \longrightarrow r_1 r_2 + C \in R/C$$

eine Abbildung ist. Sei

$$r_1+C = r_1'+C \quad , \qquad r_2+C = r_2'+C \quad ,$$

also $r_1' = r_1+c_1$, $r_2' = r_2+c_2$,

dann folgt

$$\begin{aligned} r_1' r_2' + C &= (r_1+c_1)(r_2+c_2)+C \\ &= r_1 r_2 + c_1 r_2 + r_1 c_2 + c_1 c_2 + C \\ &= r_1 r_2 + C \quad , \end{aligned}$$

denn da C zweiseitiges Ideal ist, gilt

$$c_1 r_2 + r_1 c_2 + c_1 c_2 \in C \quad .$$

Also hängt $r_1 r_2 + C$ nicht von der Wahl der Repräsentanten von r_1+C und r_2+C ab, d.h. wir haben in der Tat eine Operation. Wegen

$$\begin{aligned} (r_1+C)((r_2+C)(r_3+C)) &= r_1(r_2 r_3)+C \\ &= (r_1 r_2) r_3 + C = ((r_1+C)(r_2+C))(r_3+C) \end{aligned}$$

ist diese assoziativ. Ferner gilt

$$((r_1+C)+(r_2+C))(r_3+C) = (r_1+r_2+C)(r_3+C)$$
$$= (r_1+r_2)r_3+C$$
$$= (r_1 r_3+C)+(r_2 r_3+C)$$
$$= (r_1+C)(r_3+C)+(r_2+C)(r_3+C) \quad ,$$

analog folgt das zweite distributive Gesetz. Ist R ein Ring mit Einselement 1 , dann gilt

$$(r+C)(1+C) = r1+C = r+C \quad ,$$
$$(1+C)(r+C) = 1r+C = r+C \quad ,$$

d.h. dann ist $1+C$ Einselement von R/C . Wir fassen zusammen.

3.8. S a t z:

Sei R ein Ring und C ein zweiseitiges Ideal in R . Dann wird die Menge $R/C = \{ r+C \mid r \in R \}$ durch die Definitionen

$$(r_1+C)+(r_2+C) := r_1+r_2+C \quad , \qquad (r_1, r_2 \in R)$$
$$(r_1+C)(r_2+C) := r_1 r_2+C$$

zu einem Ring.

Besitzt R ein Einselement 1 , dann ist $1+C$ Einselement des Ringes R/C .

3.9. D e f i n i t i o n:

Der in 3.8. definierte Ring R/C heißt Faktorring oder Restklassenring von R nach C oder von R modulo C.

3.10. S a t z:

Voraussetzungen wie in 3.7. .

Die Abbildung

$$\nu : R \ni r \longrightarrow r+C \in R/C$$

ist ein Ringhomomorphismus mit $Ke(\nu) = C$.

B e w e i s:

$$\nu(r_1 + r_2) = r_1 + r_2 + C = (r_1 + C) + (r_2 + C)$$
$$= \nu(r_1) + \nu(r_2) \quad ,$$
$$\nu(r_1 \, r_2) = r_1 \, r_2 + C = (r_1 + C)(r_2 + C)$$
$$= \nu(r_1) \, \nu(r_2) \quad ,$$

also ist ν ein Ringhomomorphismus.

Für $c \in C$ folgt $\nu(c) = c + C = C = 0 + C$, also $c \in Ke(\nu)$.

Sei umgekehrt $k \in Ke(\nu)$, dann folgt

$$\nu(k) = k + C = 0 + C \quad ,$$

also $k \in C$. Somit gilt $Ke(\nu) = C$.

Wir wollen jetzt einige Beispiele für Ringe und Ideale betrachten.

Ideale des Ringes $\mathbb{Z}$ der ganzen Zahlen

Die Menge der ganzen Zahlen zusammen mit der üblichen Addition und Multiplikation von ganzen Zahlen ist ein Ring, der der Ring der ganzen Zahlen genannt und mit $\mathbb{Z}$ bezeichnet wird. Wir wollen alle Ideale von $\mathbb{Z}$ bestimmen, wobei wir jetzt nicht zwischen Links-, Rechts- und zweiseitigen Idealen unterscheiden müssen, da der Ring $\mathbb{Z}$ kommutativ ist.

Ist r_0 Element eines beliebigen Ringes R , dann ist die Menge

$$r_0 R = \{ r_0 \, r \mid r \in R \}$$

ein Rechtsideal von R , wie man leicht nachprüft. Ein solches Ideal, das aus den Vielfachen eines Elementes besteht, heißt ein Hauptideal. Ein kommutativer Ring, in dem jedes Ideal Hauptideal ist, heißt Hauptidealring.

3.11. Satz :

$\mathbb{Z}$ ist ein Hauptidealring.

B e w e i s: Sei C ein Ideal aus $\mathbb{Z}$. Ist $C = \{0\}$, dann folgt $C = 0\mathbb{Z}$. Sei nun $C \neq \{0\}$, dann gibt es ein $c \in C$, $c \neq 0$. Aus $c \neq 0$ folgt $c > 0$ oder $-c > 0$. Da mit $c \in C$ auch $(-1)c = -c \in C$, folgt

$$C^+ := C \cap \mathbb{N} \neq \emptyset .$$

Da die Ordnung von $\mathbb{N}$ eine Wohlordnung ist, gibt es in C^+ ein kleinstes Element c_0. Sei jetzt $z \in \mathbb{Z}$, dann kann z durch c_0 mit Rest geteilt werden:

$$z = c_0 q + r \quad , \quad q, r \in \mathbb{Z} , \; 0 \leq r < c_0 .$$

Sei jetzt $z \in C$, dann folgt

$$z - c_0 q = r \in C .$$

Wegen $r < c_0$ folgt $r \notin C^+$ und wegen $0 \leq r$ folgt $r = 0$, d.h. $z = c_0 q$. Damit ist $C \subset c_0 \mathbb{Z}$ gezeigt. Wegen $c_0 \in C$ gilt aber auch $c_0 \mathbb{Z} \subset C$, also $C = c_0 \mathbb{Z}$, was zu zeigen war.

3.12. F o l g e r u n g:
Seien $m, n \in \mathbb{Z}$ und sei $t \in \mathbb{Z}$ größter gemeinsamer Teiler von m und n. Dann gibt es $a, b \in \mathbb{Z}$ mit

$$ma + nb = t .$$

B e w e i s: Wie leicht zu sehen, ist

$$m\mathbb{Z} + n\mathbb{Z} := \{ mz_1 + nz_2 \mid z_1, z_2 \in \mathbb{Z} \}$$

ein Ideal in $\mathbb{Z}$. Folglich existiert ein $t \in \mathbb{Z}$ mit

$$t\mathbb{Z} = m\mathbb{Z} + n\mathbb{Z} .$$

Wegen $m, n \in t\mathbb{Z}$ ist t gemeinsamer Teiler von m und n. Sei auch $d \in \mathbb{Z}$ gemeinsamer Teiler von m und n, dann gilt $m, n \in d\mathbb{Z}$ und folglich auch

$$t\mathbb{Z} = m\mathbb{Z} + n\mathbb{Z} \subset d\mathbb{Z} .$$

Daraus folgt, daß d auch Teiler von t ist, d.h. t ist größter gemeinsamer Teiler von m und n.

Konstruktion des Polynomringes

Sei R ein Ring mit Einselement und sei $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$ (mit $0 \in \mathbb{Z}$).

Mit $\mathrm{Abb}(\mathbb{N}_0, R)$ wird die Menge aller Abbildungen von $\mathbb{N}_0$ nach R bezeichnet. Sei dann

$$R[X] = \{ \varphi \mid \varphi \in \mathrm{Abb}(\mathbb{N}_0, R) \wedge \forall k \in \mathbb{N}_0 \wedge i \in \mathbb{N}_0 [i > k \Longrightarrow \varphi(i) = 0] \}$$

d.h. die Teilmenge aller Abbildungen von $\mathbb{N}_0$ nach R mit $\varphi(i) \neq 0$ nur für höchstens endlich viele $i \in \mathbb{N}_0$.

Schreibt man φ als Familie

$$(r_i) = (r_0, r_1, r_2, \ldots), \text{ mit } r_i := \varphi(i), \; i \in \mathbb{N}_0,$$

dann sind also von einer Stelle k ab alle $r_i = 0$.

In $R[X]$ wird durch

$$(a_i) + (b_i) := (a_i + b_i)$$

und

$$(a_i)(b_i) := (c_0, c_1, c_2, \ldots)$$

mit

$$c_\ell = \sum_{i=0}^{\ell} a_i b_{\ell - i}, \quad \ell \in \mathbb{N}_0$$

eine Addition und Multiplikation eingeführt. Wie leicht nachzuprüfen, wird $R[X]$ damit zu einem Ring mit dem Nullelement $(0,0,0,\ldots)$ und dem Einselement $(1,0,0,\ldots)$.

Setzt man noch für $r \in R$ und $(a_i) \in R[X]$

$$r(a_i) := (ra_i)$$

$$X := (0,1,0,0,0,\ldots)$$

$$X^0 := (1,0,0,0,\ldots.)$$

dann gilt, wie leicht zu prüfen,

$$(r_0, r_1, \ldots, r_k, 0, 0, \ldots) = \sum_{i=0}^{k} r_i X^i .$$

Die rechts stehende Summe nennt man ein Polynom in X. Man kann also jedes Element aus $R[X]$ als Polynom in X schreiben und nennt daher auch $R[X]$ den Polynomring in der Unbestimmten X mit Koeffizienten in R. Man beachte

dabei die irreführende Bezeichnung "Unbestimmte X" , da doch X durch X = (0,1,0,0,...) wohldefiniert ist.

Boolesche Ringe

Um zu zeigen, welche zunächst etwas pathologisch erscheinende Eigenschaften ein Ring haben kann, betrachten wir Boolesche Ringe. Diese stehen im Zusammenhang mit den sogenannten Boole-schen Algebren(auf die hier nicht eingegangen wird) und spielen bei gewissen Anwendungen eine Rolle.

3.13. Definition:
Ein Ring R heißt Boolescher Ring :

$$\bigwedge r \in R \left[r^2 = r \right] .$$

3.14. Folgerung:
Sei R ein Boolescher Ring, dann gilt:

$$\bigwedge r \in R \left[r+r = 0 \right]$$

und R ist kommutativ.

Beweis: Seien $r,s \in R$

$r+s = (r+s)^2 = r^2+rs+sr+s^2 = r+s+rs+sr$

$\Longrightarrow rs+sr = 0$

Für $s = r$ folgt $0 = r^2+r^2 = r+r$.

Also gilt $r = -r$ für jedes Element $r \in R$. Damit folgen aus $rs+sr = 0$ durch Addition von rs:

$sr = 0+sr = rs+rs+sr = rs+0 = rs$,

also ist R kommutativ.

Beispiele für Boolesche Ringe erhält man auf folgende Weise.

Sei M eine beliebige Menge und sei $P(M)$ die Potenzmenge von M. In $P(M)$ werden eine Addition und eine Multiplikation folgendermaßen eingeführt: Für $r,s \in P(M)$ sei

$$r+s := (r \cup s) \setminus (r \cap s)$$

$$rs := r \cap s \quad .$$

Man prüft leicht nach, daß damit $P(M)$ ein Boolscher Ring ist. Das Nullelement dieses Ringes ist die leere Menge $\emptyset$ und das Einselement die Menge M.

Körper

3.15. Definition:
Ein Körper ist ein kommutativer Ring, bei dem die von 0 verschiedenen Elemente bei der Multiplikation eine Gruppe bilden.

Offensichtlich ist diese Definition damit äquivalent, daß ein Körper ein kommutativer Ring mit einem Einselement $1 \neq 0$ ist, bei dem jedes von 0 verschiedene Element ein inverses Element bezüglich der Multiplikation besitzt.

Beispiele für Körper: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.
Dies sind Körper, deren Elemente Zahlen sind; derartige Körper nennt man daher auch Zahlkörper.
Um weitere Beispiele für Körper zu erhalten, beweisen wir den folgenden Satz, der endliche Körper liefert.

3.16. Satz:
Für $n \in \mathbb{N}_0$ ist der Restklassenring $\mathbb{Z}/n\mathbb{Z}$ genau dann ein Körper, wenn n eine Primzahl ist.

Beweis: Sei $n = p$ eine Primzahl.

Dann sind

$$0+p\mathbb{Z},\ 1+p\mathbb{Z},\ldots,p-1+p\mathbb{Z}$$

genau die Elemente von $\mathbb{Z}/p\mathbb{Z}$.

Sei $0<k<p$, $k \in \mathbb{N}$, dann sind k und p teilerfremd.

Folglich gibt es $a,b \in \mathbb{N}$ mit

$$ka+pb = 1 \quad ,$$

also $$ka = 1-pb \quad .$$

Dann folgt

$$(k+p\mathbb{Z})(a+p\mathbb{Z}) = ka+p\mathbb{Z}$$

$$= 1-pb+p\mathbb{Z} = 1 + p\mathbb{Z} \quad ,$$

also besitzt $k+p\mathbb{Z}$ in $\mathbb{Z}/p\mathbb{Z}$ das inverse Element $a+p\mathbb{Z}$.

Folglich ist $\mathbb{Z}/p\mathbb{Z}$ ein Körper.

Sei jetzt $n \in \mathbb{N}$ keine Primzahl, dann zeigen wir, daß $\mathbb{Z}/n\mathbb{Z}$ kein Körper ist.

1.Fall: $n = 0$, also $0\mathbb{Z} = \{0\}$.

Dann gilt

$$2+\{0\} \neq \{0\} \quad \text{und aus}$$

$$(2+\{0\})(a+\{0\}) = 2a+\{0\} = 1+\{0\}$$

müßte $2a = 1$ mit $a \in \mathbb{Z}$ folgen.

2.Fall: $n = 1$, also $1\mathbb{Z} = \mathbb{Z}$.

Dann besitzt der Ring $\mathbb{Z}/\mathbb{Z}$ nur ein Element, d.h. nur das Nullelement, und ist folglich kein Körper.

3.Fall: $n = ab$ mit $a,b \in \mathbb{N} \setminus \{1\}$. Dann gilt

$a+n\mathbb{Z} \neq 0+n\mathbb{Z}$, aber $(a+n\mathbb{Z})(b+n\mathbb{Z}) = n+n\mathbb{Z} = n\mathbb{Z} = 0+n\mathbb{Z}$.

Angenommen $a+n\mathbb{Z}$ hätte ein inverses Element $c+n\mathbb{Z}$, so folgt einerseits

$$((c+n\mathbb{Z})(a+n\mathbb{Z}))(b+n\mathbb{Z}) = (1+n\mathbb{Z})(b+n\mathbb{Z}) = b+n\mathbb{Z}$$

und andererseits

$$(c+n\mathbb{Z})((a+n\mathbb{Z})(b+n\mathbb{Z})) = (c+n\mathbb{Z})(0+n\mathbb{Z}) = 0+n\mathbb{Z}$$

also $b \in n\mathbb{Z}$. Wegen b/n ergibt dies $b = 0$ oder $b = n$.

Wegen $0 \neq n = ab$, $a \neq 1$, ist beides nicht möglich, also besitzt $a+n\mathbb{Z}$ kein inverses Element, d.h. $\mathbb{Z}/n\mathbb{Z}$ ist kein Körper.

§ 4 Moduln

Hier lernen wir einen neuen Typ von algebraischen Strukturen kennen. Die bisher behandelten algebraischen Strukturen bestanden aus einer Menge mit einer (z.B.bei Gruppen) oder zwei Operationen(z.B.bei Ringen). Bei den Moduln werden zwei algebraische Strukturen, eine additive Abelsche Gruppe und ein Ring, zu einer neuen Struktur verbunden.

4.1.Definition:

a) Ein R-Linksmodul ist ein geordnetes Tripel (M,R,γ) mit folgenden Eigenschaften:

(I) M ist eine additive Abelsche Gruppe.

(II) R ist ein Ring.

(III) γ ist eine Abbildung:

$$\gamma: R\times M \ni (r,m) \longmapsto rm \in M$$

mit

1)Assoziatives Gesetz:

$$\bigwedge r_1, r_2 \in R \bigwedge m \in M \left[r_1 (r_2 m) = (r_1 r_2)m\right]$$

2)Distributive Gesetze:

$$\bigwedge r_1, r_2, r \in R \bigwedge m_1, m_2, m \in M \left[(r_1 + r_2)m = r_1 m + r_2 m \right.$$
$$\left. \wedge\, r(m_1 + m_2) = rm_1 + rm_2\right]$$

(IV) (M,R,γ) heißt unitärer R-Linksmodul, wenn R ein Ring mit Einselement 1 ist und für alle $m \in M$ gilt:

$$1m = m \quad .$$

b) Ein linearer K-Linksvektorraum ist ein unitärer K-Linksmodul (V,K,γ), wobei K ein Körper ist.

c) Entsprechende Definitionen gelten für R-Rechtsmoduln und lineare K-Rechtsvektorräume.

