Skript

Elemente der Algebra und Zahlentheorie

WS 2005/06 bei Prof. Zink

an der Humboldt Universität zu Berlin

Autor: Ewald Stamp

VL-Stand: 31.1.2006 , Letzte Änderung: 13.05.2006

Dieses Skript ist unvollständig und enthält mit Sicherheit Fehler. Insbesondere enthält es keine Beweise und Kapitel 6 ist unvollständig. Es ist nur als Ergänzung zur Vorlesung gedacht. Fehler bitte an stamp@mathematik.hu-berlin.de senden.

Inhaltsverzeichnis

0 Einführung

1. VL
24.10.05

Das Ziel der Vorlesung ist vor allem ein möglichst strenger und lückenloser Aufbau der Zahlbereiche. Es geht also um die Grundlagen, die unserem mehr oder weniger naiven, aber durch täglichen Erfahrung gut motivierten Umgang mit Zahlen zugrunde liegen. Es geht also um eine Reflexion von Dingen, mit denen wir von der Schule an ganz selbstverständlich umgehen.

Dazu gehört vor allem, dass wir uns die Axiome, d.h. die Spielregeln, klar machen auf denen unser Umgang mit Zahlen beruht, und dass wir aus diesen Axiomen die Rechengesetze deduktiv erschließen.

Axiomatischer Aufbau der Zahlenbereiche

Natürliche Zahlen	$\mathbb{N}$
Ganze Zahlen	$\mathbb{Z}$
Rationale Zahlen	$\mathbb{Q}$
Reelle Zahlen	$\mathbb{R}$
komplexe Zahlen	$\mathbb{C}$
p-adische Zahlen	$\mathbb{Q}_p$

Tabelle 1: Die Zahlbereiche

Die *natürlichen Zahlen* sind so alt wie die Menschheit. Sie entspringen aus dem Umgang mit Dingen. Aus allen alten Kulturen ist uns der Umgang mit Zahlen und dem Rechnen überliefert (Ägypten, Babel, Griechenland).

Die heutige positionelle Dezimalnotation mit 0 und den Ziffern $1,\dots,9$ entstand in Indien, Zeit -300 bis +500. Die indische Notation wurde von den Arabern insbesondere den Astronomen übernommen. Arabisch: *al-sifr* für die Null, aus der das Wort *cifra* abgeleitet wurde. Noch bei Gauß war cifra die Bezeichnung für 0. Symbol für die Null in Indien war eine $\circ$ oder $\bigcirc$.

Aus der Erfahrung, dass es neben einem Vorwärts auch ein Rückwärts, dass jeder Weg zwei Orientierungen hat, entspringen die *ganzen Zahlen* (Rechenregeln für positive und negative Zahlen bei BRAHMAGUPTA, *598) und aus dem Abmessen von Gegenständen ergibt sich die Notwendigkeit der Einführung der *rationalen Zahlen*.

Abstraktionen die über unsere Lebenswirklichkeit hinausgehen, sind das Unendliche und das Irrationale. Trotzdem die Menschheit niemals alle natürlichen Zahlen benutzen wird, wäre es willkürlich abzubrechen. Eine Reflexion führt also notwendig auf die Betrachtung *unendlicher Mengen*, trotzdem es solche Mengen in der Praxis nirgends gibt. Aber im Denken der Menschheit ist das Unendliche verankert.

Ebenso kann man nur durch Reflexion einsehen, dass es Zahlen geben muss, die nicht durch Brüche, also durch fortgesetzte Verfeinerung der Teilungsskala gemessen werden können (wie $\sqrt{2}$). Das werden Sie in der Praxis nie feststellen können.

Erst relativ spät in der Geschichte der Menschheit wurden die *komplexen* (imaginären) und noch viel später die *p-adischen Zahlen* entdeckt.

Die imaginären Zahlen erscheinen unweigerlich, wenn man versucht algebraische Gleichungen zu lösen (z.B. $x^2 + 1 = 0$). Sei der Renaissance (Geronimo CARDANO 1501-1570) werden sie betrachtet (unmögliche Zahlen). Rafael BOMBELLI (1526-1572) hat als erster das formal korrekte Rechnen mit komplexen Zahlen gelehrt. Die komplexen Zahlen bilden insbesondere einen 2-dimensionalen $\mathbb{R}$-Vektorraum, kann also durch eine Ebene leicht veranschaulicht werden. Besonderheit ist die Multiplikation. Hauptbedeutung von $\mathbb{C}$ liegt im *Fundamentalsatz der Algebra*, d.h. jede algebraische Geichung

$$a_n x^n + a_{n-1} + \cdots + a_1 x + a_0 = 0$$

mit „Zahlenkoeffizienten“ ist in $\mathbb{C}$ lösbar.

Die *p-adischen Zahlen* zu einer Primzahl p entsprangen der Beobachtung, dass man nicht nur Funktionen, sondern auch Zahlen in Potenzreihen entwickeln kann, und dass man neben dem naiven Abstand auch einem p-adischen Abstand zwischen rationalen Zahlen betrachten kann. Das wurde erst durch Kurt HENSEL (1861-1941) bemerkt. Grundidee der p-adischen Metrik: Nenne zwei ganze Zahlen p-adisch dicht beieinander, wenn ihre Differenz durch eine *hohe* Potenz von p teilbar. Abstand 0: Differenz ist durch jede Potenz von p teilbar. Dies geht nur, wenn beide Zahlen gleich sind.

Hilberts Hotel

Die natürlichen Zahlen gründen auf der Erfahrung des Zählens. Prinzipien:

(i) Durch Zählen kann man jede natürliche Zahl erreichen.

(ii) Der Abzählprozess hat kein natürliches Ende. An jeder Stelle hat man die Möglichkeit, um eins weiter zu zählen.

Die Erfahrung des Unendlichen wir am Beispiel von Hilberts Hotel (David HILBERT, 1862-1943, Göttingen) klar gemacht. Das Hotel hat unendlich viele Zimmer, nummeriert durch natürliche Zahlen, es hat nur Einzelzimmern, und in jedem Zimmer wohnt ein Gast – also voll belegt.

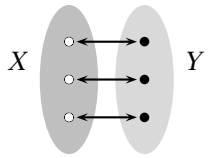
Jetzt erscheinen mitten in der Nacht 10 Personen, welche alle ein Einzelzimmer benötigen. In einem normalen Hotel müsste der Portier diese Leute wegschicken. In Hilberts Hotel gibt es bei entsprechender Hilfsbereitschaft der Gäste kein Problem. Der Portier bittet einfach alle Gäste 10 Zimmer weiter zu ziehen. Also der Gast aus Zimmer n zieht um in das Zimmer mit der Nummer $n+10$ (1 nach 11, 2 nach 12, 3 nach 13, u.s.w). Damit ist jeder Gast wieder untergebracht, und gleichzeitig sind die ersten 10 Zimmer frei geworden.

Der Portier könnte auch noch radikaler vorgehen. Um den Gästen weitere Umzüge zu ersparen, lässt er einfach den Gast aus Zimmer n in das Zimmer $2n$ umziehen (also 1 nach 2, 2 nach 4, 3 nach 6, ...). Damit sind plötzlich nur noch die Zimmer mit geraden Nummern belegt, und der Portier kann in aller Ruhe beliebig viele Neuankömmlinge empfangen.

Die Unendlichkeiten

Ob es die Menge der natürlichen Zahlen in ihrer Gesamtheit wirklich gibt, ist eine Glaubensfrage. Zeige: Es gibt unendliche Mengen genau dann, wenn es die Menge $\mathbb{N}$ gibt.

$\mathbb{N}$, der Bereich der natürlichen Zahlen, ist die erste Stufe von ∞. Welche unendlichen Mengen wollen wir als gleichwertig ansehen? Eine Menge X ist *gleichmächtig* einer Menge Y, wenn man zwischen den Elementen von X und Y eine umkehrbar eindeutige Zuordnung herstellen kann.



Satz von Cantor: Betrachten Menge M und dazu betrachten wir die so genannte Potenzmenge $\mathcal{P}(M)$,deren Elemente die Teilmengen von M sind, einschließlich $\emptyset$ und M selbst. Z.B. $\#M = 5$, dann ist $\#\mathcal{P}(M) = 2^5$. Das gilt auch für unendliche Mengen:

$$\#M < \#\mathcal{P}(M)$$

Es gibt also beliebig große Unendlichkeiten, indem man beginnend mit N fortgesetzt zur Potenzmenge übergeht.

$$\#N = \#\mathbb{Q} = \infty \qquad \#\mathbb{R} = 2^\infty$$

1 Die natürlichen Zahlen

1.1 Wiederholungen – Mengen und Abbildungen

Mengen

Definition ((Naive) Menge)**.** *Eine Menge X ist eine Gesamtheit von Objekten, welche Elemente von X genannt werden.*

Definition (Gleichheit von Mengen)**.** *$X = Y$: Jedes $x \in X$ gehört auch zu Y, jedes $y \in Y$ gehört auch zu X. Schreiben:*

$$x \in X \Rightarrow x \in Y$$
$$x \in X \Leftarrow y \in Y$$

Folgerung. *Die Gleichheit von Mengen ist eine Äquivalenzrelation, d.h. es gilt:*

(i) Reflexivität: $X = X$

(ii) Symmetrie: $X = Y \Rightarrow Y = X$

(iii) Transitivität: $X = Y$ und $Y = Z \Rightarrow X = Z$

Notation. $X = \{1,2,3,4\}$ und $Y = \{2,3,1,4\}$ sind gleiche Mengen.

Definition (Mengeninklusion)**.** *Inklusion von Mengen $A \subseteq B : x \in A \Rightarrow x \in B$, aber möglicherweise nicht umgekehrt.*

Beispiel. Die Menge der Brillenträger als Teilmenge aller Hörer in diesem Hörsaal.

Lemma. *Die Inklusion ist eine partielle Ordnung, d.h. es gilt:*

(i) Reflexivität: $A \subseteq A$

(ii) Antisymmetrie: $A \subseteq B, B \subseteq A \Rightarrow A = B$

(iii) Transitivität: $A \subseteq B, B \subseteq C \Rightarrow A \subseteq C$

Bemerkung. Die Inklusion von Mengen ist keine Totalordnung, d.h. es gilt nicht: für zwei Mengen A, B gilt entweder $A \subseteq B$ oder $B \subseteq A$. Dies ist für Mengen verletzt. Typisches Beispiel einer Totalordnung ist die lexikographische[1] Ordnung.

Definition (Mengen-Operationen)**.**

$$X \cup Y \qquad X \cap Y \qquad X \setminus Y$$

Mit *Venn-Diagrammen* können die Mengenoperationen graphisch dargestellt werden:

$A \cup B$ $A \cap B$ $A \setminus B$

Definition (Leere Menge $\emptyset$)**.** *Die $\emptyset$ hat kein Element. Die leere Menge ist in jeder beliebigen Menge X enthalten: $\emptyset \subseteq X$. D.h. für jedes X:*

$$x \in \emptyset \Rightarrow x \in X$$

Da es kein $x \in \emptyset$ gibt, muss diese Aussage nicht nach geprüft werden. Es ist eine so genannte leere Aussage. Leere Aussagen werden in der Mathematik als wahre Aussagen eingestuft.

Abbildungen

Definition (Abbildung)**.** *Eine Abbildung $f : X \to Y$ zwischen zwei Mengen ist eine eindeutige Zuordnung:*

$$X \ni x \mapsto f(x) \in Y$$

($\mapsto$: „ist zugeordnet“, „geht über in“). Wichtig ist die Eindeutigkeit.

$X =$ Objektmenge $\qquad Y =$ Datenmenge

Einwohner Berlins $\xrightarrow{f}$ Geburtsdatum

Bücher $\xrightarrow{f}$ ISBN-Nummer

Viele Möglichkeiten Daten zuzuordnen: Alter eines Einwohners, Höhe eines Berges, Temperatur eines Körpers etc.

Gegenbeispiel. Eine nicht eindeutige Zuordnung: $\mathbb{R}_+$ seien die positiven reellen Zahlen.

$$f : \mathbb{R}_+ \to \mathbb{R}$$
$$x \mapsto f(x) = \sqrt{x}$$

ist keine eindeutige Abbildung, dann $\sqrt{4}$ kann sowohl 2, als auch -2 sein. Um die Abbildung eindeutig zu machen, muss man präzisieren, ob man die positive oder negative Wurzel nimmt.

Definition (Komposition)**.** *Sind $f : X \to Y$ und $g : Y \to Z$ zwei Abbildungen, dann ist die :*

$$g \circ f : X \to Z$$

wobei $(g \circ f)(x) = g(f(x))$.

Beispiel. Zum Beispiel seien $X =$ Personen, $Y =$ Orte, $Z =$ Anzahl der Einwohner (des Ortes): $f : P \mapsto O(P), g : O \mapsto \#O$. Komposition: $g \circ f : P \mapsto \#O(P)$.

Definition (Selbstabbildungen)**.** *Selbstabbildungen sind Abbildungen einer Menge in sich: $f : X \to X$.*

Beispiel: $f : \mathbb{N} \to \mathbb{N}, n \mapsto f(n) = 2n$ Verdoppelung. Selbstabbildungen kann man iterieren:

$$f : n \mapsto 2n \quad f \circ f : n \mapsto 4n \quad f \circ f \circ f : n \mapsto 8n$$

Definition (injektiv, surjektiv, bijektiv)**.** *Eine Abbildung $f : X \to Y$ heißt*

(i) injektiv, falls $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$

(ii) surjektiv, falls zu jedem $y \in Y$ ein $x \in X$ existiert, so dass $f(x) = y$.

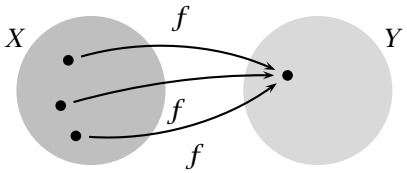
(iii) bijektiv, falls sie injektiv und surjektiv ist.

[1] Wie z.B. die Reihenfolge der Wörter in Lexika oder Wörterbüchern.

2. VL
25.10.05

Definition (Bild, Faser). *Das Bild*[2] *von $f : X \to Y$ und die Faser eines Elements $y \in Y$ (Faser über y):*

$$\operatorname{im}(f) = \{y \in Y : \exists x \in X : f(x) = y\}$$
$$f^{-1}(y) = \{x \in X : f(x) = y\}$$



Beispiel.

$$f : X \to Y$$
Einwohner Berlins Geburtsdaten
$$x \mapsto f(x)$$

Das Bild der Abbildung f sind alle Geburtsdaten, die für mindestens eine in Berlin lebende Person zutreffen. Sei $y = 25\ 10\ 1980$, dann ist die Faser $f^{-1}(y)$ die Menge aller Personen in Berlin, die heute 25 Jahre alt werden.

Die Abbildung ist weder surjektiv (nicht alle möglichen Daten kommen als Geburtsdatum einer in Berlin lebenden Person in Frage) noch injektiv (das Geburtsdatum reicht nicht aus, um einen Berliner zu identifizieren).

Bemerkung. Sei $f : X \to Y$ eine Abbildung. Dann bilden die Fasern von f eine *Partition* der Menge X, d.h. X ist disjunkte Vereinigung der Fasern:

$$X = \dot{\bigcup}_{y \in Y} f^{-1}(y)$$

(Zwei Mengen sind disjunkt, wenn ihr Durchschnitt leer ist.)

Folgerung. *Betrachte $f : X \to Y$, und die Menge X sei endlich. Dann gilt:*

$$\#X = \sum_{y \in Y} \#f^{-1}(y)$$

Folgerung. *Eine Eigenschaft endlicher Mengen X:*

(i) Eine injektive Selbstabbildung $f : X \to X$ ist automatisch auch surjektiv.

(ii) Eine surjektive Selbstabbildung ist automatisch auch injektiv.

Beweis. □

[2] englisch *image*: im

1.2 Die Peanoschen Axiome

Peanosche Axiome

Die Menge $\mathbb{N}$ der natürlichen Zahlen ist (bis auf Isomorphie) durch folgende Eigenschaften (Axiome) charakterisiert (nach Guiseppe PEANO, 1858-1932, italienischer Mathematiker):

1.2.1 Definition (Peanoschen Axiome). *Wir bezeichnen eine Menge N als Menge natürlicher Zahlen, wenn es eine Selbstabbildung $\nu : N \to N, n \mapsto \nu(n)$ gibt, so dass für das Paar (N, ν) folgendes gilt:*

(i) ν ist injektiv, d.h. wenn $\nu(n) = \nu(m)$, dann folgt $n = m$.