Ist (M,R,γ) ein R-Linksmodul, dann schreibt man dafür auch kurz ${}_RM$ oder auch nur M, wenn feststeht, um welchen Ring

K es sich handelt. Ist entsprechend ${}_K V$ ein linearer K-Linksvektorraum, so bezeichnet man diesen auch kurz als K-Vektorraum oder auch nur als Vektorraum, wenn feststeht, um welchen Körper K es sich handelt.

Bei einem Modul ${}_R M$ mit einem kommutativen Ring R, insbesondere also bei einem Vektorraum, ist die Unterscheidung nach der Seite, auf der R "operiert", unwesentlich und wird daher oft unterdrückt.

Ist nämlich R ein kommutativer Ring und (M, R, γ) ein R-Linksmodul, so erhält man durch die Definition

$$\gamma' : M \times R \ni (m,r) \longrightarrow rm \in M ,$$

d.h. also durch die Festsetzung

$$\gamma'(m,r) := \gamma(r,m)$$

einen R- Rechtsmodul, für den mit der üblichen Schreibweise $rm = \gamma(r,m)$, $mr = \gamma'(m,r)$ gilt:

$$mr = rm \quad , r \in R , m \in M .$$

Die Kommutativität von R wird benutzt, um für γ' das assoziative Gesetz nachzuweisen:

$(mr_1)r_2 = r_2(r_1 m) = (r_2 r_1)m = (r_1 r_2)m = m(r_1 r_2)$.

In diesem Sinne ist es gleichgültig, ob man M als R-Links- oder R-Rechtsmodul auffaßt.

B e i s p i e l e:

1) Ist R ein Ring (mit 1-Element), dann ist ${}_R R$ bzw. R_R ein(unitärer) R-Links- bzw. R-Rechtsmodul. Dabei ist für rm bzw. mr mit $r,m \in R$ die Multipliaktion im Ring zu nehmen.
2) Ist C ein Links- bzw. Rechtsideal eines Ringes R, dann ist ${}_R C$ bzw. C_R ein R-Links- bzw. R-Rechtsmodul, wobei ebenfalls für rc bzw. cr die Multiplikation in R zu nehmen ist.

3) Ist R ein Ring, dann ist die Menge

$$R^n = \{(r_1, \ldots, r_n) \mid r_i \in R\}$$

mit der Addition

$$(r_1, \ldots, r_n) + (s_1, \ldots, s_n) := (r_1 + s_1, \ldots, r_n + s_n)$$

und der "Modulmultiplikation"

$$r(r_1, \ldots r_n) := (rr_1, \ldots, rr_n)$$

ein R-Linksmodul.

Auf die Theorie der Moduln soll hier nicht weiter eingegangen werden, da der Spezialfall der linearen Vektorräume in der Vorlesung über lineare Algebra eingehend behandelt wird.

IV. AUFBAU DES ZAHLENSYSTEMS

§1 Die natürlichen Zahlen

In diesem Abschnitt sollen die Eigenschaften der (Menge der) natürlichen Zahlen untersucht werden. Dabei werden wir uns auf die Grundbegriffe der Mengenlehre stützen, wie sie im I.Kapitel eingeführt worden sind. Zwar ist dort von der Menge der natürlichen Zahlen schon gesprochen worden, aber nur in Beispielen, um die dort eingeführten Begriffe zu veranschaulichen. Dort, wo eine der wichtigsten Eigenschaften der natürlichen Zahlen verwendet worden ist, nämlich die (vollständige) Induktion, wurden damit Aussagen bewiesen, die wir in diesem Abschnitt nicht benötigen werden. Durch die frühzeitige Verwendung der Induktion wird hier also kein Zirkelschluß ausgeführt.
Zur Konstruktion der natürlichen Zahlen kann man folgendermaßen vorgehen. Zunächst werden einige Eigenschaften der Menge der natürlichen Zahlen, wie wir sie uns intuitiv vorstellen, ausgewählt und diese dann als Axiome zugrundegelegt. Diese Axiome sollten in der Sprache der Mengenlehre formuliert werden. Da die bisherigen Grundbegriffe der Mengenlehre nicht ausreichen, um nachzuweisen, daß es eine Menge gibt, die den ausgewählten Axiomen genügt, d.h. die ein "Modell" für die Axiome ist, werden wir die Existenz einer solchen Menge als zusätzliches Axiom der Mengenlehre fordern. Die übrigen Eigenschaften der natürlichen Zahlen, insbesondere die Addition und die Ordnung, werden dann aus den Axiomen hergeleitet.
Bevor wir uns den Axiomen für die natürlichen Zahlen zuwenden, sei hier bemerkt, daß die Zahl "Null" zur Menge der natürlichen Zahlen hinzugenommen werden soll. Das ist zwar nicht un-

bedingt erforderlich, bringt aber später bei der Entwicklung der Rechenregeln für die Addition gewisse Vorteile mit sich. Im Unterschied zur Menge $\mathbb{N} = \{1,2,3,\ldots\}$ werden wir die hier zu betrachtende Menge mit $\mathbb{N}_0 = \{0,1,2,3,\ldots\}$ bezeichnen. Übrigens kann man dasselbe Axiomsystem, das wir unten zur Einführung von $\mathbb{N}_0$ verwenden werden, auch zur Definition von $\mathbb{N}$ verwenden (denn es gibt offenbar eine ordnungstreue bijektive Abbildung $\mathbb{N}_0 \longrightarrow \mathbb{N}$). Nur müßte man dann die Addition auf andere Weise definieren.

Die wichtigsten Eigenschaften der natürlichen Zahlen, die wir in etwas abgewandelter Form als Axiome verwenden werden, wurden von Peano (1858-1932) (und früher auch schon von Dedekind (1831-1916) in ähnlicher Fassung) formuliert. Es sind die sogenannten

PEANO AXIOME:

(P1) Null ist eine natürliche Zahl.

(P2) Jede natürliche Zahl besitzt einen eindeutig bestimmten Nachfolger, der wieder eine natürliche Zahl ist.

(P3) Null ist nicht Nachfolger einer natürlichen Zahl.

(P4) Natürliche Zahlen mit gleichen Nachfolgern sind gleich.

(P5) (Prinzip der vollständigen Induktion:)
Eine Eigenschaft, die der Null zukommt und mit jeder natürlichen Zahl auch ihrem Nachfolger, kommt allen natürlichen Zahlen zu.

Man wird sofort bemerken, daß in diesen Peano Axiomen außer den logischen und mengentheoretischen Begriffen auch einige undefinierte Begriffe vorkommen, wie "Null", "natürliche Zahl", "Nachfolger". Wir wollen diese Axiome daher in der

Sprache der Mengenlehre noch weiter formalisieren. Die Axiome (P1) und (P3) sagen im wesentlichen, daß die Null ein besonders ausgezeichnetes Element von $\mathbb{N}_0$ ist. (P2) sagt, daß die Bildung des Nachfolgers eine Abbildung von $\mathbb{N}_0$ in $\mathbb{N}_0$ ist. (P4) sagt, daß die Nachfolger-Abbildung eine injektive Abbildung ist.

1.1. D e f i n i t i o n:
Ein Tripel (A, a_0, μ), bestehend aus einer Menge A, einem Element $a_0 \in A$ und einer Abbildung $\mu : A \longrightarrow A$, das den folgenden Axiomen genügt:

(P'3) $\bigwedge x \in A \; [\mu(x) \neq a_0]$

(P'4) μ ist eine injektive Abbildung

(P'5) $\bigwedge E \in P(A) \; [a_0 \in E \wedge (\bigwedge x \in E \; [\mu(x) \in E]) \Longrightarrow E = A]$

heißt "Menge der natürlichen Zahlen".

In dieser Definition sind die Axiome jetzt nur noch mit den schon bekannten Mitteln der Mengenlehre ausgedrückt. Die Existenz einer Menge der natürlichen Zahlen müssen wir jedoch über die bisherigen Axiome der Mengenlehre hinaus noch fordern:

(M 6) Es existiert eine Menge der natürlichen Zahlen.

Die nach (M 6) existierende Menge der natürlichen Zahlen werden wir fortan mit $(\mathbb{N}_0, 0, \nu)$ bezeichnen.

Das Axiom (P'5) sagt aus, daß unter allen möglichen Modellen (A, a_0, μ), die die Axiome (P'3) und (P'4) erfüllen, die Menge der natürlichen Zahlen ein minimales Modell ist. Man sieht nämlich leicht ein, daß eine Teilmenge E von $\mathbb{N}_0$, die 0 und mit jedem x auch $\mu(x)$ enthält, ein Modell

$(E,0, \nu | L : E \longrightarrow E)$ bildet, das (P'3) und (P'4) erfüllt. (P'5) beinhaltet aber auch eine der wichtigsten Beweistechniken, den Beweis durch vollständige Induktion.

1.2. S a t z Ü b e r d e n B e w e i s d u r c h v o l l s t ä n d i g e I n d u k t i o n

Für jedes $n \in \mathbb{N}_0$ sei eine mathematische Aussage $A(n)$ formuliert. Dafür gelte (Induktionsanfang:) $A(0)$ ist richtig und (Induktionsannahme:) aus der Richtigkeit von $A(n)$ (Induktionsschluß:) folgt die Richtigkeit von $A(\nu(n))$. Dann ist $A(n)$ für alle $n \in \mathbb{N}_0$ richtig.

B e w e i s: Sei $E = \{x \mid x \in \mathbb{N}_0 \wedge A(x) \text{ richtig}\}$. Es gilt $0 \in E$ und $\bigwedge x \in E \; [\nu(x) \in E]$. Nach (P'5) folgt $E = \mathbb{N}_0$.

1.3. D e f i n i t i o n d e r A d d i t i o n v o n n a t ü r l i c h e n Z a h l e n:

Für jedes $m \in \mathbb{N}_0$ sei

$$0+m := m$$

und, wenn $n+m$ für $n \in \mathbb{N}_0$ schon definiert ist,

$$\nu(n)+m := \nu(n+m).$$

Wir zeigen, daß damit $n+m$ für alle $n,m \in \mathbb{N}_0$ definiert ist. Sei $m \in \mathbb{N}_0$. Auf die Aussage:

$A_m(n)$ = "$n+m$ ist definiert"

können wir den Satz über den Beweis durch vollständige Induktion anwenden, denn $A_m(0)$ ist richtig und wenn wir annehmen, daß $A_m(n)$ richtig ist, dann ist auch $A_m(\nu(n))$ richtig. Also ist $n+m$ für alle $n,m \in \mathbb{N}_0$ definiert.

Als bequeme Abkürzung definieren wir noch $1 := \nu(0)$ und $2 := \nu(1)$.

1.4. S a t z:

1) $\bigwedge n \in \mathbb{N}_0 \; [0+n = n = n+0]$

2) $\bigwedge n \in \mathbb{N}_0 \; [1+n = \nu(n)]$

3) $\bigwedge m,n \in \mathbb{N}_0 \; [m+n = n+m]$

4) $\bigwedge m,n,r \in \mathbb{N}_0 \; [(m+n)+r = m+(n+r)]$

5) $\bigwedge m,n,r \in \mathbb{N}_0 \; [r+m = r+n \Longrightarrow m = n]$

B e w e i s:

1) $0+n = n$ gilt nach Definition der Addition für alle $n \in \mathbb{N}_0$.
$n+0 = n$ beweisen wir durch (vollständige) Induktion nach n.
Die Aussage $A(n)$ ist dabei $n+0 = n$.
Induktionsanfang: $0+0 = 0$ gilt nach Definition der Addition.
Induktionsannahme: Es gelte $n+0 = n$.
Induktionsschluß:Zu zeigen ist $\nu(n)+0 = \nu(n)$. Wegen
$n+0 = n$ ist $\nu(n)+0 = \nu(n+0) = \nu(n)$.
Nach Satz 1.2. gilt daher $n+0 = n$ für alle $n \in \mathbb{N}_0$.

2) $1+n = \nu(0)+n = \nu(0+n) = \nu(n)$.

3) Wir zeigen: $\bigwedge n \in \mathbb{N}_0 \; [\bigwedge m \in \mathbb{N}_0 \; [m+n = n+m]]$ durch
Induktion nach n. Die Aussage $A(n)$ ist dabei
$\bigwedge m \in \mathbb{N}_0 \; [m+n = n+m]$.
Induktionsanfang: $\bigwedge m \in \mathbb{N}_0 \; [m+0 = 0+m]$. Das ist die Aussage 1) des Satzes und schon oben bewiesen worden.
Induktionsannahme:Es gelte $\bigwedge m \in \mathbb{N}_0 \; [m+n = n+m]$.
Induktionsschluß:Zu zeigen ist $\bigwedge m \in \mathbb{N}_0 \; [m+\nu(n) = \nu(n)+m]$.
Das zeigen wir durch Induktion nach m. Die Aussage $A(m)$
ist dabei $m+\nu(n) = \nu(n)+m$.
Induktionsanfang: $0+\nu(n) = \nu(n)+0$ ist richtig.
Induktionsannahme:Gelte $m+\nu(n) = \nu(n)+m$.
Induktionsschluß: $\nu(m)+\nu(n) = \nu(m+\nu(n)) =$
$= \nu(\nu(n)+m)$ (wegen Induktionsannahme über m) =
$= \nu(\nu(n+m)) = \nu(\nu(m+n))$ (wegen Induktionsannahme
über n) $= \nu(\nu(m)+n) = \nu(n+\nu(m))$ (wegen Induktions-

annahme über n) = $\nu(n)+\nu(m)$. Also gilt m N

m+ (n) = (n)+m . Also gilt 3).

4) Wir zeigen $\wedge m \in \mathbb{N}_0 \,[\wedge n,r \in \mathbb{N}_0 \,[(m+n)+r = m+(n+r)]]$

durch Induktion nach m:

Induktionsanfang: $\wedge n,r \in \mathbb{N}_0 \,[(0+n)+r = n+r = 0+(n+r)]$

ist richtig.

Induktionsannahme: $\wedge n,r \in \mathbb{N}_0 \,[(m+n)+r = m+(n+r)]$

Induktionsschluß: $\wedge n,r \in \mathbb{N}_0 \,[(\nu(m)+n)+r = \nu(m+n)+r =$

$= \nu((m+n)+r) = \nu(m+(n+r)) = \nu(m) + (n+r)]$.

5) Wir zeigen $\wedge r \in \mathbb{N}_0 \,[\wedge m,n \in \mathbb{N}_0 \,[r+m = r+n \Longrightarrow m = n]]$

durch Induktion nach r:

Induktionsanfang: $\wedge m,n \in \mathbb{N}_0 \,[0+m = 0+n \Longrightarrow m = n]$

ist richtig.

Induktionsannahme: $\wedge m,n \in \mathbb{N}_0 \,[r+m = r+n \Longrightarrow m = n]$.

Induktionsschluß: $\wedge m,n \in \mathbb{N}_0 \,[\nu(r)+m = \nu(r)+n \Longrightarrow$

$\nu(r+m) = \nu(r+n) \Longrightarrow r+m = r+n$ (wegen P'4) $\Longrightarrow$

$m = n]$.

Wir haben mit diesem Satz bewiesen, daß $(\mathbb{N}_0, +)$ ein kommutatives Monoid mit 0 als neutralem Element ist. Wir sagen, daß ein kommutatives Monoid $(M, \circ)$ die Kürzungseigenschaft hat, wenn gilt

$\wedge m,n,r \in M \,[r \circ m = r \circ n \Longrightarrow m = n]$.

Also ist $(\mathbb{N}_0, +)$ ein kommutatives Monoid mit Kürzungseigenschaft.

1.5.H i l f s s a t z:

$\wedge n \in \mathbb{N}_0 \,[n \neq 0 \Longleftrightarrow \vee m \in \mathbb{N}_0 \,[\nu(m) = n]]$

B e w e i s: Nach (P'3) gilt jedenfalls $\nu(m) \neq 0$. Sei zum Beweis der Umkehrung $E = \{x \mid x \in \mathbb{N}_0 \wedge (x = 0 \vee \vee m \in \mathbb{N}_0 \,[\nu(m) = x])\}$.

Dann ist $0 \in E \subset \mathbb{N}_0$. Ist $x \in E$, so ist $\nu(x) \in E$, weil $\nu(x)$ der Bedingung $\bigvee m \in \mathbb{N}_0 \; [\nu(m) = \nu(x)]$ genügt. Nach (P'5) ist $E = \mathbb{N}_0$. Ist also $n \in \mathbb{N}_0 = E$ und $n \neq 0$, so bleibt für n nur die Möglichkeit $\bigvee m \in \mathbb{N}_0 \; [\nu(m) = n]$.

1.6. D e f i n i t i o n d e r O r d n u n g d e r n a t ü r l i c h e n Z a h l e n

Wir definieren eine Relation $\leq$ auf $\mathbb{N}_0$ durch

$$\bigwedge m,n \in \mathbb{N}_0 \; [m \leq n :\Longleftrightarrow \bigvee r \in \mathbb{N}_0 \; [r+m = n]] \quad .$$

B e h a u p t u n g: Die Relation $\leq$ auf $\mathbb{N}_0$ ist eine Wohlordnung.

B e w e i s:

1.Reflexivität: $\bigwedge n \in \mathbb{N}_0 \; [0+n = n] \Longrightarrow \bigwedge n \in \mathbb{N}_0 \; [n \leq n]$.

2.Transitivität:Gelte $m \leq n$ und $n \leq s$ für $m,n,s \in \mathbb{N}_0$.

$\Longrightarrow \bigvee r,t \in \mathbb{N}_0 \; [r+m = n \wedge t+n = s] \Longrightarrow$

$(t+r)+m = t+(r+m) = t+n = s \Longrightarrow \bigvee u \in \mathbb{N}_0 \; [u+m = s] \Longrightarrow m \leq s$.

3.Antisymmetrie:Für $m,n \in \mathbb{N}_0$ gelte $m \leq n$ und $n \leq m$. $\Longrightarrow$

$\bigvee r,s \in \mathbb{N}_0 \; [r+m = n \wedge s+n = m] \Longrightarrow (r+s)+n = r+(s+n) =$

$r+m = 0+n \Longrightarrow r+s = 0$.

Ist $r \neq 0$, so existiert ein $t \in \mathbb{N}_0$ mit $\nu(t) = r$ nach Hilfssatz 1.5. Also ist $0 = r+s = \nu(t)+s = \nu(t+s)$ im Widerspruch zu Hilfssatz 1.5. Also ist $r = 0$ und damit $m = r+m = n$.

4. $\leq$ ist ein Wohlordnung: Sei $M \subseteq \mathbb{N}_0$ ohne kleinstes Element. Es ist $M = \emptyset$ zu zeigen. Sei $E := \{x \mid x \in \mathbb{N}_0 \wedge \bigwedge m \in M \; [x \leq m]\}$. Da M kein kleinstes Element besitzt, ist $E \cap M = \emptyset$, denn $y \in E \cap M \Longrightarrow \bigwedge m \in M \; [y \leq m]$, was der Annahme über M widerspricht. Es ist sicher $0 \in E$. Sei $x \in E$ und $\nu(x) \notin E$.

$\Longrightarrow \bigvee m \in M \; [x \leq m \wedge \nu(x) \nleq m] \Longrightarrow \bigvee r \in \mathbb{N}_0 \; [r+x = m]$.

Sicher ist $r \neq 0$, denn sonst wäre $x = m \in E \cap M = \emptyset$.
Damit ist $r = \nu(s)$ und $s+ \nu(x) = \nu(s+x) = \nu(s)+x = r+x = m$,
also $\nu(x) \leq m$ im Widerspruch zu $\nu(x) \notin m$. Ist also $x \in E$,
so ist auch $\nu(x) \in E$ und damit $E = \mathbb{N}_0$ und $M = \emptyset$.

Aus dem Beweis für die Antisymmetrie merken wir uns noch die Eigenschaft

$$\bigwedge m,n \in \mathbb{N}_0 \left[m+n = 0 \Longrightarrow m = 0 = n\right] .$$

1.7. S a t z (I. M o n o t o n i e g e s e t z)

$$\bigwedge m,n,r \in \mathbb{N}_0 \left[m \leq n \Longrightarrow r+m \leq r+n\right] .$$

B e w e i s: $m = n \Rightarrow t+m = n \Longrightarrow t+r+m = r+t+m = r+n \Longrightarrow$
$r+m = r+n$.

Aus dem I.Monotoniegesetz folgt sofort die Aussage

$$\bigwedge m,n,s,t \in \mathbb{N}_0 \left[m \leq n \wedge s \leq t \Longrightarrow m+s \leq n+t\right] ,$$

denn $m+s \leq m+t = t+m \leq t+n = n+t$.
Wir führen die Multiplikation der natürlichen Zahlen an dieser Stelle nicht ein, da sie sich später aus der Multiplikation der ganzen Zahlen mit ergeben wird.
Zum Abschluß beweisen wir jedoch noch einen Satz über die Eindeutigkeit der Menge der natürlichen Zahlen. Sicherlich sind die Mengen $\{0,1,2,3,\ldots\}$ und $\{0',1',2',3',\ldots\}$ verschiedene Mengen, aber beide ergeben Modelle für eine Menge der natürlichen Zahlen. Man kann also nicht erwarten, daß es nur eine "Menge der natürlichen Zahlen" gibt. Es genügt aber auch für alle mathematischen Zwecke, daß zwei Modelle für die Menge der natürlichen Zahlen "isomorph" sind bezüglich der hier betrachteten Strukturen.

1.8. S a t z:
Seien (A,a_0,μ) und (B,b_0,ν) jeweils eine Menge der natürlichen Zahlen(im Sinne von Definition 1.1.).
Dann gibt es genau eine bijektive Abbildung $f:A \longrightarrow B$, für die gilt $f(a_0) = b_0$ und $\bigwedge x \in A\,[f(\mu(x)) = \nu f(x)]$.

B e w e i s:Wir definieren eine Abbildung $f:A \longrightarrow B$ durch
(*) $f(a_0) := b_0$ und $f(\mu(x)) := \nu(f(x))$, falls $f(x)$ schon definiert ist. Da für (A,a_0,μ) das Prinzip der vollständigen Induktion gilt, ist klar, daß die Aussage "Für alle $x \in A$ ist durch (*) genau ein Element $f(x) \in B$ definiert" richtig ist. Weiter ist $f:A \longrightarrow B$ die einzige Abbildung, die $f(a_0) = b_0$ und $\bigwedge x \in A\,[f(\mu(x)) = \nu(f(x))]$ erfüllt. Zu zeigen bleibt, daß f bijektiv ist.
Wir bilden $E = \{x \mid x \in A \wedge \bigvee y \in A\,[x \neq y \wedge f(x) = f(y)]\}$ und wollen zeigen, daß E leer ist. Ist E nicht leer, so besitzt E ein kleinstes Element $u \in E \subset A$, denn A ist nach 1.6. wohlgeordnet. Ist $u = a_0$ und $y \neq a_0$, so ist $y = \mu(z)$ für ein $z \in A$ und $f(u) = f(a_0) = b_0 \neq \nu f(z) = f\mu(z) = f(y)$. Dann könnte aber u kein Element von E sein. Also ist $u \neq a_0$.
Sei $y \neq u$ mit $f(y) = f(u)$ gegeben. Da beide $y \neq a_0$ und $u \neq a_0$, existieren $s,t \in A$ mit $\mu(s) = y$, $\mu(t) = u$, $s \neq t$, $t \leq u$ und $t \neq u$. Also ist $t \notin E$ und $f(s) \neq f(t)$. Daraus folgt $f(y) = f(\mu(s)) = \nu f(s) \neq \nu f(t) = f\mu(t) = f(u)$, ein Widerspruch zu $f(y) = f(u)$.
f ist surjektiv:Nach Definition gilt $Bi(f) \subset B$, $b_0 \in Bi(f)$. Sei nun $m \in Bi(f)$, also $f(x) = m$ für ein $x \in A$. Dann ist $f(\mu(x)) = \nu f(x) = \nu(m) \in Bi(f)$. Da auch in (B,b_0,ν) das Prinzip der vollständigen Induktion gilt, ist $Bi(f) = B$ und f surjektiv.
Man kann jetzt leicht zeigen, daß auch $f(x+y) = f(x)+f(y)$ für alle $x,y \in A$ gilt und daß weiter aus $x \leq y$ folgt $f(x) \leq f(y)$.

Daher ist es gleichgültig, ob wir Addition und Ordnung in (A, a_0, μ) oder (B, b_0, ν) studieren.

§ 2 Die ganzen Zahlen

Zur Einführung der Menge $\mathbb{Z}$ der ganzen Zahlen verfahren wir anders als bei den natürlichen Zahlen. Statt $\mathbb{Z}$ axiomatisch zu beschreiben, wird $\mathbb{Z}$ mit Hilfe von $\mathbb{N}_0$ konstruiert. Die vorzunehmende Konstruktion von $\mathbb{Z}$ läßt sich allgemeiner für beliebige kommutative Monoide mit der Kürzungseigenschaft durchführen. Wir geben diese allgemeine Konstruktion an, die es erlaubt, zu einem vorgegebenen kommutativen Monoid $(M,+)$ mit Kürzungseigenschaft eine kommutative "von M erzeugte" Gruppe zu konstruieren.

Das Problem, das zur Erweiterung von $\mathbb{N}_0$ zu $\mathbb{Z}$ führt, besteht darin, daß die Subtraktion in $\mathbb{N}_0$ nicht unbeschränkt durchführbar ist. Nun könnte man daran denken, eine Erweiterung zu $\mathbb{Z}$ dadurch zu gewinnen, daß man formal alle möglichen Differenzbildungen $m-n$ mit $m,n \in \mathbb{N}_0$ betrachtet und diejenigen Differenzen, die in $\mathbb{N}_0$ nicht zu bilden sind, zur Menge $\mathbb{N}_0$ als neue Elemente hinzunimmt. Dabei muß man aber noch beachten, daß formal verschiedene Differenzen dasselbe Element in $\mathbb{Z}$ ergeben können, wie das folgende Beispiel zeigt: die beiden formalen Differenzen $3-5$ und $2-4$ lassen sich nicht in $\mathbb{N}_0$ auflösen; wir wissen aber, daß sie in $\mathbb{Z}$ dasselbe Element -2 bestimmen. Also muß man $3-5$ und $2-4$ identifizieren. Welche formalen Differenzen(später werden das einfach Paare von Elementen von $\mathbb{N}_0$ sein) man identifiezieren muß, kann man schon in der Struktur von $\mathbb{N}_0$ ausdrücken:im Beispiel gilt $3+4 = 5+2$ (wegen $3-5 = 2-4$ in $\mathbb{Z}$); allgemein wollen wir $m-n$ mit $s-t$ identifizieren, wenn $m+t = n+s$ ist. Dabei dürfen jetzt auch die Differenzen betrachtet werden, die in $\mathbb{N}_0$ aufgelöst werden können. Das führt uns zu folgender Konstruktion:

2.1. Konstruktion der von M erzeugten kommutativen Gruppe

Sei $(M,+)$ ein kommutatives Monoid mit Kürzungseigenschaft. Auf $M\times M$ definiert $(m,n)\sim(s,t) :\Longleftrightarrow m+t = n+s$ eine Äquivalenzrelation. Wegen $m+n = n+m$ gilt $(m,n)\sim(m,n)$ für alle $(m,n)\in M\times M$. Ist $(m,n)\sim(s,t)$, so ist $m+t = n+s$ und $s+n = t+m$, also $(s,t)\sim(m,n)$. Ist schließlich $(m,n)\sim(s,t)$ und $(s,t)\sim(u,v)$, so ist $m+t = n+s$ und $s+v = t+u$, also $(m+v)+t = m+t+v = n+s+v = n+t+u = (n+u)+t$. Wegen der Kürzungseigenschaft gilt dann $m+v = n+u$ und damit $(m,n)\sim(u,v)$.

Sei $G := M\times M/\sim$ die Menge der Äquivalenzklassen in $M\times M$ und $f:(M\times M)\times(M\times M)\longrightarrow G$ die Abbildung

$$f((m,n),(u,v)) := \overline{(m+u,n+v)} ,$$

wobei $\overline{(m,n)}$ die Äquivalenzklasse bezeichnet, die (m,n) enthält. Seien $((m,n),(u,v))$ und $((m',n'),(u',v'))$ in $(M\times M)\times(M\times M)$ gegeben mit $(m,n)\sim(m',n')$ und $(u,v)\sim(u',v')$.

$\Longrightarrow m+n' = n+m' \wedge u+v' = v+u'$

$\Longrightarrow m+u+n'+v' = n+v+m'+u' \Longrightarrow (m+u,n+v)\sim(m'+u',n'+v')$

$\Longrightarrow \overline{(m+u,n+v)} = \overline{(m'+u',n'+v')}$

$\Longrightarrow f((m,n),(u,v)) = f((m',n'),(u',v'))$.

Nach II.3.10. existiert dann genau eine Abbildung $+:G\times G\longrightarrow G$, für die gilt $\overline{(m,n)}+\overline{(u,v)} = \overline{(m+u,n+v)}$.

$(G,+)$ ist eine kommutative Gruppe: anhand der Definition von $+:G\times G\longrightarrow G$ rechnet man die Eigenschaften leicht nach.

Neutrales Element ist $\overline{(0,0)}$, wobei $0\in M$ das neutrale Element für M ist. Inverses Element zu $\overline{(m,n)}$ ist $\overline{(n,m)}$, denn $\overline{(m,n)}+\overline{(n,m)} = \overline{(m+n,m+n)} = \overline{(0,0)}$ wegen $(m+n,m+n)\sim(0,0)$ und $m+n+0 = m+n+0$.

Man hat eine injektive Abbildung $\iota : M\longrightarrow G$ mit $\iota(m) := \overline{(m,0)}$. Ist nämlich $\iota(m) = \iota(n)$, also $\overline{(m,0)} = \overline{(n,0)}$, so ist $(m,0)\sim(n,0)$ und damit $m+0 = n+0$, daher ist $\iota : M\longrightarrow G$ injektiv.

Faßt man $(G,+)$ als kommutatives Monoid auf, so ist $\iota : M \longrightarrow G$ ein Monoid-Homomorphismus, denn es ist $\iota(m+n) = (\overline{m+n,0}) = (\overline{m,0})+(\overline{n,0}) = \iota(m)+\iota(n)$ und $\iota(0) = (\overline{0,0})$.
Da ι injekitv ist, kann man die Elemente $m \in M$ vermöge ι mit den Elementen $(\overline{m,0}) \in G$ identifizieren, also M als Teilmenge von G auffassen. Dabei wirken die Addition von G und die Addition von M auf Elementen von M in gleicher Weise, da ι ein Monoid-Homomorphismus ist.
Die so konstruierte kommutative Gruppe G mit dem Untermonoid M heißt die von M erzeugte kommutative Gruppe.

2.2. D e f i n i t i o n d e r M e n g e d e r g a n z e n Z a h l e n:
Die vom kommutativen Monoid $(\mathbb{N}_0, +)$ mit Kürzungsregel erzeugte kommutative Gruppe $(\mathbb{Z},+)$, die $(\mathbb{N}_0,+)$ als Untermonoid enthält, heißt Gruppe der ganzen Zahlen.
$\mathbb{Z}$ heißt dabei die Menge der ganzen Zahlen.

Die von M erzeugte kommutative Gruppe G besitzt eine "universelle" Eigenschaft, durch die sie auch häufig definiert wird. Wir werden diese universelle Eigenschaft verwenden, um weitere Eigenschaften von $\mathbb{Z}$ herzuleiten.

2.3. S a t z:
Sei M ein kommutatives Monoid mit Kürzungseigenschaft und $\iota : M \longrightarrow G$ der oben konstruierte Monoid-Homomorphismus in die von M erzeugte kommutative Gruppe G. Seien H eine weitere kommutative Gruppe und $f : M \longrightarrow H$ ein Monoid-Homomorphismus (wobei H als Monoid aufgefaßt wird).
Dann gibt es genau einen Gruppenhomomorphismus

$$f' : G \longrightarrow H \qquad \text{mit} \qquad f'\iota = f \ .$$

B e w e i s: Sei $f_1 : M \times M \longrightarrow H$ gegeben durch $f_1(m,n) := f(m)-f(n)$. Dann gilt: $(m,n) \sim (m',n') \Longrightarrow m+n' = n+m' \Longrightarrow f(m)+f(n') = f(n)+f(m') \Longrightarrow f_1(m,n) = f(m)-f(n) = f(m')-f(n') = f_1(m',n')$, also induziert nach II.3.10. f_1 genau eine Abbildung $f' : G \longrightarrow H$ mit $f'(\overline{(m,n)}) = f(m)-f(n)$.

Wegen $f'(\overline{(m,n)}+\overline{(s,t)}) = f'(\overline{(m+s,n+t)}) = f(m+s)-f(n+t) = f(m)+f(s)-f(n)-f(t) = f'(\overline{(m,n)})+f'(\overline{(s,t)})$ ist f' ein Gruppen-Homomorphismus.