(Wenn y im Bild von ν liegt, dann gibt es genau ein x mit $\nu(x) = y$. Mann nennt y den Vorgänger von x.)

(ii) ν nicht surjektiv, d.h. es gibt in N mindestens ein Elemente n, das nicht im Bild der Nachfolgeabbildung ν liegt. Wir sagen dann, n hat keinen Vorgänger.

(iii) Unter den Elementen ohne Vorgänger gibt es ein Element, welches wir $\mathbb{1}$ nennen, mit folgender Eigenschaft:

Ist $M \subseteq N$ Teilmenge, so dass

a) $\mathbb{1} \in M$

b) zu jedem $n \in M$ liegt sein Nachfolger $\nu(n) \in M$

Dann muss $M = N$ sein.

Bemerkung. (i) Wir schreiben auch $\nu(n) =: n'$.

(ii) ν heißt Nachfolgeabbildung, $\nu(n)$ heißt der Nachfolger von n.

(iii) $\nu(n)$ muss man sich als $n + 1$ vorstellen, und N als eine unendliche Menge, weil ν injektiv aber nicht surjektiv ist.

(iv) Insbesondere ist N nicht leer und eine unendliche Menge.

(v) Man nennt (iii) das Induktionsaxiom.

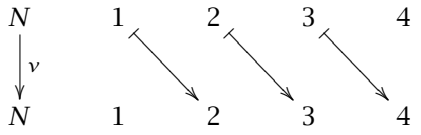
1.2.2 Lemma. *Aus dem Induktionsaxiom folgt, dass $\mathbb{1} \in N$ einzige Element ohne Vorgänger ist. D.h. $\nu : \mathbb{N} \leftrightarrow \mathbb{N} \setminus \{\mathbb{1}\}$ ist Bijektion.*

Beweis. □

1.2.3 Lemma. *Für alle $x \in \mathbb{N}$ gilt $x' \neq x$. D.h. der Nachfolger ist ungleich seinem Vorgänger.*

Beweis. □

Bemerkung.
- Sei $\mathbb{R}_{\geq 1}$ die Menge der reellen Zahlen ≥ 1, und sei $\nu(x) = x + 1$. Dann sind die Axiome (i), (iii) erfüllt, aber nicht das Induktionsaxiom (iii).
- Im Bild von Hilberts Hotel bedeutet die Nachfolgerabbildung ν, dass jeder Gast in das nächste Zimmer umzieht:



- Die Injektivität bedeutet: Wenn $x \in \mathbb{N}$ einen Vorgänger hat, d.h. $x = n'$, dann ist der Vorgänger n eindeutig bestimmt.

Addition

Grundgedanke. Um $n+m$ zu bilden, müssen wir auf n m-mal die Nachfolgeabbildung ν anwenden.

Es sei nun $N \times N$ die Menge aller geordneten Paare (x, y) mit Einträgen $x, y \in N$ ($N \times N$ ist das cartesiche Produkt von N mit sich selbst, $(x, y) \neq (y, x)$). Wir wollen eine Abbildung

$$\begin{aligned} N \times N &\to N \\ (x, y) &\mapsto \psi(x, y) \end{aligned}$$

definieren. Später schreiben wir

$$\psi(x, y) = x + y$$

und nennen dies die Summe von x und y.

1.2.4 Definition (Addition)**.** *Es sei $x \in N$ beliebig fixiert. Wir wollen $\psi(x, y)$ für alle $y \in N$ definieren. Wir nennen $M_x \subseteq N$ die Menge aller y für $\psi(x, y)$ definiert ist.*

(i) Für $y = \mathbb{1}$ definieren wir

$$\psi(x, \mathbb{1}) = x' (= \nu(x)) \tag{A1}$$

Damit ist $\mathbb{1} \in M_x$.

(ii) Es sei $n \in M_x$, d.h. $\psi(x, n)$ sei bereits definiert. Dann setzen wir

$$\psi(x, n') := (\psi(x, n))' \tag{A2}$$

Damit ist auch $n' \in M_x$.

Damit ist $M_x = N$, d.h. wir haben $\psi(x, y)$ für alle $y \in N$ definiert.

Bemerkung. Unsere Bildungsvorschrift für $\psi(x, y)$ ist eindeutig. In der Definition gehen wir von n' zurück auf seinen Vorgänger n: $\psi(x, n') = \psi(x, n)'$. Für $y = \mathbb{1}$ ist das klar. Das ist aber eindeutig $\psi(x,1) = x'$. Der Nachfolger von x ist eindeutig bestimmt. Wir nehmen an, dass $\psi(x, n)$ bereits eindeutig erklärt ist. Dann ist auch $\psi(x, n') = \psi(x, n)'$ eine eindeutige Bildungsvorschrift, denn n' hat den eindeutig bestimmten Vorgänger n ($n' = m'$ mit $m \neq n$ ist unmöglich. Ansonsten wäre $\psi(x, n') = \psi(x, m)'$ möglicherweise nicht eindeutig.)

Zwischenergebnis. Wir haben also eine wohldefinierte Abbildung

$$\begin{aligned} \psi : N \times N &\to N \\ (x, y) &\mapsto \psi(x, y) \end{aligned}$$

Und nach Konstruktion haben wir

$$\psi(x, \mathbb{1}) = x' \tag{A1}$$
$$\psi(x, y') = \psi(x, y)' \tag{A2}$$

für alle $x, y \in N$.

Satz (Eindeutigkeit von $+$)**.** *Die Abbildung $\psi : N \times N \to N$ ist die einzige Abbildung mit den Eigenschaften (A1) und (A2).*

Beweis. □

Im Folgenden schreiben wir

$$\psi(x, y) =: x + y$$

Grundidee unserer Definition: Um $x + y$ zu bilden, beginnen wir bei x und zählen so oft weiter, wie der Wert y angibt.

1.2.5 Satz (Assoziativgesetz)**.** *Für alle $x, y, z \in N$ gilt:*

$$(x + y) + z = x + (y + z)$$

Beweis. □

1.2.6 Satz (Kommutativgesetz)**.** *Für $x, y \in N$ gilt*

$$x + y = y + x$$

Beweis. □

3. VL
31.10.05

Das Paar(N, ν) ist durch die Peano-Axiome in folgendem Sinne eindeutig bestimmt:

1.2.7 Lemma (Eindeutigkeit bis auf Isomorphie)**.** *Sind (N, ν) und (M, μ) zwei Peano-Mengen, dann existiert genau eine Abbildung $\varphi : N \to M$ mit*

$$\varphi(\mathbb{1}_N) = \mathbb{1}_M$$
$$\varphi \circ \nu = \mu \circ f$$

Insbesondere für $(N, \nu) = (M, \mu)$ gibt es nur die Identität.

1.3 Ordnung

Heuristik. ν fortgesetzt angewendet auf $\mathbb{1}$ ergibt alle Elemente auf N. Damit haben wir alle Elemente aus N in einer Reihenfolge (vorausgesetzt, dass die Anwendung von ν nicht in eine Schleife führt). Das ergibt die Ordnung.

1.3.1 Satz. *Wir zeigen $\forall x, y \in N$:*

$$x + y \neq y \tag{V1}$$

Wenn $y \neq z$ dann ist

$$x + y \neq x + z \tag{V2}$$

Man nennt (V2) auch Kürzungsregel der Addition, da es äquivalent ist zu: $x + y = x + z \Rightarrow y = z$.

Beweis. □

1.3.2 Definition (Ordnung, $<$)**.** *Seien $a, b \in N$. Wir sagen $a < b$ (oder auch $b > a$) falls ein $c \in N$ existiert, so dass $a + c = b$.*

Satz. *Wenn $a < b$, dann ist das c mit $a + c = b$ eindeutig bestimmt (V2). Wir schreiben dann auch $c =: b - a$.*

1.3.3 Satz. *Seien $a, b \in N$. Dann gilt höchstens eine der Beziehungen:*

$$a < b \qquad a = b \qquad a > b$$

Beweis. □

1.3.4 Satz. *Seien $a, b \in N$. Dann gilt mindestens eine der Beziehungen:*

$$a < b \qquad a = b \qquad a > b$$

Beweis. □

Ergebnis:

1.3.5 Satz (Trichotomie)**.** *Zu je zwei $a, b \in N$ tritt genau einer der Fälle*

$$a < b \qquad a = b \qquad a > b$$

ein.

1.3.6 Lemma (Eigenschaften)**.** *Seien $a, b, c, d \in N$. Dann gilt:*

(i) *Transitivität: $a < b$ und $b < c \Rightarrow a < c$*

(ii) *Monotonie: $a < c \Rightarrow a + c < b + c$*

(iii) *$a < c$ und $c < d \Rightarrow a + c < b + d$*

(iv) *Schreibe $a \leq b$, falls $a < b$ oder $a = b$. Dann ist $\leq$ eine Totalordnung auf N.*

Beweis. □

Definition (Totalordnung)**.** *Gilt für $(M, <)$ und für alle $a, b, c \in M$:*

(i) $a \leq a$

(ii) $a \leq b \wedge b \leq a \Rightarrow a = b$

(iii) $a \leq b \leq c \Rightarrow a \leq c$

(iv) $\forall a, b \in M : a \leq b \vee b \leq a$

dann ist $<$ eine Totalordnung auf M. Gelten nur $(i) - (iii)$, dann ist $<$ eine partielle Ordnung.

1.3.7 Satz. *Aus $\mathbb{1}$ bekommt man durch wiederholte Anwendung der Nachfolgerabbildung ν alle Elemente von N, und zwar jedes genau einmal.*

Beweis. □

1.3.8 Satz (Wohlordnungssatz)**.** *Die natürlichen Zahlen (N, ν) sind wohlgeordnet, d.h. jede nichtleere Teilmenge von $M \subseteq N$ enthält ein eindeutig bestimmtes kleinstes Element $m_0 \leq x \forall\, x \in M$.*

Beweis. □

1.4 Multiplikation

Heuristik. $x \cdot y$ = addiere fortgesetzt mit x so oft, wie der Wert y es angibt.

1.4.1 Definition und Satz (Multiplikation)**.** *Es gibt genau eine Selbstabbildung $\psi : N \times N \to N$ mit den Eigenschaften $\forall\, x, y \in N$:*

$$\psi(x, \mathbb{1}) = x \qquad \text{(M1)}$$
$$\psi(x, y') = \psi(x, y) + x \qquad \text{(M2)}$$

Man schreibt dann $x \cdot y := \psi(x, y)$ und nennt dies das Produkt von x und y.

Beweis. Genau wie im Fall der Addition. □

Also haben wir jetzt $N \times N \ni (x, y) \to x \cdot y \in N$, so dass

$$x \cdot \mathbb{1} = x \qquad \text{(M1)}$$
$$x \cdot y' = x \cdot y + x \qquad \text{(M2)}$$

Des weiteren beweist man hieraus die Rechenregeln.

1.4.2 Satz (Neutrales Element)**.** $\mathbb{1} \cdot x = x$

Beweis. □

1.4.3 Satz (Distributivität)**.** $(a + b)c = ac + bc$

Konvention: Multiplikation geht vor Addition.

Beweis. □

1.4.4 Satz (Kommutativität)**.** $y \cdot x = x \cdot y$

Beweis. □

1.4.5 Lemma. *Das vertauschte Distributivitätsgesetz: $a(b + c) = ab + ac$*

1.4.6 Satz (Assoziativität)**.** $(ab)c = a(bc)$

Beweis. □

1.4.7 Satz (Kürzungsregel)**.** *Seien $a, b, c \in N$ und sei $ab = ac$. Dann folgt daraus $b = c$.*

Beweis. □

1.4.8 Lemma. *Seien $a, b, c \in N$. Dann gilt $a < b$ genau dann wenn $ac < bc$, und in diesem Fall ist $bc - ac = (b - a)c$.*

Beweis. □

Satz (Haubersches Theorem)**.** *Wenn in einer Reihe von Implikationen (Wenn – dann - Aussagen) $A_1 \Rightarrow B_1, \ldots, A_n \Rightarrow B_n$ die Voraussetzungen $A_1, \ldots, A_n$ alle möglichen Fälle erschöpfen, und wenn sich die Behauptungen $B_1, \ldots, B_n$ paarweise ausschließen, dann müssen auch die Umkehrungen $B_1 \Rightarrow A_1, \ldots, B_n \Rightarrow A_n$ gelten.*

Beweis. □

4. VL
01.11.05

1.4.9 Satz. *Sind $x, y \in N$ gegeben, dann liegt genau einer der Fälle vor:*

(i) $x = y$

(ii) Es gibt genau ein $u \in N$ mit $x = y + u$.

(iii) Es gibt genau ein $v \in N$ mit $y = x + v$.

Die Werte u, v sind eindeutig bestimmt.

Beweis. □

1.5 Teilerbeziehung und Division

1.5.1 Definition (Teiler)**.** *Seien $a, b \in N$. Dann heißt a Teiler von b (bzw. b ein Vielfaches von a), falls ein $c \in N$ existiert, so dass $ac = b$ ist. Schreibe dafür $a \mid b$.*

1.5.2 Folgerung. *Aus $a \mid b$ folgt stets $a \leq b$.*

1.5.3 Satz (Eigenschaften)**.** *(i) Wenn $a \mid b$, dann ist der Komplementärteiler c ($b = ac$) eindeutig bestimmt.*

(ii) Die Teilbarkeit in N ist eine partielle Ordnung, d.h. es gilt:

$$a \mid a$$
$$a \mid b \wedge b \mid a \Rightarrow a = b$$
$$a \mid b \mid c \Rightarrow a \mid c$$

Beweis. □

Aber $\mid$ ist (im Gegensatz zu $\leq$) keine Totalordnung (d.h. zu $a, b \in N$ gilt nicht immer $a \mid b$ oder $b \mid a$. Z.B. $b = a + 1$).

1.5.4 Folgerung. *Jedes $a \in N$ ist durch sich selbst und durch $\mathbb{1}$ teilbar.*

Definition (Primzahl)**.** *Elemente $p \neq \mathbb{1}$, welche keine weiteren (d.h. keine echten) Teiler haben, heißen Primzahlen.*

1.5.5 Satz. *Es sei $b \in N$, $b \neq \mathbb{1}$ und es sei a der kleinste Teiler von b verschieden von $\mathbb{1}$. Dann muss a eine Primzahl sein.*

Beweis. □

1.5.6 Folgerung. *(i) Wenn $b \neq \mathbb{1}$ keine Primzahl ist, dann hat der kleinste Teiler a von b die Eigenschaft $a^2 \leq b$.*

(ii) Eine Zahl $b \neq \mathbb{1}$, deren kleinster Teiler a die Eigenschaft $a^2 > b$ hat, muss Primzahl sein, d.h. $a = b$.

Beweis. □

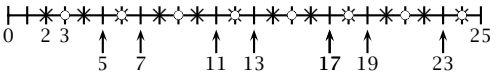
1.5.7 Satz (Das Sieb des Erathostenes)**.** *Es seien $p_1 = 2 < p_2 = 3 < \cdots < p_r$ die ersten p_r Primzahlen. Dann streichen man in der Zahlenfolge alle Primzahlen, welche durch mindestens eine dieser Primzahlen teilbar ist. Dann gilt:*

(i) die kleinste ($\neq \mathbb{1}$) der ungestrichenen Zahlen muss die nächstfolgende Primzahl p_{r+1} sein

(ii) alle ungestrichenen Zahlen a in dem Bereich $p_{r+1} \leq a \leq p_{(r+1)^2}$ sind Primzahlen.

Beweis. □

Beispiel. Wir streichen alle Vielfachen von 2 und 3. Die kleinste ungestrichene Zahl ist die nächste Primzahl 5. Und alle ungestrichenen Zahlen < 25 müssen Primzahlen sein.



Zwei berühmte Aussagen über Primzahlen:.