Für alle $m \in M$ gilt $f' \iota(m) = f'(\overline{(m,0)}) = f(m)-f(0) = f(m)$, also ist $f' \iota = f$.

Ist schließlich $f'' : G \longrightarrow H$ ein Gruppen-Homomorphismus mit $f'' \iota = f$, so ist $f''(\overline{(m,n)}) = f''(\overline{(m,0)}-\overline{(n,0)}) = f'' \iota(m)-f'' \iota(n) = f(m)-f(n) = f'(\overline{(m,n)})$, also ist $f' = f''$.

2.4.F o l g e r u n g:

Mit der Identifizierung von $\mathbb{N}_0$ mit einer Teilmenge von $\mathbb{Z}$ vermöge $\iota : \mathbb{N}_0 \longrightarrow \mathbb{Z}$ erhält man

$$\mathbb{Z} = \mathbb{N}_0 \cup \{x \mid x \in \mathbb{Z} \wedge \forall n \in \mathbb{N}_0 [n \neq 0 \wedge n = -x]\} .$$

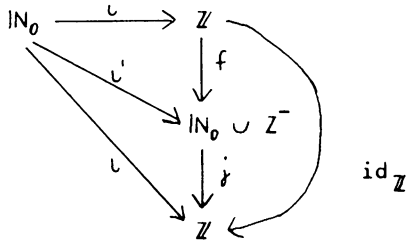
B e w e i s: Wir bezeichnen

$$\mathbb{Z}^- := \{x \mid x \in \mathbb{Z} \wedge \forall n \in \mathbb{N}_0 [n \neq 0 \wedge n = -x]\} .$$

Dann ist $\mathbb{N}_0 \cup \mathbb{Z}^-$ eine Untergruppe von $\mathbb{Z}$, denn mit $y \in \mathbb{N}_0 \cup \mathbb{Z}^-$ ist auch $-y \in \mathbb{N}_0 \cup \mathbb{Z}^-$ und mit $y,z \in \mathbb{N}_0 \cup \mathbb{Z}^-$ ist auch $y+z \in \mathbb{N}_0 \cup \mathbb{Z}^-$. Der einzige nicht-triviale Fall der letzten Behauptung ist $y \in \mathbb{N}_0$ und $z \in \mathbb{Z}^-$, also $-z = n \in \mathbb{N}_0$. Ist $y < n = -z$, so ist $y+t = n$, also $y+z = y-n = -t \in \mathbb{Z}^-$ wegen $t \neq 0$. Ist $n = -z \leq y$, so ist $n+t = y$ und $y+z = y-n = t \in \mathbb{N}_0$.

Sei $j : \mathbb{N}_0 \cup \mathbb{Z}^- \longrightarrow \mathbb{Z}$ die Inklusionsabbildung. Es ist zu zeigen, daß j surjektiv ist. Sei $\iota' : \mathbb{N}_0 \longrightarrow \mathbb{N}_0 \cup \mathbb{Z}^-$ ge-

geben mit $\iota'(n) = \iota(n)$. In dem Diagramm



sind f, j und $id_{\mathbb{Z}}$ Gruppenhomomorphismen. f existiert und ist eindeutig bestimmt durch $f\iota = \iota'$ wegen Satz 2.3. Weiter gilt $j\iota' = \iota$. Damit ist $jf\iota = \iota = id_{\mathbb{Z}}\iota$ und wegen Satz 2.3. ist $jf = id_{\mathbb{Z}}$, also ist j surjektiv. Die obige Folgerung läßt sich ebenso im Fall eines beliebigen kommutativen Monoides mit Kürzungseigenschaft beweisen. Wir haben jedoch noch eine zusätzliche Eigenschaft, nämlich $\mathbb{N}_0 \cap \mathbb{Z}^- = \emptyset$, die im allgemeinen Fall nicht gilt. Sei nämlich $x \in \mathbb{N}_0 \cap \mathbb{Z}^-$, so ist $x \in \mathbb{N}_0$ und $0 \neq -x = n \in \mathbb{N}_0$. $\Longrightarrow$ $0 = x-x = x+n \in \mathbb{N}_0 \Longrightarrow x = 0 = n$ im Widerspruch zu $n \neq 0$. Man beachte außerdem, daß $\mathbb{N}_0 \setminus \{0\} \ni n \longmapsto -n \in \mathbb{Z}^-$ eine Bijektion ist mit der Umkehrabbildung $\mathbb{Z}^- \ni x \longmapsto -x \in \mathbb{N}_0 \setminus \{0\}$.

Seien $M \subset N$ Mengen und sei auf M eine Ordnung definiert. Eine Ordnung auf N nennen wir eine Fortsetzung der Ordnung auf M , wenn ihre Einschränkung auf M die vorgegebene Ordnung auf M ist.

2.5. D i e O r d n u n g d e r g a n z e n Z a h l e n: Die folgende Relation auf $\mathbb{Z}$

$\bigwedge x,y \in \mathbb{Z}\,[x \leq y :\Longleftrightarrow y-x \in \mathbb{N}_0]$

ist eine totale Ordnung und eine Fortsetzung der Ordnung von $\mathbb{N}_0$ auf $\mathbb{Z}$.

B e w e i s:

1.Reflexivität: $x \leq x$ wegen $x-x = 0 \in \mathbb{N}_0$ für alle $x \in \mathbb{Z}$.

2.Transitivität: $x \leq y$ und $y \leq z \Longrightarrow y-x, z-y \in \mathbb{N}_0 \Longrightarrow$
$(z-y)+(y-x) = z-x \in \mathbb{N}_0 \Longrightarrow x = z$.

3.Antisymmetrie: $x \leq y$ und $y \leq x \Longrightarrow y-x, x-y \in \mathbb{N}_0 \wedge$
$(y-x)+(x-y) \in \mathbb{N}_0 \Longrightarrow y-x = 0 \Longrightarrow x = y$.

4.Totale Ordnung: $\bigwedge x,y \in \mathbb{Z} [x-y \in \mathbb{N}_0 \vee y-x \in \mathbb{N}_0] \Longrightarrow$
$\bigwedge x,y \in \mathbb{Z} [y \leq x \vee y \leq x]$.

5.Fortsetzung der Ordnung von $\mathbb{N}_0$ auf $\mathbb{Z}$:
$\bigwedge m,n \in \mathbb{N}_0 [m \leq n \text{ in } \mathbb{N}_0 \Longleftrightarrow \bigvee t \in \mathbb{N}_0 [t+m = n] \Longleftrightarrow n-m \in \mathbb{N}_0$
$\Longleftrightarrow m \leq n \text{ in } \mathbb{Z}]$.

2.6. D e f i n i t i o n d e r M u l t i p l i k a t i o n
v o n g a n z e n Z a h l e n:

Für jedes $z \in \mathbb{Z}$ definieren wir
$0 \cdot z := 0$ und $(n+1) \cdot z := n \cdot z + z$,
falls $n \cdot z$ schon definiert ist und $n \in \mathbb{N}_0$ gilt.
Für $x \in \mathbb{Z}^-$ definieren wir
$x \cdot z := -((-x) \cdot z)$.
Durch vollständige Induktion ist $n \cdot z$ für alle $n \in \mathbb{N}_0$,
$z \in \mathbb{Z}$ definiert. Oben haben wir $\mathbb{Z} = \mathbb{N}_0 \cup \mathbb{Z}^-$ gezeigt. Damit
ist $x \cdot z$ für alle $x,z \in \mathbb{Z}$ definiert.

2.7. S a t z:

$\mathbb{Z}$ mit der in 2.6. definierten Multiplikation ist ein kommutativer Ring mit Einselement.

B e w e i s:

1. $\bigwedge m \in \mathbb{N}_0$, $z \in \mathbb{Z} [m \cdot z + m = m \cdot (z+1)]$.
Beweis durch Induktion nach m: $0 \cdot z + 0 = 0 = 0 \cdot (z+1)$.
Gelte $m \cdot z + m = m \cdot (z+1)$. Dann ist $(m+1) \cdot z + (m+1) =$
$m \cdot z + z + m + 1 = m(z+1)+(z+1) = (m+1) \cdot (z+1)$.

2. $\bigwedge m,n \in \mathbb{N}_0 \left[m \cdot n = n \cdot m\right]$. Beweis durch Induktion nach n .
Induktionsanfang: $\bigwedge m \in \mathbb{N}_0 \left[m \cdot 0 = 0 = 0 \cdot m\right]$
Beweis durch Induktion nach m : $0 \cdot 0 = 0 = 0 \cdot 0$ nach Definition .
Ist $m \cdot 0 = 0 = 0 \cdot m$, so ist $(m+1) \cdot 0 = m \cdot 0 + 0 = 0 = 0 \cdot (m+1)$.
Induktionsannahme: Es gelte $\bigwedge m \in \mathbb{N}_0 \left[m \cdot n = n \cdot m\right]$
Induktionsschluß: $\bigwedge m \in \mathbb{N}_0 \left[m \cdot (n+1) = m \cdot n + m = n \cdot m + m = (n+1) \cdot m\right]$.
3. $\bigwedge m,n \in \mathbb{N}_0 \left[m \cdot (-n) = -(m \cdot n)\right]$. Beweis durch Induktion nach m.
$0 \cdot (-n) = 0 = -0 = -(0 \cdot n)$. Sei $m \cdot (-n) = -(m \cdot n)$, so ist
$(m+1) \cdot (-n) = m \cdot (-n) + (-n) = -(m \cdot n) - n = -(m \cdot n + n) = -((m+1) \cdot n)$.
4. $\bigwedge y,z \in \mathbb{Z} \left[y \cdot z = z \cdot y\right]$. Ist $y,z \in \mathbb{Z}$, so gilt $yz = zy$
wegen 2. Ist $y \in \mathbb{N}_0$, $z \in \mathbb{Z}^-$, so ist $z = -n$ für $n \in \mathbb{N}_0$
und $y \cdot z = y \cdot (-n) = -(y \cdot n) = -(n \cdot y) = (-n) \cdot y = z \cdot y$. Symmetrisch
verfährt man bei $y \in \mathbb{Z}^-$, $z \in \mathbb{N}_0$. Ist $y,z \in \mathbb{Z}^-$, also $y = -m$
und $z = -n$, so ist $y \cdot z = (-m) \cdot (-n) = -(m \cdot (-n)) = -((-n) \cdot m)$
$= -(-(n \cdot m)) = -(n \cdot (-m)) = (-n) \cdot (-m) = z \cdot y$.
5. $\bigwedge m \in \mathbb{N}_0$, $r,s \in \mathbb{Z} \left[m \cdot (r+s) = m \cdot r + m \cdot s\right]$. Beweis durch
Induktion nach m . Es ist $0 \cdot (r+s) = 0 = 0 \cdot r + 0 \cdot s$. Ist
$m(r+s) = m \cdot r + m \cdot s$, so ist $(m+1)(r+s) = m \cdot (r+s) + (r+s) =$
$= m \cdot r + m \cdot s + r + s = (m+1) \cdot r + (m+1) \cdot s$.
6. $\bigwedge m,r,s \in \mathbb{Z} \left[m(r+s) = m \cdot r + m \cdot s\right]$. Es ist nur der Fall
$m \in \mathbb{Z}^-$, $r,s \in \mathbb{Z}$ noch zu untersuchen. Sei $m = -n$ mit $n \in \mathbb{N}_0$.
Dann ist $m \cdot (r+s) = (-n) \cdot (r+s) = -(n \cdot (r+s)) = -(n \cdot r + n \cdot s) =$
$= -(n \cdot r) + (-(n \cdot s)) = (-n) \cdot r + (-n) \cdot s = m \cdot r + m \cdot s$
7. $\bigwedge m,r,s \in \mathbb{Z} \left[(r+s) \cdot m = r \cdot m + s \cdot m\right]$ gilt wegen 6. und 4.
8. $\bigwedge m \in \mathbb{N}_0$, $r,s \in \mathbb{Z} \left[(r \cdot m) \cdot s = r \cdot (m \cdot s)\right]$. Beweis durch In-
duktion nach m . Es ist $(r \cdot 0) \cdot s = 0 \cdot s = 0 = r \cdot 0 = r \cdot (0 \cdot s)$.
Ist $(r \cdot m) \cdot s = r \cdot (m \cdot s)$, so ist $(r \cdot (m+1)) \cdot s = (r \cdot m + r) \cdot s =$
$= (r \cdot m) \cdot s + r \cdot s = r \cdot (m \cdot s) + r \cdot s = r \cdot (m \cdot s + s) = r \cdot ((m+1) \cdot s)$.
9. $\bigwedge m,r,s \in \mathbb{Z} \left[(r \cdot m) \cdot s = r \cdot (m \cdot s)\right]$. Es bleibt nur der Fall
$m \in \mathbb{Z}^-$, $r,s \in \mathbb{Z}$ zu untersuchen. Sei $m = -n$ mit $n \in \mathbb{N}_0$.
Dann gilt $(r \cdot m) \cdot s = (r \cdot (-n)) \cdot s = -((r \cdot n) \cdot s) = -(r \cdot (n \cdot s)) =$
$= r \cdot ((-n) \cdot s) = r \cdot (m \cdot s)$.

§ 3 Die rationalen Zahlen

Ähnlich wie bei der Einführung der ganzen Zahlen werden wir jetzt aus $\mathbb{Z}$ die Menge $\mathbb{Q}$ der rationalen Zahlen konstruieren und ihre Eigenschaften studieren. Auch diese Konstruktion läßt sich allgemeiner für nullteilerfreie kommutative Ringe R mit Einselement durchführen. Dabei wird aus R ein Körper $\mathbb{Q}(R)$, der Quotientenkörper von R, konstruiert. Jetzt liegt das Problem in der Tatsache begründet, daß man in $\mathbb{Z}$ nicht durch jede von Null verschiedene Zahl dividieren kann. Man betrachtet daher formale Quotienten $\frac{a}{b}$ mit $a,b \in \mathbb{Z}$, $b \neq 0$ und wird $\frac{a}{b}$ und $\frac{c}{d}$ identifizieren, wenn $ad = bc$ gilt, dann ist nämlich $\frac{a}{b} = \frac{c}{d}$ (als rationale Zahlen). Man verwendet also eine ähnliche Konstruktion wie bei der Einführung der ganzen Zahlen.

3.1. Konstruktion des Quotientenkörpers von R:

Sei R ein nullteilerfreier, kommutativer Ring mit Einselement. Auf $Rx(R \setminus \{0\})$ definiert $(r,s) \sim (x,y) :\Leftrightarrow ry = sx$ eine Äquivalenzrelation. Wegen $rs = sr$ ist $(r,s) \sim (r,s)$ für alle $(r,s) \in Rx(R \setminus \{0\})$. Ist $(r,s) \sim (x,y)$, so ist $ry = sx$ und $xs = yr$, also $(x,y) \sim (r,s)$. Ist schließlich $(r,s) \sim (u,v)$ und $(u,v) \sim (x,y)$, so ist $rv = su$ und $uy = vx$, also $(ry)v = rvy = suy = svx = (sx)v$. Wegen der Nullteilerfreiheit gilt dann $ry = sx$ und damit $(r,s) \sim (x,y)$.

Sei $\mathbb{Q}(R) := Rx(R \setminus \{0\})/\sim$ die Menge der Äquivalenzklassen in $Rx(R \setminus \{o\})$ und

$f: (Rx(R \setminus \{0\}))x(Rx(R \setminus \{0\})) \longrightarrow \mathbb{Q}(R)$

10. $\bigwedge m \in \mathbb{Z}\,[1\cdot m = m = m\cdot 1]$ folgt aus $1\cdot m = (0+1)\cdot m = 0\cdot m+m = m$ und 4.

Wegen 4., 6., 7., 9. und 10. ist also $\mathbb{Z}$ ein kommutativer Ring mit Einselement.

2.8. S a t z:

Im Ring $\mathbb{Z}$ gelten folgende Rechenregeln:

a) (I. Monotoniegesetz) $\bigwedge m,n,r \in \mathbb{Z}\,[m \leq n \Longrightarrow r+m \leq r+n]$.

b) (II.Monotoniegesetz) $\bigwedge m,n,r \in \mathbb{Z}\,[m \leq n \wedge 0 \leq r \Longrightarrow r\cdot m \leq r\cdot n]$.

c) (Nullteilerfreiheit) $\bigwedge m,n \in \mathbb{Z}\,[m\cdot n = 0 \Longrightarrow m = 0 \vee n = 0]$.

B e w e i s:

a) $m \leq n \Longrightarrow n-m \in \mathbb{N}_0 \Longrightarrow r+n-(r+m) \in \mathbb{N}_0 \Longrightarrow r+m \leq r+n$.

b) $m \leq n \wedge 0 \leq r \Longrightarrow n-m, r \in \mathbb{N}_0 \Longrightarrow r\cdot(n-m) \in \mathbb{N}_0$ nach Definition der Multiplikation in $\mathbb{Z} \Longrightarrow rn-rm \in \mathbb{N}_0 \Longrightarrow rm \leq rn$.

c) Wir zeigen $m \neq 0 \wedge m\cdot n = 0 \Longrightarrow n = 0$. Es genügt, das für $m,n \in \mathbb{N}_0$ zu zeigen, da ja $(-m)\cdot n = -(m\cdot n) = m\cdot(-n)$ gilt. $m \neq 0$ und $m \in \mathbb{N}_0$ bedeutet $m = t+1$ für genau ein $t \in \mathbb{N}_0$. Also ist zu zeigen: $\bigwedge t \in \mathbb{N}_0$, $n \in \mathbb{N}_0\,[(t+1)\cdot n = 0 \Longrightarrow n = 0]$. Aber $(t+1)\cdot n = t\cdot n + n = 0$ und $t\cdot n, n \in \mathbb{N}_0$ impliziert $t\cdot n = 0$ und $n = 0$.

2.9. F o l g e r u n g:

a) $\bigwedge m,n,r \in \mathbb{Z}\,[r \neq 0 \wedge rm = rn \Longrightarrow m = n]$.

b) $\bigwedge m \in \mathbb{Z}\,[0 \leq m\cdot m = m^2]$.

c) $\bigwedge m,n,r \in \mathbb{Z}\,[0 \leq r \wedge 0 \neq r \Longrightarrow [m \leq n \Longleftrightarrow rm \leq rn]]$.

B e w e i s:

a) $r \neq 0 \wedge rm = rn \Longrightarrow r \neq 0 \wedge r(m-n) = 0 \Longrightarrow m-n = 0$
$\Longrightarrow m = n$.

b) Ist $0 \leq m \Longrightarrow 0 = 0\cdot m \leq m\cdot m = m^2$. Ist $m \leq 0$, so ist $0 = m-m \leq 0-m = -m$, also $0 \leq (-m)^2 = m^2$.

c) Sicherlich gilt $m \leq n \Longrightarrow rm \leq rn$ wegen des II. Monotoniegesetzes. Gilt $0 \leq r \wedge 0 \neq r \wedge rm \leq rn \wedge m \geq n \wedge m \neq n$, so ist $rm \geq rn \wedge rm \leq rn$, also $rm = rn$ und wegen a) ist $m = n$ im Widerspruch zu $m \neq n$. Also gilt $0 \leq r \wedge 0 \neq r \wedge rm \leq rn \Longrightarrow m \leq n$.

die Abbildung $f((r,s),(x,y)) := (\overline{rx,sy})$,
wobei $(\overline{r,s})$ die Äquivalenzklasse bezeichnet, die (r,s) enthält.
Wegen $s \neq 0 \neq y$ und der Nullteilerfreiheit von R ist $sy \neq 0$, also ist $(rx,sy) \in Rx(R \setminus \{0\})$. Damit ist f eine Abbildung.
Seien $((r,s),(x,y))$ und $((r',s'),(x',y'))$ in $(Rx(R \setminus \{0\})) \times (Rx(R \setminus \{0\}))$ gegeben mit $(r,s) \sim (r',s')$ und $(x,y) \sim (x',y')$. $\Longrightarrow$ $rs' = sr' \wedge xy' = yx' \Longrightarrow$ $rxs'y' = syr'x' \Longrightarrow (rx,sy) \sim (r'x',s'y') \Longrightarrow$ $(\overline{rx,sy}) = (\overline{r'x',s'y'}) \Longrightarrow f((r,s),(x,y)) = f((r',s')-(x',y'))$.
Nach II.3.10. existiert dann genau eine Abbildung

$$\cdot : \mathbb{Q}(R) \times \mathbb{Q}(R) \longrightarrow \mathbb{Q}(R) \quad \text{mit}$$

$(\overline{r,s})\,(\overline{x,y}) = (\overline{rx,sy})$.

Sei jetzt $g:(Rx(R \setminus \{0\})) \times (Rx(R \setminus \{0\})) \longrightarrow \mathbb{Q}(R)$ definiert durch $g((r,s),(x,y)) = (\overline{ry+sx,sy})$, so ist $sy \neq 0$ wegen $s \neq 0 \neq y$, also ist g eine Abbildung. Ist $(r,s) \sim (r',s')$ und $(x,y) \sim (x',y')$, so ist $rs' = sr'$ und $xy' = yx'$. $\Longrightarrow$
$(ry+sx)\cdot x'y' = rs'yy'+ss'xy' = r'sy'y+s'sx'y = (r'y'+s'x')\cdot sy$
$\Longrightarrow (\overline{ry+sx,sy}) = (\overline{r'y'+s'x',s'y'}) \Longrightarrow$
$g((r,s),(x,y)) = g((r',s'),(x',y'))$. Nach II.3.10. existiert dann genau eine Abbildung

$$+ : \mathbb{Q}(R) \times \mathbb{Q}(R) \longrightarrow \mathbb{Q}(R) \quad \text{mit}$$

$(\overline{r,s}) + (\overline{x,y}) = (\overline{ry+sx,sy})$.
Wenn man statt $(\overline{r,s}) \in \mathbb{Q}(R)$ die Schreibweise $\frac{r}{s} \in \mathbb{Q}(R)$ einführt, dann erfolgen Addition und Multiplikation nach den bekannten Regeln

$$\frac{r}{s} + \frac{x}{y} = \frac{ry+sx}{sy}$$

$$\frac{r}{s} \cdot \frac{x}{y} = \frac{rx}{sy} \quad .$$

Es gilt $\frac{0}{n} = \frac{0}{1}$ für alle $n \in R \setminus \{0\}$, denn $(0,n) \sim (0,1)$ wegen $0 \cdot 1 = 0 \cdot n$. Ist $\frac{m}{n} = \frac{0}{1}$, so ist $(m,n) \sim (0,1)$, also $m \cdot 1 = 0 \cdot n$. Es gilt daher

$$\frac{m}{n} = \frac{0}{1} \iff m = 0 .$$

Ebenso sieht man $\frac{1}{1} = \frac{s}{s}$ für alle $s \in R \setminus \{0\}$.

Mit den bekannten Regeln der Bruchrechnung zeigt man jetzt leicht, daß $(Q(R),+,\cdot)$ ein Körper ist mit $\frac{0}{1}$ als Nullelement, $\frac{1}{1}$ als Einselement und $\frac{s}{t}$ als inversem Element(bezüglich der Multiplikation) zu $\frac{t}{s}$. Man beachte dabei, daß $\frac{t}{s} \neq \frac{0}{1}$, falls $t \neq 0$.

Man hat eine injektive Abbildung $\iota : R \longrightarrow Q(R)$ mit $\iota(s) = \frac{s}{1}$. Ist nämlich $\iota(s) = \iota(t)$, also $\frac{s}{1} = \frac{t}{1}$, so ist $(s,1) \sim (t,1)$ und damit $s \cdot 1 = t \cdot 1$, daher ist $\iota : R \longrightarrow Q(R)$ injektiv.

Faßt man $Q(R)$ als kommutativen Ring mit Einselement auf, so ist $\iota : R \longrightarrow Q(R)$ ein unitärer Ring-Homomorphismus, denn es ist

$$\iota(s+t) = \frac{s+t}{1} = \frac{s}{1} + \frac{t}{1} = \iota(s) + \iota(t) ,$$

$$\iota(s \cdot t) = \frac{s \cdot t}{1} = \frac{s}{1} \cdot \frac{t}{1} = \iota(s) \cdot \iota(t) ,$$

$$\iota(1) = \frac{1}{1} .$$

Da ι injektiv ist, kann man die Elemente $s \in R$ vermöge ι mit den Elementen $\frac{s}{1} \in Q(R)$ identifizieren, also R als Teilmenge von $Q(R)$ auffassen. Dabei wirken die Addition bzw. Multiplikation von $Q(R)$ und die Addition bzw. Multiplikation von R auf den Elementen von R in gleicher Weise, da ι ein Ringhomomorphismus ist.

Der so konstruierte Körper $Q(R)$ mit dem Unterring R heißt Quotientenkörper von R .

3.2. D e f i n i t i o n d e r M e n g e d e r r a t i o n a l e n Z a h l e n:

Der Quotientenkörper $\mathbb{Q}$ des nullteilerfreien, kommutativen Ringes $\mathbb{Z}$ mit Einselement heißt Körper der rationalen Zahlen.

Auch der Quotientenkörper $\mathbb{Q}$ von $\mathbb{Z}$ besitzt eine "universelle" Eigenschaft, durch die er häufig definiert wird.

3.3. S a t z:

Sei R ein nullteilerfreier, kommutativer Ring mit Einselement. Sei $Q(R)$ der Quotientenkörper von R mit den oben konstruierten injektiven Ring-Homomorphismus $\iota : R \longrightarrow Q(R)$. Sei K ein weiterer Körper und $f: R \longrightarrow K$ ein injektiver Ring-Homomorphismus (wobei K als Ring aufgefaßt wird). Dann gibt es genau einen Ring-Homomorphismus (= Körper-Homomorphismus) $f': R \longrightarrow K$ mit $f'\iota = f$.

B e w e i s: Sei $f_1: Rx(R \setminus \{0\}) \longrightarrow K$ gegeben durch $f_1(r,s) = f(r)\,(f(s))^{-1}$. Dann gilt: $(r,s) \sim (x,y) \Longrightarrow ry = sx \Longrightarrow f(r)\cdot f(y) = f(s)\cdot f(x) \Longrightarrow f_1(r,s) = f(r)(f(s))^{-1} = f(x)\,(f(y))^{-1} = f_1(x,y)$. Dabei ist zu beachten, daß aus $s \neq 0 \neq y$ wegen der Injektivität von f folgt $f(s) \neq 0 \neq f(y)$, also sind $f(s)$ und $f(y)$ in K invertierbar. Nach II.3.10. induziert f_1 genau eine Abbildung $f': Q(R) \longrightarrow K$ mit $f'(\frac{r}{s}) = f(r)\cdot(f(s))^{-1}$.

f' ist ein Ring-Homomorphismus, denn es ist

$f'(\frac{r}{s} + \frac{x}{y}) = f'(\frac{ry+sx}{sy}) = (f(r)f(y)+f(s)f(x))\cdot(f(s))^{-1}\cdot(f(y))^{-1} = f(r)\cdot(f(s))^{-1} + f(x)\cdot(f(y))^{-1} = f'(\frac{r}{s}) + f'(\frac{x}{y})$ und

$f'(\frac{r}{s}\cdot\frac{x}{y}) = f'(\frac{rx}{sy}) = f(r)f(x)(f(s))^{-1}\,(f(y))^{-1} = f'(\frac{r}{s})\,f'(\frac{x}{y})$.

Für alle $r \in R$ gilt $f'\iota(r) = f'(\frac{r}{1}) = f(r)$, also ist $f'\iota = f$.

Ist schließlich $f'': Q(K) \longrightarrow K$ ein weiterer Ring-Homomorphismus mit $f'' \iota = f$, so ist $f''(\frac{r}{s}) = f''(\frac{r}{1} \cdot (\frac{s}{1})^{-1}) = f'' \iota(r)\,(f'' \iota(s))^{-1} = f(r)(f(s))^{-1} = f'(\frac{r}{s})$, also ist $f' = f''$.

Es soll die Ordnung von $\mathbb{Z}$ auf $\mathbb{Q}$ fortgesetzt werden. Ehe wir eine genaue Definition der Ordnung auf $\mathbb{Q}$ angeben, überlegen wir uns, daß für die übliche Ordnung auf $\mathbb{Q}$ gilt: $\frac{r}{s} \leq \frac{x}{y} \wedge z \in \mathbb{N}_0 \Longrightarrow z \cdot \frac{r}{s} \leq z \cdot \frac{x}{y}$. Durch geeignetes $z \in \mathbb{N}_0$ sollte man die Nenner zum Verschwinden bringen können, so daß wir schließlich auf die schon definierte Ordnung von $\mathbb{Z}$ zurückkommen. Da das Produkt der Nenner sy auch in $\mathbb{Z}^-$ liegen könnte, wählen wir $z = s^2 y^2$. Dann ist gleichzeitig $z \neq 0$, so daß wir in Analogie zu 2.9. Folgerung c) erwarten können, daß die folgende Definition den gewünschten Sachverhalt richtig wiedergibt.

3.4. Die Ordnung der rationalen Zahlen:

Die folgende Relation auf $\mathbb{Q}$

$$\bigwedge \frac{r}{s}, \frac{x}{y} \in \mathbb{Q} \left[\frac{r}{s} \leq \frac{x}{y} :\Longleftrightarrow rsy^2 \leq xys^2 \text{ in } \mathbb{Z} \right]$$

ist eine totale Ordnung und eine Fortsetzung der Ordnung von $\mathbb{Z}$ auf $\mathbb{Q}$.

Beweis:

1. Unabhängigkeit der Definition von der Wahl der Repräsentanten (r,s) bzw. (x,y) für $\frac{r}{s}$ bzw. $\frac{x}{y}$: Sei $(r,s) \sim (r',s')$ und $(x,y) \sim (x',y') \Longrightarrow rs' = r's$ und $xy' = x'y \Longrightarrow$ $\left[rsy^2 \leq xys^2 \Longleftrightarrow rsy^2 (s'y')^2 \leq xys^2 (s'y')^2 \Longleftrightarrow r's'y'^2 (sy)^2 \leq x'y's'^2 (sy)^2 \Longleftrightarrow r's'y'^2 \leq x'y's'^2 \right]$.

2. Reflexivität: $\frac{r}{s} \leq \frac{r}{s}$ wegen $rs^3 \leq rs^3$ in $\mathbb{Z}$ für alle $\frac{r}{s} \in \mathbb{Q}$.

3. Transitivität: $\frac{r}{s} \leq \frac{u}{v}$ und $\frac{u}{v} \leq \frac{x}{y} \Longrightarrow rsv^2 \leq uvs^2$ und $uvy^2 \leq xyv^2 \Longrightarrow rsv^2y^2 \leq uvs^2y^2 \leq xyv^2s^2 \Longrightarrow rsy^2 \leq xys^2$ wegen $v^2 \neq 0$, $v^2 \geq 0$ und 2.9. Folgerung c) $\Longrightarrow \frac{r}{s} \leq \frac{x}{y}$.

4. Antisymmetrie: $\frac{r}{s} \leq \frac{x}{y}$ und $\frac{x}{y} \leq \frac{r}{s} \Longrightarrow rsy^2 \leq xys^2$ und $xys^2 \leq rsy^2 \Longrightarrow rsy^2 = xys^2 \Longrightarrow \frac{r}{s} = \frac{x}{y}$, da man in $\mathbb{Q}$ durch $s^2y^2 \neq 0$ dividieren kann.

5. Totale Ordnung: $\bigwedge \frac{r}{s}, \frac{x}{y} \in \mathbb{Q} \left[rsy^2 \leq xys^2 \vee xys^2 \leq rsy^2 \text{ in } \mathbb{Z} \right] \Longrightarrow \bigwedge \frac{r}{s}, \frac{x}{y} \in \mathbb{Q} \left[\frac{r}{s} \leq \frac{x}{y} \vee \frac{x}{y} \leq \frac{r}{s} \right]$.

6. Fortsetzung der Ordnung von $\mathbb{Z}$ auf $\mathbb{Q}$:
$\bigwedge r,x \in \mathbb{Z} \left[r \leq x \text{ in } \mathbb{Z} \Longleftrightarrow r \cdot 1^3 \leq x \cdot 1^3 \text{ in } \mathbb{Z} \Longleftrightarrow \frac{r}{1} \leq \frac{x}{1} \text{ in } \mathbb{Q} \right]$.

3.5. S a t z:

Im Körper $\mathbb{Q}$ gelten folgende Rechenregeln:

a) (I.Monotoniegesetz) $\bigwedge a,b,c \in \mathbb{Q} \left[a \leq b \Longrightarrow a+c \leq b+c \right]$

b) (II.Monotoniegesetz) $\bigwedge a,b,c \in \mathbb{Q} \left[a \leq b \wedge 0 \leq c \Longrightarrow ac \leq bc \right]$.

B e w e i s:

a) Seien $a = \frac{r}{s}$, $b = \frac{u}{v}$, $c = \frac{x}{y}$. Dann gilt $\frac{r}{s} \leq \frac{u}{v} \Longrightarrow$

$rsv^2 \leq uvs^2 \Longrightarrow rsv^2y^4 + xs^2v^2y^3 \leq uvs^2y^4 + xs^2v^2y^3$

$\Longrightarrow (ry+xs)sv^2y^3 \leq (uy+xv)vs^2y^3 \Longrightarrow \frac{ry+xs}{sy} \leq \frac{uy+xv}{vy}$

$\Longrightarrow \frac{r}{s} + \frac{x}{y} \leq \frac{u}{v} + \frac{x}{y} \Longrightarrow a+c \leq b+c$.

b) Mit der Bezeichnungsweise von a) gilt $a \leq b \Longrightarrow$
$\frac{r}{s} \leq \frac{u}{v} \Longrightarrow rsv^2 \leq uvs^2$. Wegen $c = \frac{x}{y} \geq 0$ gilt $xy^3 \geq 0$.