1. Der Primzahlsatz. Wir betrachten die Primzahl-Zählfunktion[3]:

$$\pi(x) = \#\{p \leq x : p \in \mathbb{P}\}$$

Dies ist eine Treppenfunktion. Wir betrachten zum Vergleich die stetige Funktion[4]:

$$\varphi(x) = \frac{x}{\log x}$$

[3] $\mathbb{P}$ ist die Menge der Primzahlen

[4] $\log x = \log_e x = \ln x$

Satz. $\varphi(x)$ *approximiert* $\pi(x)$*:* $\pi(x) \approx \varphi(x)$*, d.h.*

$$\lim_{x\to\infty} \frac{\pi(x)}{\varphi(x)} = 1$$

d.h. $\pi(x) = \varphi(x) + r(x)$*, mit einem Fehler* $r(x)$*. Dann ist* $\frac{\pi(x)}{\varphi(x)} = 1 + \frac{r(x)}{\varphi(x)}$ *und* $\frac{r(x)}{\varphi(x)} \overset{x\to\infty}{\longrightarrow} 0$*.*

Interpretation des Resultats. $\pi(x) \approx \varphi(x)$, d.h. für Zahlen der Größenordnung T, ist die Wahrscheinlichkeit eine Primzahl anzutreffen $\frac{1}{\log T}$. Aus $\log 10^n \approx n \cdot 2{,}3$ folgt: Für Zahlen mit n Dezimalstellen ist die Wahrscheinlichkeit eine Primzahl anzutreffen *ungefähr* $\approx \frac{1}{n\cdot 2{,}3}$

n	Zahlbereich	Wahrscheinlichkeit
1	1–9	$\frac{1}{2{,}3} \approx 43{,}5\%$
2	10–99	$\frac{1}{4{,}6} \approx 21{,}7\%$
3	100–999	$\frac{1}{6{,}9} \approx 14{,}5\%$
4	1000-9999	$\frac{1}{9{,}2} \approx 10{,}9\%$

Tabelle 2: Primzahlverteilung

2. Goldbach'sche Vermutung. Von Christian GOLDBACH (Petersburg) 1742 in einem Brief an Leonard EULER (Berlin) gestellte Vermutung: *Jede gerade Zahl $n \geq 4$ ist Summe von 2 Primzahlen.* Bis heute unbeantwortet.

$$4 = 2 + 2 \quad 6 = 3 + 3 \quad 8 = 3 + 5 \quad 10 = 5 + 5$$

Der chinesische Mathematiker J. CHEN bewies 1966:

Satz (Satz von Chen)*. Jede hinreichend große gerade Zahl n hat die Eigenschaft: $n = p + P_2$, wobei p eine Primzahl ist, und P_2 höchstens 2 Primfaktoren hat, d.h. P_2 ist entweder selber prim oder $P_2 = p_1 p_2$ ist Produkt zweier Primzahlen.*

1.5.8 Satz. *Seien $a, b \in N$ und es gelte $a \mid b$ sowie $a \mid c$. Dann folgt auch $a \mid (b + c)$ und im Fall $b > c$ folgt auch $a \mid (b - c)$.*

Beweis. Siehe Satz 1.4.8. □

1.5.9 Satz (Euklid)**.** *(ca. 300 v. Chr.) Es gibt unendlich viele Primzahlen.*

Beweis. □

Beweis Variante. □

1.5.10 Satz (Division mit Rest)**.** *Seien $a > n$ zwei Elemente aus N, und sei $n \nmid a$ (kein Teiler). Dann besitzt a eine eindeutige Darstellung:*

$$a = bn + r \text{ mit } r < n$$

Beweis. □

5. VL
07.11.05

Ergänzungen zum Wohlordnungssatz (1.3.8):

1.5.11 Satz. *Sein $M \subseteq N$ eine Teilmenge. Dann ist folgendes äquivalent:*

(i) M ist endlich

(ii) M besitzt ein größtes Element, welches eindeutig bestimmt ist.

Insbesondere ist jede beschränkte Teilmenge M endlich.

Beweis. Als Übung[5] 3.1. Der letzte Teil folgt aus 1.3.7. □

1.5.12 Definition (ggT)**.** *Sei $a, b \in N$. Sei*

$$T_{a,b} = \{n \in N : n \mid a \wedge n \mid b\}$$

die Menge der gemeinsamen Teiler. Die Menge ist offensichtlich beschränkt (z.B. $n \mid a \Rightarrow n \leq a$), also hat sie ein eindeutig bestimmtes größtes Element.

$$\mathrm{ggT}(a, b) := \max T_{a,b}$$

1.5.13 Satz. *Es sei $a = qb + r$ eine Relation in N. Dann gilt:*

$$T_{a,b} = T_{b,r} \Rightarrow \mathrm{ggT}(a, b) = \mathrm{ggT}(b, r)$$

1.5.14 Satz (Euklidischer Algorithmus)**.** *Seien $a, b \in N$, $a > b$. Wenn $b \mid a$, dann ist offensichtlich $\mathrm{ggT}(a, b) = b$. Anderenfalls bilde:*

$$\begin{aligned} a &= q_1 b + r_1 && \text{mit } r_1 < b =: r_0 \\ b &= q_2 r_1 + r_2 && \text{mit } r_2 < r_1 \\ &\dots \\ r_{i-1} &= q_{i+1} r_i + r_{i+1} && \text{mit } r_{i+1} < r_i \end{aligned}$$

solange bis $r_{i+1} \mid r_i$ (Ende des Algorithmus).

Behauptung: Dann ist $r_{i+1} = \mathrm{ggT}(a, b)$ und jedes Element aus $T_{a,b}$ teilt $\mathrm{ggT}(a, b)$.

Beweis. □

1.5.15 Ping-Pong-Methode. Abkürzung des Verfahrens mit der „Ping-Pong-Methode“: Sei $a > b$. Betrachte das Paar (a, b).

(i) Bilde a minus Vielfache von b, solange bis der 1. Eintrag $< b$ ist $\Rightarrow (r_1, b)$.

(ii) Bilde b minus Vielfache von r_1, solange bis der 2. Eintrag $< r_1$ ist $\Rightarrow (r_1, r_2)$.

(iii) Das Verfahren endet, sobald einer der beiden Einträge den anderen teilt.

Beispiel. $a = 138$ und $b = 38$:

(138, 38)	(24,38)	(24,14)
(10,14)	(10,4)	(2,4)

$2 \mid 4$, also ist $2 = \mathrm{ggT}(138,38)$.

1.5.16 Definition (kgV)**.** *Wir betrachten zu $a, b \in N$ die Menge*

$$V_{a,b} = \{n \in N : a \mid n \wedge b \mid n\}$$

Nach dem Wohlordnungssatz hat $V_{a,b}$ ein eindeutig bestimmtes kleinstes Element. Setzte:

$$\mathrm{kgV}(a, b) := \min V_{a,b}$$

1.5.17 Satz. *Jedes $n \in V_{a,b}$ ist durch $\mathrm{kgV}(a, b)$ teilbar (d.h. $\mathrm{kgV}(a, b)$ teilt alle Elemente aus $V_{a,b}$).*

Beweis. □

1.5.18 Satz. *Es gilt:*

$$\mathrm{kgV}(a, b) \cdot \mathrm{ggT}(a, b) = ab$$

Beweis. Als Übung 3.2a. □

Daraus folgt $\mathrm{kgV}(a, b) = \frac{ab}{\mathrm{ggT}(a,b)}$. Also erhalten wir mit dem $\mathrm{ggT}(a, b)$ auch den $\mathrm{kgV}(a, b)$.

1.6 Weiteres

1.6.1 Satz (Allgemeines Assoziativgesetz)**.** *Eine beliebig geklammerte Summe (bzw. beliebig geklammertes Produkt) von n Zahlen $a_1, \dots, a_n \in N$ liefert stets dasselbe Ergebnis.*

Beweis. □

[5] Übung 3.1 bedeutet Serie 3, Aufgabe 1. Die Übunden und ihre Musterlösungen finden sich unter `http://www.mathematik.hu-berlin.de/~zyska/UE-ELAlg-ZT.html`.

Potenzbildung

Idee. Fortgesetzte Multiplikation ein- und desselben Elements, sooft wie der Exponent dies angibt.

1.6.2 Definition (Potenz)**.** *Wir setzen für alle $a, b \in N$:*

$$a^{\mathbb{1}} = a$$
$$a^{b'} = a^b \cdot a$$

wobei $b' = \nu(b) = b + \mathbb{1}$ der Nachfolger von b ist.

Bemerkung. Die Potenzbildung ist weder assoziativ noch kommutativ. Z.B.:

$$2^{(2^3)} \neq \left(2^2\right)^3 \qquad 2^3 \neq 3^2$$

Jedoch gelten folgende Gesetze:

1.6.3 Satz (Rechengesetze)**.** *(i)* $(ab)^n = a^n b^n$

(ii) $a^{n \cdot m} = (a^n)^m$

(iii) $a^{n+m} = a^n \cdot a^m$

(iv) $(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i$
mit $\binom{n}{i} = \frac{n!}{i!(n-i)!}$.

2 Die ganzen Zahlen

Wir wollen ein Axiomensystem für die ganzen Zahlen angeben, die komplettierte Peano-Menge.

Heuristik. Warum (N, ν) und (Z, ν, ι)? Wir wollen erklären:

(i) Das Zählen war zuerst da.

(ii) Das Rechnen entwickelt sich natürlicher Weise aus dem Zählen

Die Algebra lässt das aus, indem sie einfach sagt: Z ist eine Menge mit zwei Operationen $+$ und $\cdot$, und diese Operationen haben „die und die“ Eigenschaften.

2.1 Komplettierte Peano-Mengen

2.1.1 Definition (Komplettierte Peano-Menge)**.** *Eine komplettierte Peano-Menge ist ein Tripel (Z, ν, ι) bestehend aus einer Menge Z und zwei Selbstabbildungen*

$$\nu : Z \to Z \qquad \iota : Z \to Z$$

so dass

(i) Beide Abbildungen sind Bijektionen und ι ist sogar Involution, d.h. $\iota^2 = \mathrm{id}_Z$, $\iota(\iota(x)) = x \forall\, x \in Z$, d.h. die Abbildung ist selbstinvers. Die Umkehrabbildung von ν bezeichnen wir mit μ.

(ii) Es existieren zwei äquivalente Relationen:

$$\iota \circ \nu \circ \iota = \nu^{-1} = \mu$$
$$\nu \circ \iota \circ \nu = \iota$$

(iii) Es gibt ein $\mathbb{0} \in Z$, $N \subset Z$ so dass

a) ν induziert eine Selbstabbildung $\nu : N \to N$ und das Paar (N, ν) ist Peano-Menge.

b) Z ist die disjunkte Vereinigung (Trichotomie)

$$Z = \iota(N) \dot\cup \{\mathbb{0}\} \dot\cup N$$

c) $\mathbb{0}$ ist kein Fixpunkt von ν, d.h $\nu(\mathbb{0}) \neq \mathbb{0}$

Heuristik. ν ist die Nachfolgeabbildung, μ ist die Vorgängerabbildung. ι ist der Übergang von x zu $-x$.

2.1.2 Folgerung (Einfache Folgerungen)**.** *(i) Die Äquivalenz (ii) im Satz ist echt. „Multipliziere“ von links mit ι, von rechts mit ν. Entsprechend kommt man auch wieder zurück:*

$$\iota \circ \mu = \nu \circ \iota$$

(ii) Der Vorgänger eines Elements aus $\iota(N)$ liegt wieder in $\iota(N)$

(iii) Es muss $\nu(\mathbb{0}) = \mathbb{1} \in N$ sein.

(iv) Die $\mathbb{0}$ ist bestimmt als der einzige Fixpunkt von ι.

(v) *N ist bestimmt als die Menge alles Nachfolger von $\mathbb{O}$.*

(vi) *Es ist stets $\nu(x) \neq x$.*

(vii) *Induktion für ganze Zahlen: Ist $M \subseteq Z$ Teilmenge, so dass*

a) $\mathbb{O} \in M$

b) *Wenn $x \in M$, dann ist $\nu(x)$ und $\iota(x) \in M$.*

Dann muss $M = Z$ sein.

Beweis. □

Bemerkung. Wichtig: Zur Definition von (Z, ν, ι) gehören die Existenz von N und $\mathbb{O}$. Wir brauchen sie aber nicht anzugeben, denn sie sind eindeutig bestimmt: $\mathbb{O}$ ist der einzige Fixpunkt von ι. N ist die Menge der Nachfolger von $\mathbb{O}$. Man nennt N auch den *Positivbereich* und $\iota(N)$ den *Negativbereich* von (Z, ν, ι).

6. VL 08.11.05

Bemerkung. Natürlich soll (Z, ν, ι) ein Modell für die ganzen Zahlen sein. Konkret ist dann:

$$\begin{aligned} \nu(x) &= x + 1 \\ \mu(x) &= x - 1 \\ \iota(x) &= -x \end{aligned}$$

Die Relation $\iota\nu\iota = \mu$ bzw. $\nu\iota\nu = \iota$ sind dann offensichtlich erfüllt.

Sie enthält außer der Möglichkeit des Weiterzählens auch noch die Möglichkeit zu jedem positiven Element spiegelbildlich ein negatives Element zu bilden. Das ist codiert in der Abbildung:

$$\iota(\iota(x)) = x \qquad \iota^2 = \mathrm{id}_Z \text{ Involution}$$

Die Verknüpfungen

$$\iota\nu\iota = \mu \qquad \nu\iota\nu = \iota$$

bedeuten konkret:

$$\begin{array}{ccc} x & \overset{\mu}{\longmapsto} & x-1 \\ {\scriptstyle\iota}\downarrow & \circlearrowleft & \uparrow{\scriptstyle\iota} \\ -x & \underset{\nu}{\longmapsto} & -x+1 \end{array} \qquad \begin{array}{ccc} x & \overset{\iota}{\longmapsto} & -x \\ {\scriptstyle\nu}\downarrow & \circlearrowleft & \uparrow{\scriptstyle\nu} \\ x+1 & \underset{\iota}{\longmapsto} & -x-1 \end{array}$$

2.1.3 Satz (Eindeutigkeit (bis auf Isomorphie))**.** *Es seien (Z, ν, ι) und (Z', ν', ι') zwei komplettierte Peano-Mengen. Dann gibt es genau eine Abbildung $f : Z \to Z'$ so dass*

$$\begin{aligned} f \circ \nu &= \nu' \circ f \\ f \circ \iota &= \iota' \circ f \end{aligned}$$

Genauso gibt es auch genau eine Abbildung $g : (Z', \nu', \iota') \to (Z, \nu, \iota)$ mit den entsprechenden Eigenschaften, und es folgt, dass f und g zueinander invers sind, d.h.

$$g \circ f = \mathrm{id}_Z \qquad f \cdot g = \mathrm{id}_{Z'}$$

$$\begin{array}{ccc} Z & \xrightarrow{f} & Z' \\ {\scriptstyle\nu,\iota}\downarrow & \circlearrowleft & \downarrow{\scriptstyle\nu',\iota'} \\ Z & \underset{f}{\longrightarrow} & Z' \end{array}$$

Beweis. □

Die komplettierte Peano-Menge ist die Grundlage, um Operationen einzuführen, die sich aus ν, ι ableiten.

2.1.4 Satz (Operationen auf Z)**.** *Es gibt genau eine Fortsetzung der beiden Operationen $+, \cdot$*

$$N \times N \xrightarrow{+,\cdot} N$$

zu Operationen

$$Z \times Z \xrightarrow{+,\cdot} Z$$

so dass folgendes gilt:

Ea) *die fortgesetzten Operationen sind ebenfalls assoziativ, kommutativ und erfüllen die Distributivgesetze.*

Eb) *für alle $z \in Z : z + \mathbb{O} = a$.*
(d.h. $\mathbb{O}$ erhält die Bedeutung von „Nichts“).

Ec) *für alle $a \in N : \iota(a) + a = \mathbb{O}$.*
(d.h. $\iota(a)$ erhält die Bedeutung $-a$.)

Beweis. □

Folgerung. *Es gilt:*

(i) $\forall z \in Z : i(z) + z = \mathbb{O}$

(ii) $\forall z \in Z : z \cdot \mathbb{0} = \mathbb{0}$

(iii) $\forall a, b \in Z : \iota(a) + \iota(b) = \iota(a + b)$

(iv) $\forall\, a, b \in N$*:* $a + \iota(b) = \begin{cases} a - b & : a > b \\ \iota(b - a) & : b > a \end{cases}$

(v) $\forall a, b \in N : a \cdot \iota(b) = \iota(ab)$

(vi) $\forall a, b \in N : \iota(a) \cdot \iota(b) = ab$

Damit haben wir für Addition und Multiplikation ein vollständiges Regelwerk. Wenn man Operationen $Z \times Z \xrightarrow{+,\cdot} Z$ mit Ea), Eb) und Ec) definieren will, dann hat man nur eine Möglichkeit.

2.1.5 Folgerung. *Wenn man die Operationen $Z \times Z \xrightarrow{+,\cdot} Z$ so ansetzt wie sie durch Ea), Eb) und Ec) erzwungen werden, dann folgt insbesondere*

$$\nu(x) = x + 1 \qquad \mu(x) = x + \iota(1)$$

für alle $x \in Z$.