$\Longrightarrow rsv^2xy^3 \leq uvs^2xy^3 \Longrightarrow \frac{rx}{sy} \leq \frac{ux}{vy} \Longrightarrow ac \leq bc$.

3.6. D e f i n i t i o n:

Ein Körper K, auf dem eine totale Ordnung $\leq$ so definiert ist, daß die beiden Monotoniegesetze:

I. $\bigwedge a,b,c \in K \left[a \leq b \Longrightarrow a+c \leq b+c\right]$

II. $\bigwedge a,b,c \in K \left[a \leq b \wedge 0 \leq c \Longrightarrow ac \leq bc\right]$

gelten, heißt ein angeordneter Körper.

Wegen 3.5. ist $\mathbb{Q}$ ein angeordneter Körper. Wie wir später sehen werden, bilden auch die reellen Zahlen einen angeordneten Körper. Daher wollen wir weitere Eigenschaften von $\mathbb{Q}$ gleich allgemein für angeordnete Körper behandeln. Dabei sei $a < b$ definiert durch $a \leq b$ und $a \neq b$. In einem angeordneten Körper K gelten die folgenden Rechenregeln:

a) $\bigwedge a \in K \left[0 \leq a \Longleftrightarrow -a \leq 0\right]$

b) $\bigwedge a \in K \left[0 \leq a^2\right]$

c) Für $2 := 1+1$ gilt $0 < 1 < 2$. (Man beachte hier, daß wir nicht annehmen $\mathbb{Z} \subseteq K$!)

d) $\bigwedge a \in K \left[0 < a \Longrightarrow 0 < a^{-1}\right]$

e) $\bigwedge a,b,c \in K \left[0 < c \Longrightarrow \left[a \leq b \Longleftrightarrow ac \leq bc\right]\right]$

f) $\bigwedge a,b, \in K \left[a < b \Longrightarrow a < \frac{a+b}{2} < b\right]$.

B e w e i s:

a) $0 \leq a \Longrightarrow -a+0 \leq -a+a \Longrightarrow -a \leq 0 \Longrightarrow a-a \leq a+0 \Longrightarrow 0 \leq a$.

b) Ist $0 \leq a \Longrightarrow 0 \cdot a \leq a \cdot a \Longrightarrow 0 \leq a^2$. Ist $a \leq 0 \Longrightarrow 0 \leq -a \Longrightarrow 0 \leq (-a)^2 = a^2$.

c) K Körper $\Longrightarrow 0 \neq 1 \Longrightarrow 0 \leq 1^2 = 1 \Longrightarrow 0 < 1 \Longrightarrow 1 \leq 2$. Wäre $1 = 2$, so wäre $0 = 1$, Widerspruch $\Longrightarrow 1 < 2$.

d) Sicher ist $0 \neq a^{-1}$. Wäre $a^{-1} \leq 0 \Longrightarrow a^{-1} \cdot a = 1 \leq 0 \cdot a = 0$ Widerspruch zu $0 < 1$. Also ist $0 \leq a^{-1}$.

e) $0 < c \Longrightarrow 0 < c^{-1} \Longrightarrow \left[a \leq b \Longrightarrow ac \leq bc\right]$ nach dem II. Monotoniegesetz und ebenso $ac \leq bc \Longrightarrow acc^{-1} \leq bcc^{-1} \Longrightarrow a \leq b$.

f) Zunächst folgt aus c) $0 \neq 2$, denn $0 = 2$ ergäbe $0 \leq 1 \wedge 1 \leq 0$, also $0 = 1$. Damit ist $\frac{a+b}{2} = \frac{a}{2} + \frac{b}{2}$ definiert. Nun gilt $0 < \frac{1}{2} \Longrightarrow a < b \Longleftrightarrow \frac{a}{2} < \frac{b}{2} \Longleftrightarrow \frac{a}{2} + \frac{a}{2} < \frac{a}{2} + \frac{b}{2} < \frac{b}{2} + \frac{b}{2} \Longleftrightarrow a < \frac{a+b}{2} < b$.

Gleichheit an irgendeiner Stelle würde wegen der Umkehrbarkeit der vorgenommenen Operationen an allen Stellen Gleichheit induzieren.

Für angeordnete Körper führen wir jetzt die folgenden Abbildungen ein:

den Betrag $K \ni x \longmapsto |x| \in K$ mit $|x| = \begin{cases} x & \text{für } x \geq 0 \\ -x & \text{für } x \leq 0 \end{cases}$

das Signum(=Vorzeichen) $\operatorname{sgn}: K \longrightarrow K$ mit $\operatorname{sgn}(x) = \begin{cases} 1 & \text{für } x > 0 \\ 0 & \text{für } x = 0 \\ -1 & \text{für } x < 0 \end{cases}$

Rechenregeln für diese Abbildungen sind

a) $\bigwedge x \in K \left[\operatorname{sgn}(x) \cdot |x| = x \wedge |x| = x \cdot \operatorname{sgn}(x)\right]$

b) $\bigwedge x \in K \left[0 \leq |x| \wedge \left[0 = |x| \Longleftrightarrow 0 = x\right]\right]$

c) $\bigwedge x,y \in K \left[|x+y| \leq |x|+|y|\right]$

d) $\bigwedge x,y \in K \left[|xy| = |x|\,|y|\right]$.

B e w e i s:

a) ist klar nach Definition.

b) folgt ebenfalls direkt aus der Definition.

c) Es gelten nach Definition $x \leq |x|$, $-x \leq |x|$, $y \leq |y|$, $-y \leq |y|$. $\Longrightarrow x+y \leq |x|+|y|$ und $-(x+y) \leq |x|+|y| \Longrightarrow |x+y| \leq |x|+|y|$.

d) Wegen des II.Monotoniegesetzes sieht man leicht: $\operatorname{sgn}(xy) = \operatorname{sgn}(x)\ \operatorname{sgn}(y)$ für alle $x,y \in K$. Damit erhält man für jedes $x,y \in K$

$|xy| = \mathrm{sgn}(xy)\cdot xy = \mathrm{sgn}(x)\cdot x\cdot \mathrm{sgn}(y)\cdot y = |x|\cdot|y|$.

Für den Körper $\mathbb{Q}$ der rationalen Zahlen erwähnen wir noch eine weitere wichtige Eigenschaft:

$$\bigwedge q \in \mathbb{Q},\ q > 0 \quad \bigvee n \in \mathbb{N}_0 \left[q < n \wedge \frac{1}{n} < q\right] .$$

Sei nämlich $q = \frac{r}{s}$ mit $r,s \in \mathbb{N}_0$, $s > 0$. Dann ist $s\cdot q = r \geq q$, also $r+1 > q$. Weiter ist wegen $q \neq 0$ auch $q^{-1} > 0$, also gibt es ein $m \in \mathbb{N}_0$ mit $m > q^{-1}$. Durch Multiplikation mit $q\cdot m^{-1}$ erhält man $\frac{1}{m} < q$. Für $n = \max(r,m)$ gilt dann $q < n$ und $\frac{1}{n} < q$.

§ 4 Die reellen Zahlen

Die Menge der reellen Zahlen müssen wir mit anderen Hilfsmitteln einführen, als die Menge der ganzen oder rationalen Zahlen. Bisher haben wir nur Erweiterungen des Zahlbereichs benötigt, um gewisse algebraische Operationen wie Addition und Multiplikation umkehren zu können, also um Subtraktion und später Division einzuführen. Bekanntlich läßt sich die Umkehrung einer weiteren algebraischen Operation, des Potenzierens, in der Form des sogenannten Wurzelziehens von positiven rationalen Zahlen erst in den reellen Zahlen durchführen, doch ist weder die Quadratwurzel von -1 in den reellen Zahlen enthalten, noch läßt sich die transzendente Zahl π in Form einer Wurzel darstellen. Der Aufbau der reellen Zahlen stützt sich auf eine Grenzwertbildung und ist damit von topologischer, statt von algebraischer Natur. Das Prinzip wird bei der Betrachtung der Zahl $\pi = 3{,}1415926536\ldots$ klar. Dem Leser dürfte bekannt sein, daß die letzten drei Punkte andeuten, daß es nicht möglich ist, π als Dezimalbruch mit nur endlich vielen Stellen hinter dem Komma zu schreiben, noch daß sich die verwendeten Ziffern bei der Dezimaldarstellung von irgendeiner Stelle an periodisch wiederholen. Für fast alle technischen Zwecke ist wiederum die obige zehnstellige Angabe von π zu genau. Man kann je nach dem Verwendungszweck auskommen mit

$3{,}1$; $3{,}14$; $3{,}141$; $3{,}1415$; $3{,}14159$; $3{,}141592$; ...

und weiß dann, daß die n-te Zahl in dieser Folge von rationalen(!) Zahlen um höchstens 10^{-n} von π abweicht.

Die Schreibweise von reellen Zahlen in Form von "unendlichen" Dezimalbrüchen ist also nichts anderes als eine angenäherte Angabe der reellen Zahl mit Hilfe von gewissen rationalen Zahlen, nämlich endlichen Dezimalbrüchen, bis auf eine geforderte Ge-

nauigkeit. Man könnte nun zunächst daran denken, die reellen Zahlen als Folgen von Dezimalbrüchen einzuführen, wobei man (wie oben bei der Darstellung von π) jedes folgende Folgenglied aus dem vorhergehenden durch Anfügen einer weiteren Dezimalziffer erhält. Das bringt gewisse Schwierigkeiten mit sich. Bekanntlich sind die reellen Zahlen 3,0000... und 2,9999...(mit sich jeweils wiederholenden Ziffern) gleich, obwohl sie durch verschiedene Folgen rationaler Zahlen angenähert werden. Weiter weiß man zunächst nicht, ob die Dezimalschreibweise andere reelle Zahlen ergibt, als etwa die Dualschreibweise(nur mit den Ziffern 0 und 1). Schließlich läßt sich die Addition von so dargestellten reellen Zahlen, deren Ziffern alle größer als 5 sind, schwer beschreiben, die Beschreibung der Multiplikation ist noch problematischer.
Wir betrachten daher eine wesentlich größere Klasse von Folgen rationaler Zahlen und führen darauf eine Äquivalenzrelation ein, die dann beim Übergang zu den Äquivalenzklassen auch klärt, warum 3,0000... = 2,9999... gilt. Die Konstruktion wollen wir wieder allgemeiner für einen angeordneten Körper K vornehmen. Die hier angegebene Konstruktion des Körpers der reellen Zahlen ist nicht die einzig mögliche. Einen etwas leichteren Zugang bietet die Konstruktion mit Hilfe von Dedekind'schen Schnitten. Jedoch ist die von uns angegebene Konstruktion der Menge der reellen Zahlen als Vervollständigung der Cauchy-Folgen rationaler Zahlen ein auch in vielen anderen Gebieten der Mathematik nützliches Verfahren.

4.1. D e f i n i t i o n:
Eine Folge $(x_n \mid x_n \in K \wedge n \in \mathbb{N}_0)$ in einem angeordneten Körper K heißt Cauchy-Folge oder Fundamental-Folge, wenn gilt

$$\bigwedge \varepsilon \in K, \varepsilon > 0 \ \bigvee n_0 \in \mathbb{N}_0 \ \bigwedge m,n \in \mathbb{N}_0 \left[n_0 \leq m, n_0 \leq n \implies |x_m - x_n| < \varepsilon \right]$$

Eine Folge (x_n) in K heißt Nullfolge, wenn gilt:

$$\bigwedge \varepsilon \in K, \varepsilon > 0 \bigvee n_0 \in \mathbb{N}_0 \bigwedge n \in \mathbb{N}_0 \left[n_0 \leq n \Longrightarrow |x_n| < \varepsilon \right] .$$

Eine Folge (x_n) in K hat den Grenzwert $x \in K$, wenn gilt:

$$\bigwedge \varepsilon \in K, \varepsilon > 0 \bigvee n_0 \in \mathbb{N}_0 \bigwedge n \in \mathbb{N}_0 \left[n_0 \leq n \Longrightarrow |x_n - x| < \varepsilon \right] .$$

x ist also genau dann Grenzwert der Folge (x_n), wenn $(x_n - x)$ eine Nullfolge ist.
Wenn eine Folge (x_n) in K einen Grenzwert besitzt, so heißt die Folge konvergent und der Grenzwert ist eindeutig bestimmt.
Wir schreiben dann $x = \lim\limits_{n \to \infty} x_n$ für den Grenzwert.

Daß der Grenzwert einer konvergenten Folge eindeutig bestimmt ist, sieht man wie folgt. Seien x, y Grenzwerte für (x_n). Sei $x \neq y$, dann ist $\varepsilon := \frac{1}{2} \cdot |x-y| \in K, \varepsilon > 0$. Sei $n_0 \in \mathbb{N}_0$ so gewählt, daß sowohl $|x_n - x| < \varepsilon$ für alle $n \geq n_0$ als auch $|x_n - y| < \varepsilon$ für alle $n \geq n_0$. Dann ist $|x-y| = |x-x_n+x_n-y| \leq |x-x_n| + |x_n-y| < 2\varepsilon = |x-y|$, ein Widerspruch aus der Annahme $x \neq y$. Also ist $x = y$.

B e h a u p t u n g:
Jede Nullfolge in K ist konvergent mit dem Grenzwert 0.
Jede konvergente Folge in K ist eine Cauchy-Folge.

B e w e i s: Die erste Behauptung ist klar nach Definition.
Sei (x_n) konvergent mit $x = \lim\limits_{n \to \infty} x_n$. Zu $\varepsilon > 0$ sei $n_0 \in \mathbb{N}_0$ so gewählt, daß für alle $n \geq n_0$ gilt $|x_n - x| < \frac{\varepsilon}{2}$. Für $m \geq n_0$, $n \geq n_0$ ist dann $|x_m - x_n| \leq |x_m - x| + |x - x_n| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$.

Sei $C(k)$ die Menge der Cauchy-Folgen in dem angeordneten Körper K. Für jedes $(x_n) \in C(K)$ existiert ein $z \in K$ mit $|x_n| \leq z$ für alle $n \in \mathbb{N}_0$, d.h. jede Cauchy-Folge ist beschränkt.

Wählen wir nämlich zu einem $\varepsilon > 0$ ein $n_0 \in \mathbb{N}_0$, so daß für alle $n \geq n_0$ gilt $|x_n - x_{n_0}| < \varepsilon$, so ist $|x_n| < |x_{n_0}| + \varepsilon$ für alle $n \geq n_0$, also ist $|x_n| \leq \max(|x_0|, \ldots, |x_{n_0-1}|, |x_{n_0}| + \varepsilon) = z$.

4.2. S a t z:

Sei K ein angeordneter Körper und $C(K)$ die Menge der Cauchy-Folgen in K. Dann ist $C(K)$

mit der Addition $(x_n)+(y_n) := (x_n+y_n)$

und der Multiplikation $(x_n)\cdot(y_n) := (x_n y_n)$

ein kommutativer Ring mit Einselement.

Das Einselement ist die Folge (x_n) mit $x_n = 1$ für alle $n \in \mathbb{N}_0$.

B e w e i s:

1) Mit (x_n) und (y_n) ist auch (x_n+y_n) eine Cauchy-Folge. Sei nämlich $\varepsilon > 0$, $\varepsilon \in K$. Dann gibt es ein $n_1 \in \mathbb{N}_0$, so daß für alle $m,n \geq n_1$ gilt $|x_m - x_n| < \frac{\varepsilon}{2}$. Ebenso gibt es ein $n_2 \in \mathbb{N}_0$, so daß für alle $m,n \geq n_2$ gilt $|y_m - y_n| < \frac{\varepsilon}{2}$. Für alle $m,n \geq n_0 := \max(n_1, n_2)$ ist dann $|(x_m+y_m)-(x_n+y_n)| \leq |x_m - x_n| + |y_m - y_n| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$.

2) Mit (x_n) und (y_n) ist auch $(x_n y_n)$ eine Cauchy-Folge. Sei nämlich $\varepsilon > 0$, $\varepsilon \in K$. Seien weiter $|x_n| \leq z_1$, $|y_n| \leq z_2$ für alle $n \in \mathbb{N}_0$ und $z = \max(z_1, z_2, 1)$. Dann gibt es ein $n_0 \in \mathbb{N}_0$, so daß für alle $m,n \geq n_0$ gilt $|x_m - x_n| < \frac{\varepsilon}{2z}$ und $|y_m - y_n| < \frac{\varepsilon}{2z}$. Daraus folgt $|x_m y_m - x_n y_n| = |x_m y_m - x_m y_n + x_m y_n - x_n y_n| \leq |x_m||y_m - y_n| + |x_m - x_n||y_n| < 2z \frac{\varepsilon}{2z} = \varepsilon$.

3) Die Folge (x_n) mit $x_n = 1$ für alle $n \in \mathbb{N}_0$ ist trivialerweise das Einselement der Multiplikation.

4) Die Ringeigenschaften lassen sich jetzt durch komponentenweise Rechnungen leicht nachprüfen, wie z.B. die Kommutativität der Addition: $(x_n)+(y_n) = (x_n+y_n) = (y_n+x_n) = (y_n)+(x_n)$.

4.3. S a t z:
Die Menge der Nullfolgen $N(K)$ ist ein Ideal in $C(K)$.

B e w e i s:
1) Seien (x_n) und (y_n) Nullfolgen. Dann ist auch $(x_n)+(y_n)$ ein Nullfolge. Für $\varepsilon > 0$ gibt es nämlich ein $n_0 \in \mathbb{N}_0$, so daß für alle $n \geq n_0$ gilt: $|x_n| < \frac{\varepsilon}{2}$ und $|y_n| < \frac{\varepsilon}{2}$.
Dann ist $|x_n + y_n| \leq |x_n| + |y_n| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$.
2) Sei $(x_n) \in C(K)$ und $(y_n) \in N(K)$. Dann ist $(x_n)(y_n) \in N(K)$. Sei nämlich $\varepsilon > 0$. Es gibt ein $z > 0$ mit $|x_n| < z$ für alle $n \in \mathbb{N}_0$. Weiter gibt es ein $n_0 \in \mathbb{N}_0$ mit $|y_n| < \frac{\varepsilon}{z}$ für alle $n \geq n_0$. Dann gilt $|x_n y_n| = |x_n||y_n| < z \frac{\varepsilon}{z} = \varepsilon$ für alle $n \geq n_0$.

4.4. S a t z:
$C(K)/N(K)$ ist ein Körper.

B e w e i s: Aus III.3.8. ist bekannt, daß $C(K)/N(K)$ ein kommutativer Ring mit Einselement $\overline{(e_n)} := (e_n)+N(K)$ mit $e_n = 1$ für alle $n \in \mathbb{N}_0$ ist. Die Folge (e_n) ist sicher keine Nullfolge. Zu einem beliebigen Element $\overline{(x_n)} = (x_n)+N(K) \in C(K)/N(K))$mit $\overline{(x_n)} \neq 0$ ist ein inverses Element zu finden, also zu $(x_n) \in C(K) \setminus N(K)$ ein $(y_n) \in C(K)$ so zu finden, daß $(x_n y_n - 1) \in N(K)$ ist.
Da (x_n) keine Nullfolge ist, existiert ein $\varepsilon > 0$, so daß für jedes $n \in \mathbb{N}_0$ ein $m \geq n$ existiert mit $|x_m| \geq \varepsilon$.
Da (x_n) eine Cauchy-Folge ist, existiert ein $n_0 \in \mathbb{N}_0$, so daß für alle $m,n \geq n_0$ gilt $|x_m - x_n| < \frac{\varepsilon}{2}$. Zu n_0 existiert ein n_1 mit $|x_{n_1}| \geq \varepsilon$. Also gilt für alle $m \geq n_1$: $|x_m| \geq |x_{n_1}| - |x_m - x_{n_1}|$ (wegen der Dreiecksungleichung) $> |x_{n_1}| - \frac{\varepsilon}{2} \geq \frac{\varepsilon}{2}$. Wir definieren (y_n) durch $y_n = x_n^{-1}$ für alle $n \geq n_1$ und $y_n = 1$ für $n < n_1$. Für alle $n \geq n_1$ gilt jetzt $x_n y_n = 1$, also $|x_n y_n - 1| = 0$. Damit ist $(x_n y_n - 1)$

eine Nullfolge. Zu zeigen bleibt, daß (y_n) eine Cauchy-Folge ist. Zunächst ist $|x_n| \geq \frac{\varepsilon}{2}$ für alle $n \geq n_1$. Ist nun $\varepsilon' > 0$ gegeben, so existiert ein $n_2 \geq n_1$, so daß für alle $m,n \geq n_2$ gilt $|x_n - x_m| < \varepsilon' \cdot \frac{\varepsilon^2}{4}$. Dann gilt für alle $m,n \geq n_2$: $|y_n - y_m| = \left|\frac{x_n - x_m}{x_n x_m}\right| < \varepsilon' \cdot \frac{\varepsilon^2}{4} \frac{4}{\varepsilon^2} = \varepsilon'$.
Also ist $(y_n) \in C(K)$.

Die Abbildung $\varphi : K \ni x \longmapsto (\overline{x_n}) \in C(K)/N(K)$ mit $x_n = x$ für alle $n \in \mathbb{N}_0$ ist ein Ringhomomorphismus, weil die Operationen in $C(K)$ komponentenweise definiert sind. Die Cauchy-Folgen (x_n) mit $x_n = x$ für alle $n \in \mathbb{N}_0$ nennen wir konstante Folgen. Zwei konstante Folgen (x_n) und (y_n) liegen genau dann in derselben Äquivalenzklasse in $C(K)/N(K)$, wenn die konstante Folge $(x_n - y_n)$ eine Nullfolge ist, d.h. aber, wenn $x_n = y_n$ für alle $n \in \mathbb{N}_0$ ist, denn es gibt nur die konstante Nullfolge (z_n) mit $z_n = 0$ für alle $n \in \mathbb{N}_0$. Damit ist der Homomorphismus $\varphi : K \longrightarrow C(K)/N(K)$ injektiv. Wir wollen vermöge φ die Elemente aus K mit den Äquivalenzklassen von konstanten Folgen in $C(K)/N(K)$ identifizieren. Damit ist dann $C(K)/N(K)$ eine Körpererweiterung von K.

4.5. D e f i n i t i o n:
Für $K = \mathbb{Q}$, den Körper der rationalen Zahlen, heißt die Körpererweiterung $\mathbb{R} := C(\mathbb{Q})/N(\mathbb{Q})$ Körper der reellen Zahlen.

Jeder "unendliche" Dezimalbruch kann also jetzt als Element von $\mathbb{R}$ aufgefaßt werden, wenn man ihn als Folge von rationalen Zahlen wie in der Einleitung zu diesem Paragrafen auffaßt. Jede solche Folge ist nämlich eine Cauchy-Folge in $\mathbb{Q}$ und bestimmt daher ein Element in $C(\mathbb{Q})/N(\mathbb{Q})$. Jetzt kann man auch leicht einsehen, warum die reellen Zahlen 3,0000... und 2,9999..

gleich sind. Umgekehrt kann man auch jeder reellen Zahl $(\overline{x_n})$ einen "unendlichen" Dezimalbruch zuordnen. Diese Zuordnung, die einer speziellen Konstruktion bedarf, um die rationalen Zahlen in geeigneter Weise in endliche Dezimalbrüche umzuwandeln, soll hier nicht durchgeführt werden. Andere wichtige Eigenschaften für $\mathbb{R}$ werden wir wieder für $C(K)/N(K)$ mit einem beliebigen angeordneten Körper K untersuchen.

4.6. S a t z:

$C(K)/N(K)$ ist mit der Relation

$$(\overline{x_n}) \leq (\overline{y_n}) :\Longleftrightarrow \bigwedge \varepsilon > 0, \varepsilon \in K \bigvee n_0 \in \mathbb{N}_0 \bigwedge n \in \mathbb{N}_0 : [n \geq n_0 \Longrightarrow (x_n - y_n) < \varepsilon]$$

ein angeordneter Körper. Die gegebene Ordnung setzt die Ordnung von K fort.

B e w e i s:

1) Zunächst ist zu zeigen, daß die gegebene Definition der Ordnung unabhängig von der erfolgten Auswahl der Repräsentanten von $(\overline{x_n})$ bzw. $(\overline{y_n})$ ist. Seien $(x_n),(x'_n)$ Repräsentanten für $(\overline{x_n})$ und $(y_n),(y'_n)$ für $(\overline{y_n})$. Für (x_n) und (y_n) gelte die Bedingung der Definition in 4.6. . Zu $\varepsilon > 0$, $\varepsilon \in K$ gibt es dann $n_0 \in \mathbb{N}_0$, so daß für alle $n \in \mathbb{N}_0$ mit $n \geq n_0$ gilt $x_n - y_n < \frac{\varepsilon}{3}$. Weiter gibt es ein $n_1 \in \mathbb{N}_0$, so daß für alle $n \geq n_1$ gilt $|x_n - x'_n| < \frac{\varepsilon}{3}$, und es gibt ein $n_2 \in \mathbb{N}_0$, so daß für alle $n \geq n_2$ gilt $|y_n - y'_n| < \frac{\varepsilon}{3}$. Für $n_3 = \max(n_0, n_1, n_2)$ und alle $n \geq n_3$ gilt dann $x'_n - y'_n = (x'_n - x_n) + (x_n - y_n) + (y_n - y'_n) < \frac{\varepsilon}{3} + \frac{\varepsilon}{3} + \frac{\varepsilon}{3} = \varepsilon$. Also gilt die Bedingung der Definition auch für (x'_n) und (y'_n).

2) Es ist $(\overline{x_n}) \leq (\overline{y_n})$ genau dann, wenn $(\overline{x_n}) = (\overline{y_n})$ oder wenn gilt:

$$\bigvee \delta > 0, \delta \in K \bigvee n_0 \in \mathbb{N}_0 \bigwedge n \in \mathbb{N}_0 \left[n \geq n_0 \Longrightarrow y_n - x_n > \delta\right] .$$

Da die letzte Bedingung nur erfüllt sein kann, wenn $(y_n - x_n)$ keine Nullfolge ist, also $(\overline{x_n}) \neq (\overline{y_n})$ gilt, ist sie dann auch äquivalent zu $(\overline{x_n}) < (\overline{y_n})$. Sei $(\overline{x_n}) \leq (\overline{y_n})$ und $(\overline{x_n}) \neq (\overline{y_n})$. Da $(y_n - x_n)$ keine Nullfolge ist, gibt es nach den Überlegungen im Beweis von 4.4. ein $\varepsilon > 0$, $\varepsilon \in K$ und ein $n_0 \in \mathbb{N}_0$, so daß für alle $n \geq n_0$ gilt $|y_n - x_n| > \varepsilon$. Wegen $(\overline{x_n}) \leq (\overline{y_n})$ gibt es zu ε ein $n_1 \in \mathbb{N}_0$, so daß für alle $n \geq n_1$ gilt $x_n - y_n < \varepsilon$. Für alle $n \geq \max(n_0, n_1)$ gilt also $y_n - x_n > \varepsilon$. Ist umgekehrt $(\overline{x_n}) = (\overline{y_n})$, so gilt: $\bigwedge \varepsilon > 0 \bigvee n_0 \in \mathbb{N}_0 \bigwedge n \in \mathbb{N}_0 \left[n \geq n_0 \Longrightarrow |x_n - y_n| < \varepsilon \right]$, also insbesondere $(\overline{x_n}) \leq (\overline{y_n})$. Gilt die letzte unter 2) genannte Bedingung, so gibt es insbesondere ein $n_0 \in \mathbb{N}_0$, so daß für alle $n \geq n_0$ gilt $x_n - y_n \leq 0$, also für jedes $\varepsilon > 0$ gilt dann $x_n - y_n < \varepsilon$. Auch dann folgt $(\overline{x_n}) \leq (\overline{y_n})$.

3) Für $(\overline{x_n}), (\overline{y_n})$ ist zu zeigen: es gilt eine der Relationen $(\overline{x_n}) < (\overline{y_n})$, $(\overline{x_n}) = (\overline{y_n})$, $(\overline{x_n}) > (\overline{y_n})$. Wir nehmen an, daß $(\overline{x_n}) \neq (\overline{y_n})$ gilt. Dann gibt es ein $\varepsilon > 0$ und ein $n_0 \in \mathbb{N}_0$, so daß für alle $n \geq n_0$ gilt $|x_n - y_n| > \varepsilon$. Außerdem gibt es ein $n_1 \in \mathbb{N}_0$, so daß für alle $m, n \geq n_1$ gilt $|x_m - x_n| < \varepsilon$ und $|y_m - y_n| < \varepsilon$. Wären nun $r, s \in \mathbb{N}_0$ mit $r, s \geq \max(n_0, n_1)$ gegeben, so daß $x_r - y_r > \varepsilon$ und $x_s - y_s < -\varepsilon$, so erhielte man $2\varepsilon < x_r - y_r - x_s + y_s = (x_r - x_s) + (y_s - y_r) \leq |x_r - x_s| + |y_s - y_r| < 2\varepsilon$, also einen Widerspruch. Zu $\varepsilon > 0$ und $n_2 = \max(n_0, n_1)$ gilt also für alle $n \geq n_2$ $x_n - y_n > \varepsilon$ oder für alle $n \geq n_2$ $y_n - x_n > \varepsilon$. Damit gilt eine der Relationen $(\overline{x_n}) < (\overline{y_n})$ oder $(\overline{y_n}) < (\overline{x_n})$.

4) $(\overline{x_n}) \leq (\overline{y_n})$ und $(\overline{y_n}) \leq (\overline{x_n})$ sei gegeben. Dann gibt es zu jedem $\varepsilon > 0$ ein $n_0 \in \mathbb{N}_0$, so daß für alle $n \geq n_0$ gilt $x_n - y_n < \varepsilon$ und $y_n - x_n < \varepsilon$, also $|x_n - y_n| < \varepsilon$. Damit ist $(x_n - y_n)$ eine Nullfolge und $(\overline{x_n}) = (\overline{y_n})$.

5) Gelte $(\overline{x_n}) \leq (\overline{y_n})$ und $(\overline{y_n}) \leq (\overline{z_n})$. Wenn in einem oder beiden Fällen die Gleichheit gilt, dann ist $(\overline{x_n}) \leq (\overline{z_n})$. Gilt aber $(\overline{x_n}) < (\overline{y_n})$ und $(\overline{y_n}) < (\overline{z_n})$, so existieren $\delta_1, \delta_2 > 0$ und $n_1, n_2 \in \mathbb{N}_0$, so daß für alle $n \geq n_1$ gilt $x_n - y_n > \delta_1$, und für alle $n \geq n_2$ gilt $y_n - z_n > \delta_2$. Für $\delta = \delta_1 + \delta_2$ und $n_0 = \max(n_1, n_2)$ ist dann für alle $n \geq n_0$ $x_n - z_n = x_n - y_n + y_n - z_n > \delta_1 + \delta_2 = \delta_3$.
Daher gilt $(\overline{x_n}) \leq (\overline{z_n})$

6) Wir zeigen, daß die gegebene totale Ordnung die Ordnung von K fortsetzt. Es seien $x, y \in K$ und $(\overline{x_n}), (\overline{y_n})$ die entsprechenden durch konstante Folgen dargestellten Elemente in $C(K)/N(K)$. Dann ist $x < y \iff y - x = 2\delta > \delta > 0 \iff \bigwedge n \geq 0$ gilt $y_n - x_n > \delta > 0 \iff (\overline{x_n}) < (\overline{y_n})$. Die Gleichheit überträgt sich wegen der Injektivität von $\varphi : K \longrightarrow C(K)/N(K)$.

7) Es bleiben die Monotoniegesetze zu zeigen. Seien $(\overline{x_n}) \leq (\overline{y_n})$ und $(\overline{z_n}) \in C(K)/N(K)$ gegeben. Für jedes $\varepsilon > 0$ gibt es ein $n_0 \in \mathbb{N}_0$, so daß für alle $n \in \mathbb{N}_0$ gilt $x_n - y_n < \varepsilon$. Dann gilt aber auch $(x_n + z_n) - (y_n + z_n) < \varepsilon$. Damit folgt $(\overline{x_n}) + (\overline{z_n}) \leq (\overline{y_n}) + (\overline{z_n})$.