Bemerkung (Translation der Zahlengeraden). Sei (Z, ν, ι) eine komplettierte Peano-Menge. Dann sind $\mathbb{0}$ = Fixpunkt von ι und $\mathbb{1} = \nu(\mathbb{0})$ eindeutig bestimmt. Aber die Bedeutung $\mathbb{0}, \mathbb{1}$ bekommen sie erst durch die Definition von Addition und Multiplikation. Ohne diese Operationen ist $(Z, \nu, \iota\nu^{-2n})$ ebenfalls komplettierte Peano-Menge mit dem Fixpunkt n, dem Positivbereich $n+N$ und dem Negativbereich $(\iota\nu^{-2n})(n+N) = n + \iota(N)$

$$Z = n + \iota(N) \dot\cup \{n\} \dot\cup\, n + N$$

Dies ist eine Translation der Zahlengeraden um n.

Wir benutzen jetzt die aus den Forderungen Ea), Eb) und Ec) abgeleiteten Formeln zur Definition einer Operation $Z \times Z \xrightarrow{+,\cdot} Z$. Dabei gehen wir davon aus, dass $a + b$, ab für $a, b \in N$ bereits definiert ist.

2.1.6 Definition $(+,\cdot)$**.** *Setze für alle $z \in Z$:*

$$z + \mathbb{0} := z \tag{Ai}$$

$$\mathbb{0} + z := z$$

$$z + \iota(z) := \mathbb{0} \tag{Aii}$$

Jetzt brauchen wir die weiteren Kombinationen für $a, b \in N$:

$$a + \iota(b) := \begin{cases} a - b & \text{falls } a > b \\ \iota(b - a) & \text{falls } b > a \end{cases} \tag{Aiii}$$

$$\iota(a) + b := \begin{cases} b - a & \text{falls } b > a \\ \iota(a - b) & \text{falls } a > b \end{cases} \tag{Aiv}$$

a, b seien immer in N. Dann ist $a \cdot b$ bereits definiert. Setze für alle $z \in Z$:

$$z \cdot \mathbb{0} := \mathbb{0} \cdot z := \mathbb{0} \tag{Mi}$$

$$\iota(a)b := \iota(ab) \tag{Mii}$$

$$a\iota(b) := \iota(ab) \tag{Miii}$$

$$\iota(a)\iota(b) := ab \tag{Miv}$$

Damit haben wir ein vollständiges Regelwerk von Operationen. Zu zeigen:

2.1.7 Satz. *Diese Definitionen ergeben zwei Operationen $Z \times Z \xrightarrow{+,\cdot} Z$ welche die erwarteten Eigenschaften Ea), Eb) und Ec) tatsächlich besitzen. Darüber hinaus gilt:*

$$z \cdot \mathbb{1} = \mathbb{1} \cdot z = z \quad \forall\, z \in Z$$

und, wenn $z, z' \in Z$ beide $\neq 0$ sind, dann ist auch

$$z \cdot z' \neq 0$$

Diese Eigenschaft nennt man Nullteilerfreiheit.

Beweis. □

2.2 Ordnung und Teilbarkeit

Als Vorbereitung zeigt man:

Lemma.

$$\iota(z) + \iota(z') = \iota(z + z')$$

gilt für alle $z, z' \in Z$.

Beweis. Nach Definition (Aiv) gilt das zunächst für $z, z' \in N$. □

Ordnung

2.2.1 Definition (Ordnung)**.** *Dann definieren wir* $\forall\, z, z' \in Z$*:*

$$z > z' :\Leftrightarrow z + \iota(z') \in N$$

bzw. entsprechend $z' < z$*.*

Folgerung (Trichotomie)**.** *Wegen der Trichotomie*

$$Z = \iota(N) \dot\cup \{\mathbb{0}\} \dot\cup N$$

gilt dann für alle $z, z' \in Z$ *genau einer der drei Fälle:*

$$z > z' \qquad z = z' \qquad z < z'$$

Beweis. □

Folgerung. *Setze* $z \geq z'$ *(bzw.* $z' \leq z$*) falls* $z > z'$ *oder* $z = z'$*. Dann ist* $\geq$ *eine Totalordnung auf* Z*.*

Beweis. □

Teilbarkeit

2.2.2 Definition und Satz (Teilbarkeit)**.** *Setze* $z \mid z'$ *für* $z, z' \in Z$*, falls ein* $x \in Z$ *existiert, so dass* $z' = zx$*. Insbesondere ist* $z' \neq 0$*, dann müssen* z, x *beide* $\neq 0$ *und* x *ist eindeutig bestimmt.* x *heißt Komplementärteiler von* z*.*

Beweis. □

Folgerung. *Offensichtlich gilt* $z \mid z$ *und die Transitivität:*

$$z_1 \mid z_2 \mid z_3 \Rightarrow z_1 \mid z_3$$

2.2.3 Satz. *Es gilt* $z \mid \mathbb{1}$ *genau dann wenn* $z = \mathbb{1}$ *oder* $z = \iota(\mathbb{1}) = -\mathbb{1}$*.*

Beweis. □

7. VL
14.11.05

Folgerung. *Eine Zahl* $x \in Z$ *teilt sämtliche Elemente in* Z *genau dann wenn* $x \mid \mathbb{1}$*, genau dann wenn* $x \in \{\mathbb{1}, \iota(\mathbb{1})\}$

Notation. Wir haben (Z, ν, ι) mit den Operationen $+, \cdot$. Ab jetzt benutzen wir die Bezeichnungen:

$$\begin{aligned} -x &\text{ statt } \iota(x) \\ x + 1 &\text{ statt } \nu(x) \\ x - 1 &\text{ statt } \mu(x) \\ -N &\text{ statt } \iota(N) \end{aligned}$$

Dies ist gerechtfertigt durch die Einführung der Operationen $+$ und $\cdot$ auf Z.

Der Absolutbetrag

2.2.4 Definition (Absolutbetrag)**.** *Der Absolutbetrag ist eine Abbildung*

$$Z \ni z \mapsto |z| \in N \dot\cup \{\mathbb{0}\}$$

und zwar

$$|z| = \begin{cases} 0 & \text{falls } z = 0 \\ z & \text{falls } z \in N \\ -z & \text{falls } z \in -N \end{cases}$$

Folgerung. *Die einzige Zahl mit Absolutbetrag* $\mathbb{0}$ *ist* $z = \mathbb{0}$*. Für* $a \in N$ *sind die einzigen Zahlen mit Absolutbetrag* $|z| = a$ *die Zahlen* $z = a$ *und* $z = -a$*.*

Beweis. □

2.2.5 Satz (Eigenschaften)**.** *(i)* $\forall\, x, y \in Z$ *:*

$$|xy| = |x| \cdot |y|$$

(ii) Sei $y \neq 0$*. Dann gilt:*

$$x \mid y \text{ in } Z \Leftrightarrow |x| \mid |y| \text{ in } N$$

(iii) Wenn $x \mid y$ *dann folgt* $|x| \leq |y|$

(iv) Insbesondere $x \mid y$ *und* $y \mid x \Leftrightarrow |x| = |y|$*, also* $x = \pm y$*.*

Beweis. Als Übung 4.3. □

Die Teilbarkeit in Z ist also nicht antisymmetrisch im eigentlichen Sinne. Zahlen, die sich nur mit Vorzeichen unterscheiden heißen *assoziiert*.

Der ggT und das kgV

2.2.6 Definition und Satz. *Seien* $x, y \in Z$ *und seien*

$$\begin{aligned} T_{x,y} &= \{z \in Z : z \mid x \text{ und } z \mid y\} \\ V_{x,y} &= \{z \in Z : x \mid z \text{ und } y \mid z\} \end{aligned}$$

die Menge der gemeinsamen Teiler und der gemeinsamen Vielfachen in Z. Dann gilt:

$$z \in T_{x,y} \Leftrightarrow |z| \in T^{(N)}_{|x|,|y|}$$
$$z \in V_{x,y} \Leftrightarrow |z| \in V^{(N)}_{|x|,|y|} \text{ oder } z = 0.$$

Wir setzen:

$$\mathrm{ggT}(a,b) := \mathrm{ggT}_N(|x|,|y|) \in N$$
$$\mathrm{kgV}(a,b) := \mathrm{kgV}_N(|x|,|y|) \in N$$

Dann haben sie die gleichen Eigenschaften wie zuvor der ggT *und* kgV *in N, nämlich:*

Jeder gemeinsame Teiler von x, y in Z teilt den ggT*, und jedes gemeinsame Vielfache von x, y ist durch* kgV *teilbar.*

Beweis. □

Man braucht hier nur den Absolutbetrag und die Division in N.

2.2.7 Folgerung (Lineardarstellung des ggT)**.** *Seien $a, b \in N$. Dann ist der* ggT(a,b) *linear aus a, b kombinierbar, d.h*

$$\mathrm{ggT}(a,b) = xa + yb$$

für geeignete $x, y \in Z$.

Beweis. □

Für $a, b \in Z$ statt $\in N$ gilt das auch:

Folgerung. ggT(a,b) *ist linear kombinierbar, weil* ggT$(a,b) =$ ggT$(|a|,|b|)$ *kombinierbar aus $|x|, |y|$.*

Eine Variante von 2.2.7:

2.2.8 Satz. *Sei $\mathfrak{I} \subset Z$ eine Teilmenge mit den Eigenschaften:*

(i) $x, y \in \mathfrak{I} \Rightarrow x + y \in \mathfrak{I}$

(ii) $x \in \mathfrak{I} \Rightarrow zx \in \mathfrak{I} \quad \forall\, z \in Z.$

(Zuvor war $\mathfrak{I} = M =$ alle Linearkombinationen von a, b.) Weiter sei $m \in N$ der kleinste Absolutbetrag ($\neq 0$) aller Elemente aus $\mathfrak{I}$.

Behauptung: Dann besteht $\mathfrak{I}$ genau aus allen ganzzahligen Vielfachen von m:

$$\mathfrak{I} = \{xm : x \in Z\} = Zm$$

Beweis. □

Linearkombination des ggT

Verfahren. Wir wollen den ggT(a,b) aus $a, b \in N$ linear kombinieren. *Bekannt:*

$$\begin{aligned} a &= q_1 b + r_1 && \text{mit } r_1 < b =: r_0 \\ b &= q_2 r_1 + r_2 && \text{mit } r_2 < r_1 \\ &\dots \\ r_{i-1} &= q_{i+1} r_i + r_{i+1} && \text{mit } r_{i+1} < r_i \end{aligned}$$

Rückrechnung ergibt r_{i+1} als Linearkombination von a und b.

Eine weitere Methode: OBdA sei $a > b$. Betrachte die Matrix

$$R = \left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) \in N^{2\times 2} \subset Z^{2\times 2}$$

Sie hat die Zeilen $z_1 = (a,b)$ und $z_2 = (0,1)$.

$$\begin{aligned} z_1 - bz_2 &= (a,b) - (0,b) = (a,0) \\ &= a(1,0) \end{aligned}$$

D.h. die Einträge der Zeile $z_1 - bz_2$ sind Vielfache von a. Sei jetzt $A \in Z^{2\times 2}$ 2×2-Matrix mit Koeffizienten in Z. Bilde das Matrix-Produkt RA. Für die Zeilen der Produkt-Matrix gilt:

$$z_1(RA) = z_1(R)A = z_1 \cdot A$$
$$z_2(RA) = z_2(R)A = z_2 \cdot A$$

Demzufolge

$$\begin{aligned} z_1(RA) - bz_2(RA) &= (z_1 - bz_2)A = a(1,0)A \\ &= az_1(A) \end{aligned}$$

Lemma. Für jede Matrix $A \in Z^{2\times 2}$ ist

$$z_1(RA) - bz_2(RA) = az_1(A)$$

das a-fache eines ganzzahligen Zeilenvektors, d.h. die Einträge der Zeile $z_1(RA) - bz_2(RA)$ sind beide durch a teilbar.

Aus der Linearen Algebra folgt: Die Anwendung elementarer Spaltenoperationen auf die Matrix $R = \left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)$, wobei jetzt nur Skalare in Z benutzt werden dürfen, bedeutet die Bildung von Matrizen RA mit $A \in Z^{2\times 2}$.

Folgerung. Bei Anwendung ganzzahliger Spaltenoperationen auf die Matrix $R = \left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)$ ergeben sich stets Matrizen M, so dass $z_1(M) - bz_2(M)$ das a-fache eines ganzzahligen Zahlenvektors ist, d.h. beide Einträge der Zeile $z_1(M) - bz_2(M)$ sind durch a teilbar.

Erweiterte Ping-Pong-Methode. Starte mit $R = \left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)$. Wende elementare Spaltenoperationen an, um die Größen von a und b zu reduzieren, solange bis ein Eintrag der ersten Zeile den anderen Eintrag teilt.

$$R \sim \begin{pmatrix} r_i & r_{i+1} \\ s_i & s_{i+1} \end{pmatrix} = M \text{ mit } r_{i+1} \mid r_i$$

Dann ist

$$r_{i+1} = \mathrm{ggT}(a,b)$$

und es gilt:

$$(r_i, r_{i+1}) - b(s_i, s_{i+1})$$

ist durch a teilbar. Insbesondere ist

$$r_{i+1} - bs_{i+1} = xa$$

Also:

$$\mathrm{ggT}(a,b) = r_{i+1} = xa + bs_{i+1}$$

wobei s_{i+1} der unter r_{i+1} stehende Eintrag der Matrix M ist, und

$$x = \frac{r_{i+1} - bs_{i+1}}{a}$$

Beispiel. Sei $a = 138$ und $b = 38$.

$$\begin{pmatrix} 138 & 38 \\ 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 24 & 38 \\ -3 & 1 \end{pmatrix} \sim \begin{pmatrix} 24 & 14 \\ -3 & 4 \end{pmatrix} \sim \begin{pmatrix} -4 & 14 \\ -11 & 4 \end{pmatrix} \sim \begin{pmatrix} -4 & 2 \\ -11 & -29 \end{pmatrix}$$

Wegen $2 \mid -4$ ist 2 der ggT.

$$2 - 38(-29) = 1104 = 8 \cdot 138$$

ist durch $a = 138$ teilbar. Also:

$$2 = (-29) \cdot 38 + 8 \cdot 138$$

Bemerkung. Dieses Verfahren ist wichtig für das ganzzahlige Lösen von Gleichungen

$$ax + by = c$$

Das Lösungsverfahren ist Thema der Übung 5.3.

Primfaktorzerlegung

2.2.9 Satz (Lemma von Euklid)**.** *Es seien $a, b \in N$ und p eine Primzahl mit $p \mid ab$. Dann gilt $p \mid a$ oder $p \mid b$.*

Beweis. □

Bemerkung. Es gilt auch die Umkehrung.

8. VL
15.11.05

2.2.10 Hauptsatz (der Arithmetik)**.** *Eindeutigkeit der Primfaktorzerlegung:*

(i) Jede natürliche Zahl $a \in N$ schreibt sich eindeutig (bis auf die Reihenfolge) als Produkt von Primzahlen.

(ii) Jede ganze Zahl $z \in Z$, $z \neq 0$, schreibt sich eindeutig (bis auf die Reihenfolge) in der Form

$$z = \varepsilon \cdot p_1^{\alpha_1} \cdots p_r^{\alpha_r}$$

mit $\varepsilon \in \{\pm 1\}$, Exponenten $\alpha_i > 0$ und $p_1, \ldots, p_r$ sind verschiedene Primzahlen. Dabei ist der Fall $r = 0$ zugelassen, und das leere Produkt ist definitionsgemäß gleich 1.

Beweis. □

Einführung des p-Exponenten

Als Folgerung betrachten wir den Begriff des p-Exponenten:

2.2.11 Definition (p-Exponent)**.** *Wir fixieren eine Primzahl p. Sei z eine ganze Zahl, $z \neq 0$. Dann setze*

$$\nu_p(z) = \begin{cases} 0 & \text{falls } p \nmid z \\ \max\{k \in N : p^k \mid z\} & \text{falls } p \mid z \\ \infty & \text{falls } z = 0 \end{cases}$$

Weil 0 durch jede Zahl, insbesondere durch jede Potenz von p teilbar ist.

Beispiel. Für $z = 18 = 2^1 \cdot 3^2$:

$$\nu_2(z) = 1 \quad \nu_3(z) = 2 \quad \nu_p(z) = 0 \text{ für } p \neq 2,3$$

Aus der Eindeutigkeit der Primfaktorzerlegung ergibt sich:

Folgerung. $\nu_p(z_1 z_2) = \nu_p(z_1) + \nu_p(z_2)$

und daraus folgendes Kriterium:

Folgerung (Kriterium). *Für ganze Zahlen gilt $z_1 \mid z_2$ genau dann, wenn $\nu_p(z_1) \le \nu_p(z_2)$ für alle Primzahlen p.*

Man erhält folgende Eigenschaften:

Folgerung (Eigenschaften).

$$\begin{aligned}
\nu_p(z_1 z_2) &= \nu_p(z_1) + \nu_p(z_2)\\
\nu_p(z_1 + z_2) &\ge \min\{\nu_p(z_1), \nu_p(z_2)\}\\
\nu_p\left(\mathrm{ggT}(z_1, z_2)\right) &= \min\{\nu_p(z_1), \nu_p(z_2)\}\\
\nu_p\left(\mathrm{kgV}(z_1, z_2)\right) &= \max\{\nu_p(z_1), \nu_p(z_2)\}\\
z_1 \mid z_2 &\Rightarrow \nu_p(z_1) \le \nu_p(z_2)\\
\forall\, p : \nu_p(z) = \nu_p(z') &\Leftrightarrow |z| = |z'|\\
\mathrm{ggT}(z_1, z_2) &= \prod_p p^{\min\{\nu_p(z_1), \nu_p(z_2)\}}\\
\mathrm{kgV}(z_1, z_2) &= \prod_p p^{\max\{\nu_p(z_1), \nu_p(z_2)\}}
\end{aligned}$$

Division mit Rest in (Z, ν, ι)

Nachtrag zur Division mit Rest in Z:

2.2.12 Satz (Division mit Rest). *Sei $x, y \in Z$. Dann gilt entweder $y \mid x$ oder es gibt eine Darstellung*

$$x = qy + r \qquad \text{mit } |r| < |y|$$

Beweis. □

Man braucht in Beweis nur den Absolutbetrag und die Division mit Rest in N.

Folgerung. *Seien $a, b \in N$. Dann ist* $\mathrm{ggT}(a, b)$ *linear aus a, b kombinierbar, d.h.*

$$\mathrm{ggT}(a, b) = xa + yb$$

für geeignete $x, y \in Z$.

Beweis. □

Nachtrag

Man betrachte dazu auch die Definition von $\mathbb{Z}m$ in 3.1.6. $\mathbb{Z}$ sei das uns geläufige Modell einer komplettierten Peano-Menge.

2.2.13 Satz (Ein Teilbarkeitskriterium). *In $\mathbb{Z}$ gilt*

$$a \mid b \Leftrightarrow \mathbb{Z}a \supseteq \mathbb{Z}b$$

Die Teilbarkeit wird mengentheoretisch ausgedrückt.

Beweis. □

2.2.14 Anwendung. Seien $b_1, \dots, b_n \in \mathbb{Z}$ gegeben. Dann ist a ein gemeinsamer Teiler aller b_i genau dann, wenn $\mathbb{Z}a \supseteq \mathbb{Z}b_1, \mathbb{Z}b_2, \dots, \mathbb{Z}b_n$ ist. b ist gemeinsames Vielfaches aller b_i genau dann, wenn $\mathbb{Z}b \subseteq \mathbb{Z}b_1, \dots, \mathbb{Z}b_n$.

Technik: Betrachte die Menge $\mathbb{Z}(\ni x, y)$ als $\mathbb{Z}$-Vektorraum ($\ni \alpha$): $\alpha \cdot x \in \mathbb{Z}$ und $x + y \in \mathbb{Z}$:

$$\begin{aligned}
\alpha = 1, \quad 1 \cdot x &= x\\
(\alpha + \beta)x &= \alpha x + \beta x\\
\alpha(x + y) &= \alpha x + \alpha y
\end{aligned}$$

Das Bild wird „schief“, weil man im Skalarbereich $\mathbb{Z}$ nicht uneingeschränkt dividieren kann. Ersetze den Begriff des $\mathbb{Z}$-Vektorraums durch den Begriff $\mathbb{Z}$-*Moduls*. Damit erhalten wir auch den Begriff des $\mathbb{Z}$-*Untermoduls* (entspricht Teilvektorraum).

Eine Teilmenge $\mathfrak{I}$ ist ein $\mathbb{Z}$-Untermodul (=: Ideal), wenn mit Elementen $x, y \in \mathfrak{I}$ auch alle Linearkombinationen $\lambda x + \mu y$ ($\lambda, \mu \in \mathbb{Z}$) wieder in $\mathfrak{I}$ liegen.

Offensichtliche Ideale von $\mathbb{Z}$ sind alle Teilmengen $\mathbb{Z}a$ (1-dimensionaler Untermodul, welcher vom „Vektor“ a erzeugt wird). Man nennt die Ideale $\mathbb{Z}a$ Hauptideale, weil sie nur von einem einzigen Element a erzeugt werden. In diesem Zusammenhang gilt 2.2.8. Jedes Ideal in $\mathbb{Z}$ ist vom Typ $\mathfrak{I} = \mathbb{Z}a$.

Sei $\mathfrak{I} = \mathbb{Z}a$. Dann ist a bis auf das Vorzeichen eindeutig bestimmt, d.h. $|a| = |b| \Rightarrow \mathfrak{I} = \mathbb{Z}a = \mathbb{Z}b$.

2.2.15 Satz (Mengentheoretische Charakterisierung des ggT und kgV). *Seien $b_1, \dots, b_n \in \mathbb{Z}$. Wir bilden die Ideale*

$$\begin{aligned}
\mathfrak{I} &= \mathbb{Z}b_1 + \cdots + \mathbb{Z}b_n =: \langle b_1, \dots, b_n \rangle\\
\mathfrak{J} &= \mathbb{Z}b_1 \cap \cdots \cap \mathbb{Z}b_n
\end{aligned}$$

als Spann bzw. Durchschnitt der Unterräume. Wir wissen: es gibt $r, s \in \mathbb{Z}$ (OBdA $r, s > 0$) mit

$$\begin{aligned}
\mathfrak{I} &= \mathbb{Z}r\\
\mathfrak{J} &= \mathbb{Z}s
\end{aligned}$$

Dann gilt:

$$r = \mathrm{ggT}(b_1, \ldots, b_n)$$
$$s = \mathrm{kgV}(b_1, \ldots, b_n)$$

Beweis. □

3 Gruppen und Ringe

3.1 Äquivalenzrelationen

3.1.1 Definition (Äquivalenzrelation)**.** *Gegeben sei eine Menge X. Eine Äquivalenzrelation auf X ist eine Relation*[6] *$\sim$, die zwischen gewissen Elementen von X besteht, und folgende Eigenschaften hat:*

(i) Reflexivität: $a \sim a$

(ii) Symmetrie: $a \sim b \Rightarrow b \sim a$

(iii) Transitivität: $a \sim b$ und $b \sim c \Rightarrow a \sim c$

3.1.2 Satz. *Gegeben sei die Relation $(X, \sim)$. Für $a, b \in X$ seien $[a], [b]$ die zugehörigen Äquivalenzklassen. Dann tritt genau einer der folgenden Fälle ein:*

(i) $[a] = [b]$, falls $a \sim b$

(ii) $[a] \cap [b] = \emptyset$, falls $a \not\sim b$

Beweis. Bemerkung: Wegen der Reflexivität ist stets $a \in [a]$. □

3.1.3 Definition. *Gegeben $(X, \sim)$ wie bisher. Dann bildet man eine neue Menge:*

$$X/\sim := \text{ Quotientenmenge von } X \text{ bezüglich } \sim$$

$X/\sim$ ist definiert als die Menge der Äquivalenzklassen.

$a \in X/\sim$ gibt keinen Sinn, jedoch $[a] \in X/\sim$!

Beispiel. Sei $f : X \to Y$ eine Abbildung. Dann gehört dazu auf X eine Relation „f-Äquivalenz“: $a \sim b$, falls $f(a) = f(b)$. Man sieht leicht, dass dies tatsächlich eine Äquivalenzrelation ist. Die Äquivalenzklassen $[a]$ bestehen in diesem Fall aus allen Elementen von X, welche unter f dasselbe Bild haben wie a.

X = Objektmenge $\xrightarrow{f}$ Y = Datenmenge. $[a]$ = Menge aller $x \in X$, zu denen dasselbe Datum gehört wie zu a, Z.B. Menge aller Personen mit demselben Geburtsdatum.

Betrachte die Abbildung $f : \mathbb{Z} \to \mathbb{N} \cup \{0\}, z \to f(z) = |z|$. Die Äquivalenzklassen sind die Zahlen mit demselben Absolutbetrag. Jede Äquivalenzklasse besteht aus zwei Elementen, bis auf eine Ausnahme: die Äquivalenzklasse $[0]$ besteht nur aus 0.

9. VL 21.11.05

3.1.4 Satz. *Sei $f : X \to Y$ eine beliebige Abbildung und sei $\sim$ die zugehörige Äquivalenzrelation auf X. Dann induziert f eine Bijektion*

$$f_* : X/\sim \longleftrightarrow \mathrm{im}(f)$$

zwischen der Quotientenmenge und dem Bild von f.

Beweis. □

3.1.5 Bemerkung (Äquivalenzrelationen und Partitionen)**.** Sei $(X, \sim)$ eine Äquivalenzrelation auf der Menge X. Dann wird dadurch eine Partition (Zerteilung) der Menge in paarweise disjunkte Teilmengen bestimmt, nämlich die Zerteilung in die verschiedenen Äquivalenzklassen.

Umgekehrt bestimmt jede Partition von X eine Äquivalenzrelation, nämlich ist $X = \dot{\bigcup}_{i \in J} X_i$ disjunkte Vereinigung, dann sage $a \sim b$ genau dann, wenn a und b sind Elemente derselben Teilmenge X_i.

Restklassen ganzer Zahlen $\mathbb{Z}$

$\mathbb{Z}$ sei das uns geläufige Modell einer komplettierten Peano-Menge.

3.1.6 Definition (Modul, modulo, Restklassen)**.** *Fixiere eine positive Zahl $m > 1$. Mann nennt m den Modul. Wir wollen $\mathbb{Z}$ zerteilen in Restklassen nach dem Modul m (modulo m).*

Sei z eine beliebige ganze Zahl. Schreibe

$$z = qm + r \quad \text{mit } 0 \le r < m$$

Dadurch ist der (nicht negative) Rest r eindeutig bestimmt. Nämlich betrachte alle nicht negativen Zahlen x von $x = z - qm$. r ist dann das

[6] Eine Relation R ist eine Teilmenge $R \subseteq X \times X$, also mit Elementen $(a, b) \in R$ $(a, b \in X)$. Man schreibt dann aRb, falls $(a, b) \in R$. Hier also: $a \sim b \Leftrightarrow (a, b) \in {\sim} \subseteq X \times X$.

eindeutig bestimmte kleinste Element unter allen solchen x.

Also erhalten wir eine wohl bestimmte Restabbildung (modulo m):

$$r : \mathbb{Z} \to \{0, 1, \dots, m-1\}$$
$$z \mapsto r(z), z = qm + r(z)$$

Die Abbildung r induziert auf $\mathbb{Z}$ eine Äquivalenzrelation, nämlich

$$z_1 \sim z_2 \quad \Leftrightarrow r(z_1) = r(z_2)$$

Diese Äquivalenzklassen nennt man Restklassen modulo m.

Beispiel. Modul $m = 3$. Die Restklassen sind $[0], [1]$ und $[2]$:

$$[0] = \{\dots, -6, -3, 0, 3, 6, 9, \dots\}$$
$$[1] = \{\dots, -5, -2, 1, 4, 7, 10, \dots\}$$
$$[2] = \{\dots, -4, -1, 2, 5, 8, 11, \dots\}$$

Notation. Sprechweise für diese Äquivalenzrelation:

z_1 ist kongruent zu z_2 modulo m.

Schreibweise:

$$z_1 \equiv z_2 \mod m$$

Eine Variante, um diese Kongruenz auszudrücken:

Lemma. *Es gilt $z_1 \equiv z_2 \mod m$ genau dann, wenn $z_1 - z_2$ durch m teilbar ist.*

Beweis. □

Folgerung. *Die Äquivalenzklasse von $a \in \mathbb{Z}$ ist demzufolge*

$$[a] = [a]_m = \{a + qm | q \in \mathbb{Z}\}$$
$$= a + \mathbb{Z}m = a + [0]$$

Also alle Zahlen, die sich von a um ein Vielfaches von m unterscheiden. Dabei ist $\mathbb{Z}m = \{qm | q \in \mathbb{Z}\}$ die Menge aller Vielfachen von m.

Beispiel. $[0] = \mathbb{Z}3, [1] = 1 + \mathbb{Z}3 = 1 + [0]$ und $[2] = 2 + \mathbb{Z}3 = 2 + [0]$

3.2 Das Rechnen mit Restklassen

Sei $m > 1$ im folgenden ein fixierter Modul.

Notation. $\mathbb{Z}/m\mathbb{Z}$ bezeichnet die Menge der Restklassen modulo $m = \mathbb{Z}/\sim$ (Quotientenmenge), wobei $a \sim b \Leftrightarrow r(a) = r(b) \Leftrightarrow m \mid (a - b)$.

Ziel. Wir wollen auf $\mathbb{Z}/m\mathbb{Z}$ eine Addition und eine Multiplikation einführen. Schwierigkeit: $\mathbb{Z}/m\mathbb{Z}$ besteht nicht aus einzelnen Elementen, sondern aus Äquivalenzklassen, also Mengen.

Vorschlag:

3.2.1 Definition. *Sind $[a], [b] \in \mathbb{Z}/m\mathbb{Z}$, dann definiere:*

$$[a] + [b] := [a + b]$$
$$[a] \cdot [b] := [a \cdot b]$$

3.2.2 Lemma. *Die Definition ist repräsentantenunabhängig, d.h. ist $[a] = [a']$ und $[b] = [b']$, dann ist*

$$[a] + [b] = [a'] + [b']$$
$$[a] \cdot [b] = [a'] \cdot [b']$$

Beweis. □

Beispiel. Modul $m = 10$. Addition:

$$[9] + [3] = [19] + [23]$$
$$[12] = [42]$$

Wenn man durch 10 teilt, erhält man denselben Rest. Multiplikation:

$$[9] \cdot [3] = [19] \cdot [23]$$
$$[27] = [437]$$
$$[7] = [7]$$

10. VL 22.11.05

3.2.3 Lemma. *Alle üblichen Rechenregeln vererben sich von $\mathbb{Z}$ auf $\mathbb{Z}/m\mathbb{Z}$. Die neutralen Elemente bezüglich Addition und Multiplikation sind $[0]$ und $[1]$.*

Beweis. □

3.2.4 Unterschiede im Vergleich zu $\mathbb{Z}$.

(i) $\mathbb{Z}/m\mathbb{Z}$ ist als Menge *endlich*

(ii) In $\mathbb{Z}/m\mathbb{Z}$ kann es so genannte Nullteiler geben, d.h. finde $[a], [b]$, beide $\neq [0]$, aber $[a][b] = [0]$.

Beispiel: $\mathbb{Z}/10\mathbb{Z} \ni [2], [5]$.

$$[2] \cdot [5] = [10] = [0]$$

(iii) In $\mathbb{Z}/mZ$ gibt es im Allgemeinen viele Teiler der $[1]$. $[a][b] = [1]$ bedeutet, dass $[a]$ und $[b]$ in $\mathbb{Z}/m\mathbb{Z}$ zueinander invers sind.

3.2.5 Satz. *Die Klasse $[a] \in \mathbb{Z}/m\mathbb{Z}$ ist Teiler von $[1]$ genau dann, wenn $\mathrm{ggT}(a, m) = 1$ ist. Diese Bedingung hängt nur von der Restklasse $[a]$ ab, aber nicht von dem speziellen Repräsentanten a.*

Beweis. □

Definition (prim, Einheit)**.** *Wenn $\mathrm{ggT}(a, m) = 1$ ist, dann nennt man $[a]$ eine prime Restklasse modulo m. Man nennt die Teiler der $[1]$ auch Einheiten (in $\mathbb{Z}/m\mathbb{Z}$).*

Sei $[a]$ prime Restklasse in $\mathbb{Z}/m\mathbb{Z}$. Wie berechnet man $[a]^{-1}$?