8) Seien jetzt $(\overline{x_n}) \leq (\overline{y_n})$ und $0 \leq (\overline{z_n})$ gegeben. Zu zeigen ist $(\overline{x_n})(\overline{z_n}) \leq (\overline{y_n})(\overline{z_n})$. Es gibt ein $z \in K$ mit $z > |x_n - y_n|$ und $z > |z_n|$. Zu $\varepsilon > 0$ sei ein $n_0 \in \mathbb{N}_0$ gewählt, so daß für alle $n \geq n_0$ gilt $-z_n < \frac{\varepsilon}{z}$ wegen $(\overline{z_n}) \geq 0$ und $x_n - y_n < \frac{\varepsilon}{z}$ wegen $(\overline{x_n}) \leq (\overline{y_n})$.
Dann gilt $x_n z_n - y_n z_n = (x_n - y_n) z_n < \varepsilon$ für alle $n \geq n_0$.
Ist nämlich $z_n \geq 0$, so ist $z_n < z$ und damit $(x_n - y_n) z < \varepsilon$.
Ist $z_n < 0$ und $x_n - y_n \geq 0$, so ist $(x_n - y_n) z_n \leq 0$.
Ist schließlich $z_n < 0$ und $x_n - y_n < 0$, so ist $-z_n < \frac{\varepsilon}{z}$ und $y_n - x_n < z$, also $(x_n - y_n) z_n < z \frac{\varepsilon}{z} = \varepsilon$.
Damit ist auch $(\overline{x_n})(\overline{z_n}) \leq (\overline{y_n})(\overline{z_n})$ bewiesen.

4.7. F o l g e r u n g:
Seien $(\overline{x_n}), (\overline{y_n}) \in C(K)/N(K)$ gegeben mit $(\overline{x_n}) < (\overline{y_n})$. Dann existiert ein $z \in K$ mit $(\overline{x_n}) < z < (\overline{y_n})$. Man sagt dann auch, daß K dichte Teilmenge von $C(K)/N(K)$ ist.

B e w e i s: Nach Punkt 2) des Beweises von Satz 4.6. gibt es ein $\delta > 0$ und ein $n_0 \in \mathbb{N}_0$, so daß für alle $n \geq n_0$ gilt $y_n - x_n > \delta$. Sei ε mit $4\varepsilon = \delta$ gewählt. Dann gibt es ein $n_1 \geq n_0$, so daß für alle $n \geq n_1$ gilt $|y_n - y_{n_1}| < \varepsilon$ und $|x_n - x_{n_1}| < \varepsilon$. Für $z := x_{n_1} + 2\varepsilon$ gilt
$y_n - z = y_n - y_{n_1} + y_{n_1} - x_{n_1} - 2\varepsilon > y_{n_1} - x_{n_1} - 3\varepsilon > \varepsilon$ und
$z - x_n = x_{n_1} - x_n + 2\varepsilon > \varepsilon$ für alle $n \geq n_1$. Damit folgt $(\overline{x_n}) < z < (\overline{y_n})$.

Wir nennen einen angeordneten Körper K folgen-vollständig, wenn jede Cauchy-Folge aus $C(K)$ in K konvergiert. Eine Cauchy-Folge $(x_n) \in C(K)$ hat den Grenzwert $x \in K$ genau dann, wenn $(\overline{x_n}) = x$ in $C(K)/N(K)$ gilt. Das folgt direkt aus den Definitionen. Damit ist aber $K = C(K)/N(K)$ genau dann, wenn K folgen-vollständig ist. Wegen der Identifizierung von K mit einem Unterkörper von $C(K)/N(K)$ kann man Cauchy-Folgen mit Koeffizienten aus K auch auffassen als spezielle Cauchy-Folgen in $C(K)/N(K)$. Wir werden zeigen, daß bei dieser Auffassung jede Cauchy-Folge (x_n) in K den Grenzwert $(\overline{x_n})$ in $C(K)/N(K)$ besitzt. $C(K)/N(K)$ entsteht also aus K durch Hinzunahme aller Grenzwerte von Cauchy-Folgen in K. Schließlich werden wir weiter beweisen, daß $C(K)/N(K)$ folgen-vollständig ist, also alle Cauchy-Folgen in $C(K)/N(K)$, nicht nur die mit Koeffizienten aus K, konvergieren. Damit gilt $L = C(L)/N(L)$ für $L = C(K)/N(K)$, die angegebene Konstruktion der "Vervollständigung" von K (zu $C(K)/N(K)$) führt durch Iteration nicht

mehr zu weiteren echten Körpererweiterungen. Zunächst beweisen wir einen Hilfssatz über das Verhalten des Betrages in $C(K)/N(K)$.

4.8. H i l f s s a t z:
Für $\varepsilon \in C(K)/N(K)$, $\varepsilon > 0$ und $(\overline{x_n}),(\overline{y_n}) \in C(K)/N(K)$ gilt $|(\overline{x_n})-(\overline{y_n})| < \varepsilon$ genau dann, wenn es ein $\delta \in K$ mit $0 < \delta < \varepsilon$ und ein $n_0 \in \mathbb{N}_0$ gibt, so daß für alle $n \geq n_0$ gilt $|x_n - y_n| < \delta$.

B e w e i s: Sei $|(\overline{x_n})-(\overline{y_n})| < \varepsilon$. Dann gibt es nach 4.7. ein $\delta \in K$ mit $|(\overline{x_n})-(\overline{y_n})| < \delta < \varepsilon$, also mit $(\overline{x_n})-(\overline{y_n}) < \delta$ und $(\overline{y_n})-(\overline{x_n}) < \delta$. Nach der Charakterisierung der Ordnung von $C(K)/N(K)$ im Beweis von 4.6. gibt es ein $\eta > 0$, $\eta \in K$ und $n_0 \in \mathbb{N}_0$, so daß für alle $n \geq n_0$ gilt $\delta - x_n + y_n > \eta$ und $\delta - y_n + x_n > \eta$, also $|x_n - y_n| < \delta - \eta < \delta$.
Das beweist die eine Richtung der Behauptung.
Sei ein $\delta \in K$ mit $0 < \delta < \varepsilon$ gegeben und ein $n_0 \in \mathbb{N}_0$, so daß für alle $n \geq n_0$ gilt $|x_n - y_n| < \delta$. Dann existiert ein $\eta \in K$ mit $\delta < \delta + \eta < \varepsilon$. Für $n \geq n_0$ gilt dann $0 < \delta - x_n + y_n$ und $0 < \delta - y_n + x_n$, also auch $\eta < \varepsilon - x_n + y_n$ und $\eta < \varepsilon - y_n + x_n$. Daraus folgt $(\overline{x_n})-(\overline{y_n}) < \varepsilon$ und $(\overline{y_n})-(\overline{x_n}) < \varepsilon$,also auch $|(\overline{x_n})-(\overline{y_n})| < \varepsilon$.

4.9. S a t z:
Sei $(x_n) \in C(K)$. Dann hat (x_n) in $C(K)/N(K)$ den Grenzwert $(\overline{x_n})$.

B e w e i s: Es gilt wegen $(x_n) \in C(K)$
$\wedge\, \delta > 0, \delta \in K \vee n_0 \in \mathbb{N}_0 \wedge t,n \geq n_0 \,[\, |x_t - x_n| < \delta \,]$.
Daraus folgt $\wedge\, \varepsilon > 0, \varepsilon \in C(K)/N(K) \vee n_0 \in \mathbb{N}_0 \wedge t \geq n_0 \vee \delta \in K,$
$0 < \delta < \varepsilon \quad \wedge\, n \geq n_0 \,[\, |x_t - x_n| < \delta \,]$.
Das impliziert $\wedge\, \varepsilon > 0 \vee n_0 \in \mathbb{N}_0 \wedge t \geq n_0 \,[\, |x_t - (\overline{x_n})| < \varepsilon \,]$,
was die geforderte Behauptung ergibt.

4.10. S a t z:

$C(K)/N(K)$ ist folgen-vollständig.

B e w e i s:

1) Sei (y_i) eine Cauchy-Folge in $C(K)/N(K)$ mit $y_i = (\overline{x_{i,n}})$ für alle $i \in \mathbb{N}_0$, $x_{i,n} \in K$. Zunächst wählen wir besonders geeignete Repräsentanten für die y_i aus. Sei i fest vorgegeben und sei $\varepsilon_j = \frac{1}{j}$ für $j \in \mathbb{N}_0$, $j \neq 0$ und $\varepsilon_0 = 1$. Durch Induktion erhalten wir zu jedem $j \in \mathbb{N}_0$ ein n_j mit $n_j \geq \max(n_{j-1}, j)$, so daß für alle $m,n \geq n_j$ gilt $|x_{i,m} - x_{i,n}| < \varepsilon_j$. Wir definieren Folgen $z_{i,j} := x_{i,n_j}$ für jedes $i \in \mathbb{N}_0$.

2) Es ist zu zeigen $(z_{i,j}) \in C(K)$ für alle $i \in \mathbb{N}_0$. Zu jedem $\varepsilon > 0$, $\varepsilon \in K$ existiert ein j mit $\varepsilon > \varepsilon_j > 0$ und für alle $s,t \geq j$ gilt $|z_{i,s} - z_{i,t}| = |x_{i,n_s} - x_{i,n_t}| < \varepsilon_j < \varepsilon$ wegen $n_s, n_t \geq n_j$.

3) Wir zeigen jetzt, daß $y_i = (\overline{z_{i,n}})$ für alle $i \in \mathbb{N}_0$ gilt. Für jedes $\varepsilon > 0$ existiert ein $j \in \mathbb{N}_0$, so daß für alle $m \geq n_j$ gilt $|z_{i,m} - x_{i,m}| = |x_{i,n_m} - x_{i,m}| < \varepsilon_j < \varepsilon$ wegen $n_m \geq m \geq n_j$. Damit ist $(z_{i,m} - x_{i,m})$ eine Nullfolge, also $(\overline{z_{i,m}}) = (\overline{x_{i,m}})$.

4) Es gibt zu jedem $\varepsilon > 0$, $\varepsilon \in C(K)/N(K)$ ein $n_0 \in \mathbb{N}_0$, so daß für alle $m,n,i,k \geq n_0$ gilt $|z_{i,m} - z_{k,n}| < \varepsilon$. Da (y_i) eine Cauchy-Folge ist, gibt es nämlich zu jedem $\varepsilon > 0$ ein $n_1 \in \mathbb{N}_0$, so daß für alle $i,k \geq n_1$ gilt $|y_i - y_k| < \frac{\varepsilon}{3}$, also gibt es ein $n_2 = n_2(i,k) \in \mathbb{N}_0$, so daß für alle $l \geq n_2$ gilt $|z_{i,l} - z_{k,l}| < \frac{\varepsilon}{3}$ nach Hilfssatz 4.8. Weiter gibt es ein j mit $0 < \varepsilon_j < \frac{\varepsilon}{3}$, so daß für alle $i,m,n \geq j$ gilt $|z_{i,m} - z_{i,n}| < \varepsilon_j$ nach Konstruktion der $z_{i,m}$. Für alle i,k, $m,n \geq n_0 := \max(j, n_1)$ gibt es daher ein $l \geq \max(j, n_1, n_2(i,k))$, so daß gilt

$|z_{i,m}-z_{k,n}| \leq |z_{i,m}-z_{i,\ell}|+|z_{i,\ell}-z_{k,\ell}|+|z_{k,\ell}-z_{k,m}| < \varepsilon_j + \frac{\varepsilon}{3} + \varepsilon_j < \varepsilon$.

5) Es ist $(z_{i,i} \mid i \in \mathbb{N}_0)$ eine Cauchy-Folge. Nach 4) gibt es nämlich zu jedem $\varepsilon > 0$, $\varepsilon \in K$ ein $n_0 \in \mathbb{N}_0$, so daß für alle $i,j \geq n_0$ gilt $|z_{i,i} - z_{j,j}| < \varepsilon$.

6) $(\overline{z_{i,i}})$ ist der Grenzwert von (y_i) in $C(K)/N(K)$, denn zu jedem $\varepsilon > 0$, $\varepsilon \in C(K)/N(K)$ existiert ein $j \in \mathbb{N}_0$, so daß für alle $i,n \geq j$ gilt $|z_{i,n} - z_{n,n}| < \varepsilon_j < \varepsilon$ nach 4). Wegen Hilfssatz 4.8. folgt damit $|y_i - (\overline{z_{i,i}})| < \varepsilon$ für alle $i \geq j$.

Zum Schluß dieses Abschnittes wollen wir noch eine der wichtigsten Eigenschaften der reellen Zahlen beweisen, die äquivalent zur Folgen-Vollständigkeit ist, aber technisch leichter verwendbar ist.

4.11. S a t z:
Jede nicht-leere, beschränkte Menge M in $\mathbb{R}$ besitzt ein Supremum und ein Infimum.

B e w e i s: Wir definieren zwei Folgen rationaler Zahlen (a_n) und (b_n) mit i) $a_n < b_n$ für alle $n \in \mathbb{N}_0$

ii) $\{x \in M \mid a_n < x \leq b_n\} \neq \emptyset$

iii) $\{x \in M \mid b_n < x\} = \emptyset$.

Sei nämlich $r \in \mathbb{Q}$ mit $-r < x < r$ für alle $x \in M$. Sei $a_0 := -r$, $b_0 := r$. Dann sind sicher i),ii), und iii) erfüllt. Seien a_n, b_n schon konstruiert. Ist $\{x \in M \mid \frac{a_n+b_n}{2} < x\} = \emptyset$, so sei $a_{n+1} := a_n$ und $b_{n+1} := \frac{a_n+b_n}{2}$. Sonst sei $a_{n+1} := \frac{a_n+b_n}{2}$ und $b_{n+1} := b_n$. Dann sieht man leicht, daß auch a_{n+1} und b_{n+1} die Bedingungen i), ii) und iii) erfüllen. Wegen $a_n \leq a_{n+1} < b_{n+1} \leq b_n$ und $b_n - a_n = \frac{r}{2^{n-1}}$, wie durch

Induktion sofort gesehen werden kann, ist $|a_m - a_n| < \frac{r}{2^{n-1}}$ für alle $m \geq n$, also ist (a_n) eine Cauchy-Folge. Dasselbe gilt für (b_n). Wegen $b_n - a_n = \frac{r}{2^{n-1}}$ ist $(b_n - a_n)$ eine Nullfolge, also $(\overline{a_n}) = (\overline{b_n})$. Für alle $m \in \mathbb{N}_0$ gilt sogar $a_m \leq (\overline{a_n}) \leq b_m$. Für jedes $x \in \mathbb{R}$ mit $(\overline{a_n}) < x$ gibt es ein $m \in \mathbb{N}_0$ mit $(\overline{a_n}) \leq b_m < x$, also ist $x \notin M$ und $(\overline{a_n})$ eine obere Schranke von M. Ebenso gibt es für jedes $y < (\overline{a_n})$ ein $m \in \mathbb{N}_0$ mit $y < a_m \leq (\overline{a_n})$ und damit ein $x \in M$ mit $y < a_m < x$, also ist y keine obere Schranke von M. Damit ist $(\overline{a_n})$ das Supremum von M. Der Beweis für die Existenz der Infimums verläuft analog und sei dem Leser überlassen.

§ 5 Die komplexen Zahlen

In diesem kurzen Abschnitt soll die Definition des Körpers der komplexen Zahlen gegeben werden. Der Körper der komplexen Zahlen ist kein angeordneter Körper, denn es gibt komplexe Zahlen, deren Quadrat $-1 < 0$ ist im Widerspruch zu den unter 3.6. entwickelten Rechenregeln.
Daher brauchen wir auch keine Ordnung zu definieren. Andere Eigenschaften des Körpers der komplexen Zahlen werden in der Funktionentheorie bewiesen, insbesondere der Fundamentalsatz der Algebra, der besagt, saß jedes komplexe Polynom vom Grade größer oder gleich 1 mindestens eine komplexe Nullstelle besitzt.

Wir beweisen, daß $\mathbb{R}\times\mathbb{R}$ mit der Addition

$$(x,y)+(x',y') := (x+x',y+y')$$

und der Multiplikation

$$(x,y)\,(x',y') := (xx'-yy',xy'+x'y)$$

einen kommutativen Körper bildet, den Körper $\mathbb{C}$ der komplexen Zahlen.

Es ist klar, daß $\mathbb{R}\times\mathbb{R}$ mit der Addition eine kommutative Gruppe bildet. Die Ringeigenschaften von $\mathbb{C}$ lassen sich durch Nachrechnen leicht verifizieren. Das neutrale Element bei der Multiplikation ist dabei $(1,0)$. Inverses Element zu $(x,y) \neq (0,0)$ ist $\left(\frac{x}{x^2+y^2}, -\frac{y}{x^2+y^2}\right)$. Auch das kann sofort nachgerechnet werden.

Die Abbildung $\mathbb{R} \ni x \longmapsto (x,0) \in \mathbb{C}$ ist ein injektiver Ring-Homomorphismus. Daher identifiziert man $\mathbb{R}$ mit dem Unterkörper $\{(x,0) \mid x \in \mathbb{R}\}$ in $\mathbb{C}$.
Üblicherweise schreibt man $i := (0,1)$ und allgemein $x+yi = (x,y)$. Insbesondere ist dann $i^2 = -1$.