3.2.6 Methode. Bilde $\left(\begin{smallmatrix} m & a \\ 0 & 1 \end{smallmatrix}\right)$, und wende hierauf (ganzzahlige) elementare Spaltenoperationen an, und erreiche irgendeine Matrix $\left(\begin{smallmatrix} x & y \\ u_x & u_y \end{smallmatrix}\right)$. Dann gilt immer

$$x \equiv u_x \cdot a \mod m$$

Wenn $\mathrm{ggT}(a, m) = 1$, dann finden wir schließlich eine Matrix, bei der $x = 1$ ist (bzw. $y = 1$). D.h.

$$\begin{aligned} 1 &\equiv u_x a \mod m \\ [1] &\equiv [u_x][a] \mod m \end{aligned}$$

Also $[u_x]$ ist invers zu $[a]$ (modulo m), $a^{-1} \equiv u_x \mod m$.

Variante: Man endet mit $x = -1$

$$\begin{aligned} -1 &\equiv u_x a \mod m \\ 1 &\equiv (-u_x) a \mod m \end{aligned}$$

In diesem Fall wäre $[-u_x]$ invers zu $[a]$.

Man vergleiche dazu auch die Erweiterte Ping-Pong-Methode in 2.2, Seite 15.

Beispiel. Modul $m = 53$, $[a] = [8]$.

$$\begin{pmatrix} 53 & 8 \\ 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 5 & 8 \\ -6 & 1 \end{pmatrix} \sim \begin{pmatrix} 5 & -2 \\ -6 & 13 \end{pmatrix} \sim \begin{pmatrix} 1 & -2 \\ 20 & 13 \end{pmatrix}$$

Also ist $8^{-1} \equiv 20 \mod m$.

Eulersche ϕ-Funktion

Ziel. Wie viele Einheiten (d.h. prime Restklassen) gibt es in $\mathbb{Z}/m\mathbb{Z}$? Die Eulersche Funktion $\phi(m)$ ist genau diese Zahl.

Über die Bedeutung der Funktion $\phi(m)$:

Einschub über Gruppen

Definition. *Eine Gruppe G ist eine Menge versehen mit einer Operation*

$$G \times G \dot{\to} G$$

welche folgende Eigenschaften hat:

(i) Assoziativität: $(xy)z = x(yz)$

(ii) Es gibt ein neutrales Element $\mathbb{1}$*:*

$$\forall x \in G : x \cdot \mathbb{1} = \mathbb{1} \cdot x = x$$

(iii) Es gibt zu jedem $x \in G$ ein Inverses x^{-1}, so dass

$$x^{-1} \cdot x = x \cdot x^{-1} = 1$$

Man nennt G kommutativ oder abelsch[7]*, falls stets $xy = yx$ ist.*

Bemerkung. (i) $\mathbb{1}$ ist eindeutig bestimmt

(ii) x^{-1} ist eindeutig bestimmt

(iii) Man darf kürzen:

$$\begin{aligned} xz = yz \quad &\Rightarrow \quad x = y \\ zx = zy \quad &\Rightarrow \quad x = y \end{aligned}$$

(indem man mit z^{-1} multipliziert)

[7] Niels Henrik Abel, norwegischer Mathematiker, 1802-1829. Er war ein wichtiger Mitbegründer der Gruppentheorie.

Satz. *Sei G eine Gruppe, sei $g \in G$ ein fixiertes Element. Dann ist die Selbstabbildung $G \ni x \mapsto xg \in G$ stets bijektiv.*

Beweis. □

Folgerung. *Es sei G eine kommutative Gruppe mit n Elementen (endlich). Dann gilt für jedes $g \in G : g^n = 1$.*

Beweis. □

Betrachte jetzt wieder $\mathbb{Z}/m\mathbb{Z}$.

Lemma. *Die Einheiten in $\mathbb{Z}/m\mathbb{Z}$ bilden eine multiplikative Gruppe.*

3.2.7 Fazit. Die Menge $(\mathbb{Z}/m\mathbb{Z})^\times$ der primen Restklassen bildet bezüglich der Multiplikation eine Gruppe. $\phi(m)$ ist die Ordnung dieser Gruppe. Deshalb gilt für jede prime Restklasse $[a]$:

$$[a]^{\phi(m)} = [1]$$

D.h. wenn $\mathrm{ggT}(a, m) = 1$

$$a^{\phi(m)} \equiv 1 \mod m$$

Explizite Bestimmung von $\phi(m)$

3.2.8 Satz. *Es sei $m = p^n$ Potenz einer Primzahl. Dann gilt:*

$$\phi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$$

Beweis. □

3.2.9 Satz (Chinesischer Restsatz)**.** *Es seien $m_1, \ldots, m_n$ Zahlen ≥ 2 mit*

$$\mathrm{ggT}(m_i, m_j) = 1 \qquad 1 \leq i \neq j \leq n$$

Weiter seien $a_1, \ldots, a_n$ beliebige ganze Zahlen. Dann ist die simultane Kongruenz

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2 \\ &\ldots \\ x &\equiv a_n \mod m_n \end{aligned}$$

immer lösbar und es gibt eine eindeutig bestimmte Lösung mit der Eigenschaft: $0 \leq x < m_1 m_2 \cdots m_n$.

Beweis. □

Bemerkung. Man kann diesen Satz auch als einen Isomorphiesatz für Ringe formulieren. Dazu vergleiche 3.6.6 bis 3.6.8 sowie Übung 8.5.

Folgerung. *Man findet für die simultane Kongruenz auch eine eindeutig bestimmte Lösung $x \in \mathbb{Z}$ mit $|x| \leq \frac{1}{2} m_1 \cdots m_n$.*

Beweis. □

3.2.10 Satz (Anwendung)**.** *Sei* $\mathrm{ggT}(m, n) = 1$. *Betrachte zwei Mengen:*

$$A = \{a \in \mathbb{Z} : 1 \leq a < mn \text{ mit } \mathrm{ggT}(a, mn) = 1\}$$
$$B = \{(b, c) \in \mathbb{Z}^2 : 1 \leq b < m, 1 \leq c < n\}$$

Es ist $\#A = \phi(mn)$ und $\#B = \phi(m)\phi(m)$. Behauptung: $\#A = \#B$.

Beweis. Durch Anwendung von 3.2.9 für $m_1 = m, a_1 = b$ sowie $m_2 = n, a_2 = c$. □

Folgerung. *Es gilt also $\phi(mn) = \phi(m)\phi(n)$, falls* $\mathrm{ggT}(m, n) = 1$.

Public Key Cryptography

Nach dem RSA-Code (1978 von RIVEST, SHAMIR und ADLEMAN).

Problem. Eine Person P will verschlüsselte Nachrichten empfangen mit folgenden Randbedingungen:

(i) Methode der Verschlüsselung einer Nachricht ist öffentlich

(ii) Die Entschlüsselung soll nur für P selbst möglich sein.

Wahl. Dazu trifft P folgende Wahlen:

(i) Wahl eines Kodierungsmoduls m. D.h. alle Rechnungen spielen sich in der primen Restklassengruppe $(\mathbb{Z}/m\mathbb{Z})^\times$ ab.

(ii) Eine Folge $A, B, C, \ldots, Z \in (\mathbb{Z}/m\mathbb{Z})^\times$, welche die Buchstaben repräsentieren.

(iii) Einen Kodierungsexponenten t.

Diese Daten werden veröffentlicht.

Zusatzanforderungen. Modul $m = p \cdot q$ ist Produkt zweier (verschiedener) Primzahlen. t soll prim sein zu $\phi(m) = (p-1)(q-1)$.

Geheimhaltung. Zerlegung $m = p \cdot q$ ist geheim! Damit ist auch $\phi(m)$ geheim. Geheim ist damit auch der „Dekodierungsexponent“ u mit der Eigenschaft:

$$t \cdot u \equiv 1 \mod \phi(m)$$
$$[u]_{\phi(m)} = [t]^{-1}_{\phi(m)}$$

Nachrichtenübermittlung. Wie funktioniert die Nachrichtenübermittlung? Sei X ein Buchstabe.

$$\begin{array}{ccc} (\mathbb{Z}/m\mathbb{Z})^\times \ni X & \xmapsto{\text{kodieren}} & x := X^t \in (\mathbb{Z}/m\mathbb{Z})^\times \\ & & \Big\downarrow \text{sende} \\ X = x^u \mod m & \xleftarrow[\text{dekodieren}]{} & x \in (\mathbb{Z}/m\mathbb{Z})^\times \end{array}$$

Denn $x^u \equiv (X^t)^u \mod m$ und $tu = 1 + q \cdot \phi(m)$. Also:

$$X^{tu} = X^{1+q\cdot\phi(m)} \equiv X \mod m$$

weil $X^{\phi(m)} \equiv 1 \mod m$.

Beispiel. Alles was in Klammern steht bleibt geheim:

(i) $m = 1763$ $(= 41 \cdot 43)$

(ii) $A = 11, B = 12, \ldots, Z = 36 \mod 1763$

(iii) $t = 11$ (ist prim zu $\phi(m) = (p-1)(q-1) = 40 \cdot 43 = 1680$)

(iv) (Der Dekodierungsexponent u:

$$[u]_{1680} = [t]^{-1}_{1680} = [11]^{-1}_{1680} = [611]_{1680}$$

Also $u = 611$.)

Verfahren: Schreibe t, u in 2-adischer Entwicklung:

$$t = 11 = 2^3 + 2 + 1$$
$$u = 611 = 2^9 + 2^6 + 2^5 + 2 + 1$$

Wir wollen $B = 12$ verschlüsseln. Dazu bilde:

$$B^{11} \equiv B^{2^3} \cdot B^2 \cdot B \in \mathbb{Z}/1763\mathbb{Z} \mod 1763$$

$B = 12$ drei mal quadrieren:

$$B^2 = 144$$
$$B^{2^2} \equiv 144^2 \equiv -420 \mod 1763$$
$$B^{2^3} \equiv (-420)^2 \equiv 100 \mod 1763$$

Also:

$$B^{11} \equiv 100 \cdot 144 \cdot 12 \equiv 26 \mod 1763$$

Sende $b = B^{11} \equiv 26 \mod 1763$. Zum dekodieren berechne

$$b^{611} \equiv b^{2^9} \cdot b^{2^6} \cdot b^{2^5} \cdot b^2 \cdot b \mod 1763$$

und finde

$$26^{611} \equiv 12 \mod 1763$$

Je größer die beteiligten Faktoren p, q sind, um so sicherer ist der Code (und umso langsamer).

3.3 Ringe

Wir haben bisher $\mathbb{Z}$ und $\mathbb{Z}/m\mathbb{Z}$ betrachtet. Dies sind Ringe:

3.3.1 Definition (Ring)**.** *Ein Ring ist eine Menge mit Operationen:*

$$R \times R \xrightarrow{+} R \qquad (a,b) \mapsto a + b \in R$$
$$R \times R \xrightarrow{\cdot} R \qquad (a,b) \mapsto a \cdot b \in R$$

mit folgenden Eigenschaften:

(i) $(R, +)$ *soll eine kommutative Gruppe sein, mit neutralem Element* 0 *und inversem Element* $-x$*.*

(ii) Multiplikation soll assoziativ sein:

$$(ab)c = a(bc)$$

(iii) Es gelten die Distributivgesetze:

$$(a+b)c = ac + bc$$
$$a(b+c) = ab + ac$$

Mögliche Zusatzanforderungen:

(i) Ring soll ein Einselement 1_R haben (Ring mit 1), d.h.

$$\forall x \in R : x \cdot 1_R = 1_R \cdot x = x$$

(ii) Kommutativer Ring: $ab = ba \forall a, b \in R$

(iii) Nullteilerfreier Ring: $ab = 0 \Rightarrow a = 0$ oder $b = 0$. Im nullteilerfreien Ring kann man kürzen.

(iv) Der Ring R heißt Körper, falls er kommutativ mit 1 ist, und jedes $r \neq 0 \in R$ ein multiplikatives Invers hat. Insbesondere ist ein Körper nullteilerfrei.

Folgerung. *(i) R habe eine 1. Dann ist die 1 eindeutig bestimmt.*

(ii) Entsprechend ist die 0 eindeutig bestimmt.

Beweis. □

3.3.2 Beispiele. (i) $R = \mathbb{Z}$, kommutativer Ring mit 1 und nullteilerfrei.

(ii) $R = \mathbb{Z}/m\mathbb{Z}$, Restklassenringe, kommutativ mit 1, i.A. existieren Nullteiler

(iii) $R = \mathbb{Z}/p\mathbb{Z}$, mit p Primzahl, ist ein Körper. Alle Restklassen außer $[0]$ sind prime Restklassen, und damit Teiler der $[1]$. $\phi(p) = p - 1$.

(iv) Nicht kommutative Ringe: Sei K ein Körper. Sei $K^{n\times n} = R$ die $n \times n$-Matrizen. In R haben wir Addition und Multiplikation von Matrizen. Die Multiplikation ist nicht kommutativ. Einselement ist $1_R = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$. R hat wieder Nullteiler: $n = 2 : \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$.

11. VL 29.11.05

3.3.3 Lemma (Einfachste Rechenregeln)**.**

(i) $0 \cdot a = a \cdot 0 = 0$

(ii) $a(-b) = (-a)b = -(ab)$

(iii) $(-a)(-b) = ab$

(iv) Wenn 1_R existiert, dann ist es eindeutig, und es gilt: $(-1)a = -a$ und $(-1)(-1) = 1$.

Beweis. □

3.3.4 Definition und Satz (Einheiten eines Rings mit 1)**.** *$r \in R$ heißt Einheit, falls r ein Teiler der 1 ist, d.h. es existiert $s \in R$:*

$$sr = rs = 1$$

Die zu r „komplementäre" Einheit s ist dann eindeutig bestimmt.

Beweis. □

Satz. *Die Einheiten $R^\times$ eines Ringes R bilden bezüglich der Multiplikation eine Gruppe.*

3.3.5 Beispiele. (i) $R = \mathbb{Z}$, $\mathbb{Z}^\times = \{1, -1\}$

(ii) $R = \mathbb{Z}/m\mathbb{Z}$, $(\mathbb{Z}/m\mathbb{Z})^\times = \{[a] : \mathrm{ggT}(a, m) = 1\}$ = Gruppe der primen Restklassen.

Eulersche ϕ-Funktion:

$$\phi(m) := \#(\mathbb{Z}/m\mathbb{Z})^\times$$

Formel für $m = p_1^{a_1} \cdots p_r^{a_r}$:

$$\phi(m) = p_1^{a_1-1}(p_1 - 1) \cdots p_r^{a_r-1}(p_r - 1)$$

und

$$\frac{\phi(m)}{m} = \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$

„ist der Prozentsatz der Restklassen, welche prim sind."

(iii) $R = K[X]$ Polynome mit Koeffizienten in einem Körper K.

Bemerkung. In der Algebra wird die nicht als Menge von Funktionen gesehen, sondern rein formal betrachtet. D.h.: Betrachte R als K-Vektorraum mit der Basis $X^0 = 1, X, X^2, X^3, \ldots$.

Es ist dann

$$\sum a_i X^i = \sum b_i X^i \quad \Leftrightarrow \quad a_i = b_i$$

Die Addition ist komponentenweise definiert. Wir müssen rein formal eine Multiplikation erklären:

$$\left(\sum a_i X^i\right) \cdot \left(\sum b_j X^j\right) := \sum c_k X^k$$
$$c_k := \sum_{i+j=k} a_i b_j$$

$R = K[X]$ mit den angegebenen Operationen ist ein Ring. R ist kommutativ:

$$a_i X^i \cdot b_j X^j = a_i b_j X^{i+j}$$

weil K kommutativ ist.

Einheiten in K[X]:

a) Einheiten in einem Körper K:

$$K^\times = K \setminus \{0\}$$

b) $K[X] \ni 1$. Die Einheit ist definiert als das konstante Polynom

$$1 = 1_K \cdot X^0$$

Der Grad:

$$\deg(\sum a_i X^i) := \max\{i, a_i \neq 0\}$$

Sind a, b zwei Polynome, dann gilt:

$$\deg(a \cdot b) = \deg(a) + \deg(b)$$

Jedoch $\deg(1) = 0$.

Ergebnis. $K[X]^\times = K^\times$. Alle konstanten Polynome $\neq 0$.

(iv) Einheiten im Matrizenring $K^{n\times n}$ ($n \times n$ Format, Einträge in K) sind genau die invertierbaren Matrizen $A \Leftrightarrow \det(A) \neq 0$.

$$\mathrm{GL}_n(K) := (K^{n\times n})^\times$$

3.3.6 Definition (Potenz)**.** *Sei R ein Ring mit 1. Die Potenzen eines Ringelements $r \in R$ werden rekursiv definiert:*

$$r^0 := 1_R \qquad n \in \mathbb{N} : r^n := \prod_{i=1}^{n} r = \underbrace{r \cdot \cdots \cdot r}_{n\text{-mal}}$$

Wenn $n < 0$, dann ist r^n nur definiert, falls r eine Einheit ist:

$$r^n := (r^{-1})^{-n}$$

Eine Charakterisierung der ganzen Zahlen von Standpunkt der Ringtheorie

Bisher hatten wir: die komplettierte Peano-Menge $(\mathbb{Z}, \nu, \iota)$ ist ein Ring. Jetzt wollen wir eine Charakterisierung von $\mathbb{Z}$ als Ring.

Bisher:	$(\mathbb{Z}, \nu, \iota)$	$\Rightarrow$	R
Jetzt:	$\mathbb{Z}$	$\Leftarrow$	R

3.3.7 Definition (geordnet)**.** *Ein Ring heißt geordnet, falls es in R einen Positivbereich R_+ gibt, so dass:*

(Pi) $a, b \in R_+ \Rightarrow a + b, a \cdot b \in R_+$.

(Pii) Für beliebige $a \in R$ ist genau eine der Eigenschaften $a \in R_+$, $a = 0$ oder $-a \in R_+$ erfüllt

$$R = R_+ \dot\cup \{0\} \dot\cup -R_+ \qquad \text{(Trichotomie)}$$

3.3.8 Folgerung. *Ein geordneter Ring hat folgende Eigenschaften:*

(i) $a \neq 0 \Rightarrow a^2 \in R_+$

(ii) R ist nullteilerfrei

(iii) Es kann niemals ein Vielfaches der 1_R gleich 0 werden.

Beweis. □

Beispiele (für (iii)). $\mathbb{Z}/m\mathbb{Z} \in [1], m[1] = \sum_{i=1}^{m}[1] = [m] = [0]$. Das gilt insbesondere für $\mathbb{Z}/p\mathbb{Z}$, wenn p eine Primzahl ist: $p[1] = [0]$. Andererseits ist $\mathbb{Z}/p\mathbb{Z}$ ein Körper, weil

$$(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{Z}/p\mathbb{Z} \setminus \{0\} \quad 0 \cdot 1 \equiv p \cdot 1 \equiv 0 \mod p$$

und trotzdem nullteilerfrei.

Die Bezeichnung geordneter Ring wird gerechtfertigt durch die

3.3.9 Definition (Ordnung)**.** *Einführung einer Ordnung:*

$$a > b : \Leftrightarrow a - b \in R_+$$

Für $a \neq 0$ ist $a^2 > 0$. $a \geq b$ ist Totalordnung auf R (benutze Trichotomie).

3.3.10 Definition (Wohlordnung)**.** *Ein geordneter Ring heißt wohlgeordnet, falls jede nichtleere Teilmenge $M \subseteq R_+$ ein kleinstes Element hat.*

3.3.11 Satz. *(Charakterisierung von $\mathbb{Z}$) Bis auf Isomorphie ist $\mathbb{Z}$ der einzige wohlgeordnete Ring mit 1.*

Beweis. □

3.4 Teilbarkeit in Integritätsbereichen

Ziel. Formalisierung der Teilbarkeitslehre, welches sind die allgemeinsten Bedingungen, unter denen der Hauptsatz der Arithmetik (Eindeutigkeit der Primfaktorzerlegung) gilt.

3.4.1 Definition. *Ein Ring R heißt Integritätsbereich (oder Integritätsring), falls*

(i) R ist kommutativer Ring mit $1_R \neq 0_R$.

(ii) R hat keine Nullteiler.

Wäre $1_R = 0_R$, dann $x = 1 \cdot x = 0 \cdot x = 0 \Rightarrow R = \{0\}$. Kein Nullteiler bedeutet, dass man kürzen darf.

3.4.2 Definition (Teiler, echte, Assoziierte)**.** *Für $a, b \in R$ sage $a \mid b$, falls ein $c \in R$ existiert mit $b = ca$. c heißt Komplementärteiler.*

Wenn $b \neq 0$, dann ist der Komplementärteiler eindeutig bestimmt, da man kürzen darf.

Sage $a \mid b$ echt, *falls $b \nmid a$.*

Wenn $a \mid b$ und $b \mid a$, dann nennt man a und b assoziiert. Dies ist eine Äquivalenzrelation. Schreibe $a \sim b$.

12. VL
05.12.05

3.4.3 Satz (Mengentheoretische Charakterisierung der Teilbarkeit)**.** *Es gilt $a \mid b$ genau dann, wenn $Ra \supseteq Rb$. (Die Menge der Vielfachen von a enthält die Menge der Vielfachen von b.)*

Beweis. □

3.4.4 Folgerung. *Für Elemente $a, b \in R$ ist folgendes äquivalent:*

(i) $a \sim b$, d.h. $a \mid b$ und $b \mid a$

(ii) $Ra = Rb$

(iii) Es existiert eine Einheit $\varepsilon \in R^\times : b = \varepsilon a$.

Beweis. □

Bemerkung. Sei $a \mid b$. Wir nennen a einen *echten Teiler* von b, falls

(i) $b \nmid a$

(ii) a ist keine Einheit

Das bedeutet mengentheoretisch:

$$R \supset Ra \supset Rb \text{ mit echten Inklusionen}$$

$R = Ra$ würde bedeuten: a ist Einheit. $Ra = Rb$ würde bedeuten: a und b teilen sich gegenseitig.

3.4.5 Definition (irreduzibel, Primelement)**.** *Sei $a \in R$ keine Einheit, d.h. $R \neq Ra$.*

(i) a heißt irreduzibel, falls a keine echten Teiler hat.

(ii) a heißt Primelement, falls aus einer Teilbarkeitsbeziehung $a \mid bc$ stets folgt $a \mid b$ oder $a \mid c$.

In einem allgemeinen Ring sind diese Begriffe a priori verschieden.

Lemma. *R nullteilerfrei hat zur Folge (ii) ⇒ (i): Jedes Primelement ist irreduzibel.*

Beweis. □

3.4.6 Definition (faktorieller Ring)**.** *Sei R ein Ring, $x \in R$ und seinen $x = p_1 \cdots p_r = q_1 \cdots q_s$ zwei Zerlegungen von x in irreduzible Faktoren.*

(i) Wir sagen, dass die Zerlegungen äquivalent sind, falls $r = s$, und bis auf die Reihenfolge $p_i \sim q_i$ gilt. (d.h. $p_i \mid q_i$ und $q_i \mid p_i$, d.h. p_i und q_i unterscheiden sich nur um eine Einheit.)

(ii) Wir sagen, dass $x \in R$ eindeutige Zerlegung in Primfaktoren erlaubt, falls alle möglichen Zerlegungen von x äquivalent sind.

(iii) Wir sagen r ist faktorieller Ring, falls jedes $x \in R$, x keine Einheit, eine eindeutige Zerlegung in irreduzible Faktoren besitzt.

3.4.7 Hauptsatz. *Für einen Integritätsbereich R ist folgendes äquivalent:*

(i) R ist faktorieller Ring

(ii) In R gilt der so genannte Teilerkettensatz (jede echte Teilerkette $a_2 | a_1, a_3 | a_2, \ldots$, d.h. mengentheoretisch: $Ra_1 \subset Ra_2 \subset Ra_3 \cdots$, bricht nach endlich vielen Schritten ab) und in R ist jedes irreduzible Element immer auch ein Primelement.

Beweis. □

3.4.8 Satz (Lemma von Euklid)**.** *Wenn in R der Teilerkettensatz gilt, dann ist jedes $a \in R, a \neq 0, a \notin R^\times$ ein Produkt von endlich vielen irreduziblen Elementen.*

Beweis. □

Weiteres Ziel. Wir wollen sehen, dass jeder Hauptidealring faktoriell ist, weil er die charakteristischen Eigenschaften besitzt.

3.4.9 Definition (Ideal, Untermodul, Hauptideal, Hauptidealring)**.** *Ein Ideal $\mathfrak{I}$ in R ist eine Teilmenge, welche ein „R-Unterraum“ von R ist.*

D.h. Sind $x_1, \ldots, x_n \in \mathfrak{I}$, dann liegen auch alle Linearkombinationen $r_1x_1 + \cdots + r_nx_n, r_i \in R$ wieder in $\mathfrak{I}$.

Weil R kein Körper ist, sondern ein Ring, spricht man von R-Untermodul.

Wir nennen $\mathfrak{I}$ Hauptideal, falls ein Element $x \in R$ existiert, sodass $\mathfrak{I} = Rx$ ist („eindimensional“).

Wir nennen R Hauptidealring, falls jedes Ideal $\mathfrak{I}$ Hauptideal ist.

Folgerung. *Wenn $R = K$ ein Körper ist, dann gibt es für $\mathfrak{I}$ nur die Möglichkeiten*

(i) $\mathfrak{I} = \{0\}$

(ii) $\mathfrak{I} = K$

Beweis. □

13. VL
06.12.05

Ziel. Welches sind die allgemeinsten Bedingungen, unter denen der so genannte *Hauptsatz der Arithmetik* gilt, d.h. „eindeutige“ Zerlegung in irreduzible Faktoren.

Satz 2.2.8 sagt dann aus: $R = \mathbb{Z}$ ist Hauptidealring. Sei $\mathfrak{I} \subseteq \mathbb{Z}$, wähle $x \in \mathfrak{I}$ mit minimalen Absolutbetrag, dann ist $\mathfrak{I} = \mathbb{Z}x$.

3.4.10 Satz. *Der Integritätsbereich R sei ein Hauptidealring. Dann ist R faktoriell.*

Beweis. □

3.4.11 Definition (euklidischer Ring)**.** *Ein Integritätsbereich R heißt euklidischer Ring, falls es in R eine „Division mit Rest“ gibt. D.h. es existiert eine Gewichtsfunktion*

$$g : R \setminus \{0\} \to \mathbb{N} \qquad r \neq 0 \mapsto g(r)$$

Sind $a, b \in R, b \neq 0$, dann gibt es stets eine Darstellung:

$$a = qb + r \qquad \begin{array}{l} \text{mit } r = 0 (\text{d.h. } b \mid a) \\ \text{oder } g(r) < g(b) \end{array}$$

Man schreibt dann (R, g).

Bisher hatten wir $(\mathbb{Z}, |\cdot|)$, mit $g(x) = |x|$ in $\mathbb{Z}$.

3.4.12 Satz. *Ein euklidischer Ring (R, g) ist immer Hauptidealring und daher faktoriell.*

Beweis. □

Ein weiteres Beispiel für einen euklidischen Ring ist der Ring $K[X]$ aller Polynome mit Koeffizienten in einem Körper. Als Gewichtsfunktion nimmt man den Grad eines Polynoms, d.h. die höchste Potenz von X, welche in einem Polynom auftaucht.

Bemerkung. Da Nullpolynom hat keinen Grad. Konstanten ($\neq 0$) erhalten den Grad 0.

$$\begin{aligned} a &= a_0 + a_1X + \cdots + a_nX^n \\ a_n &\neq 0 \quad \deg(a) = n \\ b &= b_0 + b_1X + \cdots + b_nX^m \\ b_m &\neq 0 \quad \deg(b) = m \end{aligned}$$

$a \cdot b$ ist definiert durch formales Ausmultiplizieren unter Benutzung der Distributivität und man darf Koeffizienten von X beliebig vertauschen.

$$a \cdot b = \cdots + a_nb_mX^{n+m}$$

Wenn der Koeffizientenbereich ein nullteilerfreier Ring ist, dann folgt:

$$\deg(a \cdot b) = \deg(a) + \deg(b)$$

Körper sind insbesondere nullteilerfreie Ringe.

Lemma. *Seien $a, b \in K[X]$ zwei Polynome, $b \neq 0$ und $\deg(a) \geq \deg(b)$. Dann existiert ein Monom*[8] *M, so dass*

$$a = Mb + r \text{ und } \deg(r) < \deg(a) \text{ oder } r = 0$$

[8] ein Polynom der Art $M = aX^\nu$, mit Koeffizient a

3.4.13 Satz. $(K[X], \deg)$ *ist ein euklidischer Ring.*

Beweis. □

$K[X]$ ist faktorieller Ring. Die irreduziblen Elemente im faktoriellen Ring $K[X]$ heißen irreduzible Polynome.

Beispiel. Alle Polynome vom Grad 1 sind irreduzibel. Echter Teiler müssen den Grad 0 haben, als Konstante = Einheit.

Fall $K = \mathbb{R}$.

Zerlegung in irreduzible Faktoren

Noch eine Bemerkung zur Zerlegung in irreduzible Faktoren. Im Allgemeinen kann der Ring R viele Einheiten haben.

Betrachte: $\mathcal{P}$ = Menge aller irreduziblen Elemente und

$$p_1 \sim p_2 \quad \text{falls} \quad p_2 = \varepsilon p_1 \text{ mit } \varepsilon \in R^\times$$

Es gibt eine Äquivalenzrelation auf $\mathcal{P}$:

(i) Wähle einen Schnitt S für $\mathcal{P}/\sim$, d.h. wähle aus jeder Äquivalenzklasse genau einen Vertreter.

(ii) Dann: $x \in R, x \neq 0, x \notin R^\times$. Dann ist

$$x = p_1 \cdots p_n$$

ein Produkt irreduzibler Faktoren und es gilt auch

$$\begin{aligned} p_1 \sim s_1 \in S \text{ eindeutig } p_1 &= \varepsilon_1 s_1 \\ &\dots \\ p_n \sim s_n \in S \text{ eindeutig } p_n &= \varepsilon_n s_n \end{aligned}$$

Damit ist

$$x = (\varepsilon_1 \cdots \varepsilon_n) \cdot s_1 \cdots s_n$$

und man erhält mit $\varepsilon = \varepsilon_1 \cdots \varepsilon_n$, Einheit, eine Standardisierte Faktorzerlegung, die eindeutig bis auf die Reihenfolge ist:

$$x = \varepsilon s_1 \cdots s_n$$

Die Eindeutigkeit folgt aus: $s, s' \in S, s \mid s', s' \mid s \Rightarrow s \sim s' \Rightarrow s = s'$.

Beispiel (Polynomring $K[X]$). Einheiten = Konstanten $\neq 0$. Zu jedem Polynom $a_n X^n + a_{n-1} X^{n-1} + \cdots$ gibt es genau ein äquivalentes Polynom, welches den höchsten Koeffizienten = 1 hat:

$$a_n^{-1} \cdot a = 1 \cdot X^n + \cdots$$

Polynome mit höchstem Koeffizienten = 1 heißen *normiert*. Als Schnitt S für $\mathcal{P}/\sim$ nehmen wir die normierten irreduziblen Polynome.

Jedes Polynom $a \in K[X], \deg(a) \geq 1$ schreibt sich eindeutig

$$a = \varepsilon \cdot p_1 \cdots p_n$$

mit einer Konstanten $\varepsilon \in K$ und irreduziblen normierten Polynomen $p_i \in S$.

14. VL 12.12.05

Zusammenfassung.

$$\begin{aligned} &\text{Integritätsbereiche} \supset \text{Faktorielle Ringe} \\ &\supset \text{Hauptidealring} \supset \text{Euklidische Ringe } (R, g) \end{aligned}$$

3.5 Polynome und Funktionen

Sei $a = \sum_{i=0}^n a_i X^i \in K[X]$ ein Polynom mit Koeffizienten $a_i \in K$ im Körper K. Wir können dann Polynomen eine Funktion zuordnen:

$$K \ni x \mapsto a(x) \in K$$

$a(x) = \sum_{i=0}^n a_i x = a_0 +_K a_1 \cdot_K x + \cdots +_K a_n \cdot_K x^n$

3.5.1 Satz. *Sei $a \in K[X], x_0 \in K$. Dann ist x_0 eine Nullstelle der Funktion $a(x)$, d.h. $a(x_0) = 0 \in K$ genau dann, wenn $X - x_0 \mid a$ in $K[X]$.*

Beweis. □

3.5.2 Bemerkung. Wenn $a(x_0) = 0 \Rightarrow X - x_0 \mid a$. Es kann sein, dass sogar höhere Potenzen von $(X - x_0)$ das a teilen. Die höchste derartige Potenz nennt man *Vielfachheit* der Nullstelle x_0 von a.

3.5.3 Satz. *Sei $a \in K[X]$ ein Polynom, $a \neq 0$. Dann ist die Anzahl der Nullstellen von $a(x)$ im Körper K, einschließlich aller Vielfachen immer $\leq \deg(a)$.*

Beweis. □

3.5.4 Folgerung. *Seien $a, b \in K[X]$, beide von Grad $\leq n$. Und es gelte $a(x_i) = b(x_i)$ für mindestens $n+1$ verschiedene Argumente $x_i \in K$. Dann folgt: $a = b \in K[X]$.*

Beweis. Als Übung 8.1. □

3.6 Restklassen, Homomorphismen und Charakteristik

3.6.1 Definition und Satz. *Seien R ein kommutativer Ring, und $\mathfrak{I} \subset R$ ein Ideal. Für $x, y \in R$ sagen wir: $x \sim y$, falls $x - y \in \mathfrak{I}$. Das ist tatsächlich eine Äquivalenzrelation. Die Menge der Äquivalenzklassen, genannt Quotientenmenge, bezeichnet man mit $R/\mathfrak{I}$.*

Beweis. □

Bemerkung. Bisher hatten wir $R = \mathbb{Z}$ und $\mathfrak{I} = \mathbb{Z}m$.

$$\begin{aligned} x \sim y &\Leftrightarrow x - y \in \mathbb{Z}m \\ &\Leftrightarrow m \mid x - y \\ &\Leftrightarrow x = y + rm \text{ für ein } r \in \mathbb{Z} \end{aligned}$$

3.6.2 Definition und Satz. *Seien $[a], [b] \in R/\mathfrak{I}$ zwei Restklassen. Dann ist die Definition*

$$\begin{aligned} [a] + [b] &:= [a + b] \\ [a] \cdot [b] &:= [a \cdot b] \end{aligned}$$

repräsentantenunabhängig und macht aus $R/\mathfrak{I}$ einen kommutativen Ring mit Nullelement $[0_R]$ und dem Einselement $[1_R]$.

Beweis. □

3.6.3 Folgerung (Anwendung 1)**.** *$R, \mathfrak{I}$ wie zuvor. Dann ist $R/\mathfrak{I}$ ein Körper genau dann, wenn das Ideal $\mathfrak{I}$ maximal in R ist.*

Beweis. □

3.6.4 Folgerung (Anwendung 2)**.** *Sei R ein nullteilerfreier Hauptidealring (also faktoriell), und $\pi \in R$ ein irreduzibles Element. Dann ist der Restklassenring $R/\pi R$ stets ein Körper.*

Beweis. □

3.6.5 Folgerung (Anwendung 3)**.** *Für Polynomringe $R = K[X]$. Sei $a \in K[x]$ ein Polynom mit Grad $n \geq 1$. Wir betrachten den Restklassenring*

$$L = K[X]/a \cdot K[X]$$

Dann gilt:

(i) Sämtliche Polynome $b = \sum_{i=0}^{m} b_i X^i$ von einem Grad $m < n$ bilden genau ein Repräsentantensystem für die Restklassen in L.

(ii) K ist eingebettet in L als die Restklassen der konstanten Polynome.

(iii) Wir können L als K-Vektorraum betrachten, und dann hat er genau die Dimension n, und eine Basis ist

$$\mathcal{B} = \{[1_K], [X], [X^2], \cdots, [X^{n-1}]\}$$

(iv) Insbesondere: Wenn a ein irreduzibles Polynom ist, dann ist L sogar ein Körper, welcher K „enthält", und $\dim_K(L) = \deg(a)$.

Beweis. Als Übung 8.2. □

Bemerkung. (iv) ist die wichtigste Methode, um ausgehend von K größere Körper zu konstruieren.

Lemma (Hinweis)**.** *In $K[X]$ haben wir folgenden Eindeutigkeitssatz für die Division mit Rest: Seien $a, b \in K[X], a \neq 0$. Sei*

$$b = qa + r$$

mit $r = 0$ oder $\deg(r) < \deg(a)$. Dann ist diese Darstellung ist eindeutig.

Beweis. □

3.6.6 Definition (Homomorphismus)**.** *Eine Abbildung $f : R \to S$ zwischen zwei Ringen heißt Homomorphismus, falls*

(i) $f(r_1 +_R r_2) = f(r_1) +_S f(r_2)$

(ii) $f(r_1 \cdot_R r_2) = f(r_1) \cdot_S f(r_2)$.

3.6.7 Folgerung (Eigenschaften)**.** *Sechs Eigenschaften von Homomorphismen:*

(i) $f(0_R) = 0_S, f(-r) = -f(r)$

(ii) Wenn 1_R existiert, dann hat $s = f(1_R)$ die Eigenschaft:

$$s^2 = s$$

ein so genanntes Idempotent in S. Fall S nullteilerfrei mit 1_S, dann dürfen wir kürzen, und es folgt $s = 1_S$, d.h. $f(1_R) = 1_S$.

(iii) Sei $\ker(f) := \{r \in R, f(r) = 0_S\}$ *der so genannte Kern von f. Denn ist* $\ker(f)$ *immer in zweiseitiges Ideal in R. (D.h. ist stabil bei Linearkombination mir R von links und von rechts. Ist egal, falls R kommutativ ist.)*

(iv) $\mathrm{im}(f) := \{s \in S : s \in f(R)\}$ *ist ein Teilring von S.*

(v) $f : R \to S$ sei ein Ringhomomorphismus, welcher als Abbildung bijektiv ist. Dann ist die Umkehrabbildung wohldefiniert. $f^{-1} : S \to R$ ist ebenfalls ein Homomorphismus von Ringen.

Die Hintereinanderausführung von zwei Homomorphismen ist wieder ein Homomorphismus. Wenn f, g beide bijektiv sind, ist es die Komposition $f \circ g$ ebenfalls.

(vi) R sein kommutativer Ring, und $\mathfrak{I}_1, \mathfrak{I}_2$ zwei Ideale. Restklassenringe $R/\mathfrak{I}_1, R/\mathfrak{I}_2$ und Restklassen $[a]_1 \in R/\mathfrak{I}_1, [a]_2 \in R/\mathfrak{I}_2$.

Frage: Wann ist $[a]_1 \mapsto [a]_2$ ein vernünftige Abbildung? Genau dann, wenn $\mathfrak{I}_1 \subseteq \mathfrak{I}_2$ ist, und in diesem Fall ist die Abbildung ein Homomorphismus von Ringen.

Beweis. □

15. VL 13.12.05

3.6.8 Satz (Homomorphiesatz für Ringe)**.** *Es sei $f : R \to S$ ein Homomorphismus (kommutativer) Ringe. Dann induziert f einen Isomorphismus*

$$f_* : R/\ker(f) \xrightarrow{\sim} \mathrm{im}(f)$$

zwischen dem Restklassenring $R/\ker(f)$ und dem Bildring $\mathrm{im}(f)$.

Beweis. □

3.6.9 Satz. *Es sei $\mathbb{Z}$ der Ring der ganzen Zahlen, und es sei R ein beliebiger Ring mit Eins 1_R. Dann gibt es genau einen Homomorphismus von Ringen $\iota_R : \mathbb{Z} \to R$, welcher $\mathbb{Z} \in 1 \mapsto 1_R \in R$ abbildet.*

Beweis. □

3.6.10 Folgerung. *Sei R ein beliebiger Ring mit Eins. Dann induziert $\iota_R : \mathbb{Z} \to R$ einen Isomorphismus*

$$\iota_{R,*} : \mathbb{Z}/\ker(\iota_R) \xrightarrow{\sim} \mathrm{im}(\iota_R)$$

Andererseits ist $\ker(\iota_R)$ *ein Ideal im Hauptidealring $\mathbb{Z}$, also ist* $\ker(f) = d \cdot \mathbb{Z}$. *Zwei Fälle:*

(i) $d = 0$, d.h. ι_R ist injektiv, wir dürfen dann unter ι_R unser $\mathbb{Z}$ als Teilring von R auffassen.

(ii) $d \neq 0$. Dann o.B.d.A. $d > 0$. Dann ist d die kleinste Vielfachheit von 1_R, welche $= 0_R$ ist. Es ist $\iota_R : \mathbb{Z}/d\mathbb{Z} \to \mathrm{im}(\iota_R)$.

Beispiel. $\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}, a \mapsto [a], 1 \mapsto [1]$

Spezialfall. Was kann passieren, wenn der Ring R nullteilerfrei ist?

$$\iota_{R,*} : \mathbb{Z}/\ker(\iota_R) \xrightarrow{\sim} \mathrm{im}(\iota_R) \subset R$$

In diesem Fall ist auch das Bild nullteilerfrei, d.h. $\mathbb{Z}/\ker(\iota_R)$ ist nullteilerfrei.

Im ersten Fall $\ker(\iota_R) = 0$ ist $\mathbb{Z}/0 \cdot \mathbb{Z} = \mathbb{Z}$ nullteilerfrei.

Im zweiten Fall $\ker(\iota_R) = d\mathbb{Z}$ ($d \geq 1$, Ideal in $\mathbb{Z}$) ist $\mathbb{Z}/d\mathbb{Z}$ genau dann nullteilerfrei, wenn $d = p$ eine Primzahl ist.

Definition (Charakteristik)**.** *Wenn R nullteilerfrei ist, gibt es zwei Optionen:*

(i) $\mathbb{Z} \xhookrightarrow{\sim} R$, Vielfache der 1_R. Sage: Der Ring R hat die Charakteristik 0 ($\ker(\iota_R) = 0$).

(ii) Die kleinste Vielfachheit $m \cdot 1_R = 0$ ist $m = p$ eine Primzahl. Dann sagen wir: R hat die Charakteristik p ($\ker(\iota_R) = p \cdot \mathbb{Z}$)

Charakteristik p bedeutet, dass unser Ring R ein Vektorraum über dem Körper $\mathbb{Z}/p\mathbb{Z}$ mit p Elementen ist.

Bemerkung. Ist R ein Integritätsbereich, dann identifizieren sich die Vielfachen von 1_R mit $\mathbb{Z}$ genau dann, wenn R die Charakteristik 0 hat.

16. VL 02.01.06

4 Ganze und rationale Zahlen als Quotientenmenge

Erinnerung. Sei $(X, \sim)$ eine Menge mit Äquivalenzrelation, dann wird die Menge $X/\sim$ der Äquivalenzklassen, als die zugehöre Quotientenmenge bezeichnet.

Beispiel. Restklassenringe.

4.1 Konstruktion der ganzen Zahlen als Quotientenmenge

Gegeben ist $\mathbb{N} = \{1, 2, 3, \dots\}$ die Menge der natürlichen Zahlen. $\mathbb{N}$ ist ein kommutativer *Halbring* mit Operationen $+, \cdot$. Die üblichen Rechenregeln in einem Ring sind erfüllt, aber wir sprechen von Halbring, weil folgender Defekt besteht:

In $\mathbb{N}$ haben wir für die Addition kein neutrales Element und erst recht haben wir zu gegebenen $x \in \mathbb{N}$ kein „Negatives".

Zur Beherrschung dieses Defektes haben in 2.1 den Begriff der komplettierten Peano-Menge $(\mathbb{Z}, \nu, \iota)$ eingeführt, bestehend aus $\mathbb{N}, 0$ und dem Spiegelbild von $\mathbb{N}$.

Jetzt folgt eine etwas andere Konstruktion, ausgehend von der Vorstellung, dass jede ganze Zahl Differenz von zwei natürlichen Zahlen ist. Also betrachte die Menge der geordneten Paare:

$$\mathbb{N} \times \mathbb{N} = \{(a, b) : a, b \in \mathbb{N}\}$$

Wir wollen aus dem Paar (a, b) die ganze Zahl $a - b$ machen. Äquivalenz:

$$(a, b) \sim (c, d) \quad \text{falls} \quad a + d = b + c$$

Das äquivalente $a - b = c - d$ geht noch nicht, da in $\mathbb{N}$ kein „Negatives" existiert. Diese Relation ist in $\mathbb{N}$ wohldefiniert.

4.1.1 Definition und Satz. *Auf $\mathbb{N} \times \mathbb{N}$ definieren die Relation:*

$$(a, b) \sim (c, d) \quad :\Leftrightarrow \quad a + d = b + c$$

Dies ist eine Äquivalenzrelation.

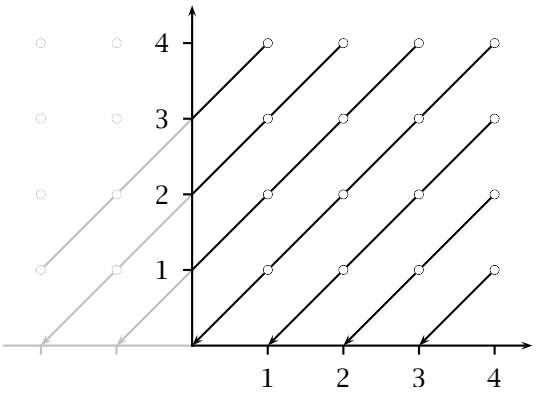
Beweis. □

4.1.2 Definition. *Damit dürfen wir jetzt zur Quotientenmenge*

$$\mathbb{Z} := \mathbb{N} \times \mathbb{N}/\sim$$

übergehen.

4.1.3 Veranschaulichung. Die Äquivalenzklassen sind jeweils alle Punkte, welche auf ein- und derselben Diagonalen liegen.



4.1.4 Definition und Satz (Addition auf $\mathbb{Z}$)**.** *Bezeichne mit $[a, b]$ die Äquivalenzklasse des Paares (a, b) und definiere:*

$$[a, b] + [c, d] := [a + c, b + d]$$

Diese Definition ist repräsentantenunabhängig, d.h. wenn $(a', b') \sim (a, b)$ und $(c', d') \sim (c, d)$, dann ist auch $(a' + c', b' + d') \sim (a + c, b + d)$.

Beweis. □

Heuristik. Nach der obigen Definition soll gelten:

$$(a - b) + (c - d) = (a + c) - (b + d)$$

In $\mathbb{N}$ existiert jedoch kein „Negatives"!

4.1.5 Satz. *Die Menge $(\mathbb{Z}, +)$ mit der soeben definierten Addition ist eine kommutative Gruppe mit dem neutralen Element $0 = [a, a]$ und dem Negativen $-[a, b] = [b, a]$.*

Beweis. □

4.1.6 Definition und Satz (Trichotomie auf $\mathbb{Z}$)**.** *Wir setzen:*

$$\begin{aligned} \mathbb{Z}_+ &:= \{[a, b] : a > b\} \\ 0 &:= \{[a, b] : a = b\} \\ \mathbb{Z}_- &:= \{[a, b] : a < b\} \end{aligned}$$

(benutze hier die Ordnungsrelation auf $\mathbb{N}$, siehe 1.3). Diese Definitionen sind repräsentantenunabhängig und ergeben die Trichotomie $\mathbb{Z} = \mathbb{Z}_+ \dot\cup 0 \dot\cup \mathbb{Z}_-$.

Beweis. □

Schließlich wollen wir noch sehen, dass $\mathbb{Z}$ eine komplettierte Peano-Menge ist, d.h. wir brauchen eine Einbettung von $\mathbb{N}$ in $\mathbb{Z}$.

4.1.7 Definition (Einbettung von $\mathbb{N}$ in $\mathbb{Z}$)**.**

$$\begin{aligned} \iota : \mathbb{N} &\to \mathbb{Z} \\ a &\mapsto i(a) := [a+x, x] \end{aligned}$$

für irgendein x aus $\mathbb{N}$. Da wir die Äquivalenzklasse betrachten spielt die Wahl von $x \in \mathbb{N}$ keine Rolle.

Dieses ι induziert eine Bijektion zwischen $\mathbb{N}$ und dem Positivbereich $\mathbb{Z}_+$, $\iota(a) \in \mathbb{Z}_+$, weil $a + x > x$. Umgekehrt: $[a,b] \in \mathbb{Z}_+$, d.h. $a > b$, damit ist $a - b$ die wohldefinierte natürliche Zahl, sodass $b + (a - b) = a$ ist (1.3.2).

$$\begin{aligned} \mathbb{N} &\to \mathbb{Z}_+ \\ a &\mapsto [a+x, x] \\ a - b &\mapsfrom [a,b] \end{aligned}$$

Offensichtlich sind die beiden Abbildung zueinander invers, d.h. Hintereinanderschalten ergibt die Identität. Damit ist $\mathbb{N}$ als $\mathbb{Z}_+$ in $\mathbb{Z}$ eingebettet.

4.1.8 Satz. *Die Einbettung $\iota : \mathbb{N} \to \mathbb{Z}$ ist*

(i) ein Homomorphismus, d.h. $\iota(a+b) = \iota(a) + \iota(b)$.

(ii) innerhalb von $\mathbb{Z}$ gilt $[a,b] = \iota(a) - \iota(b)$.

Beweis. □

4.1.9 Folgerung. *$(\mathbb{Z}, \nu, \iota)$ mit*

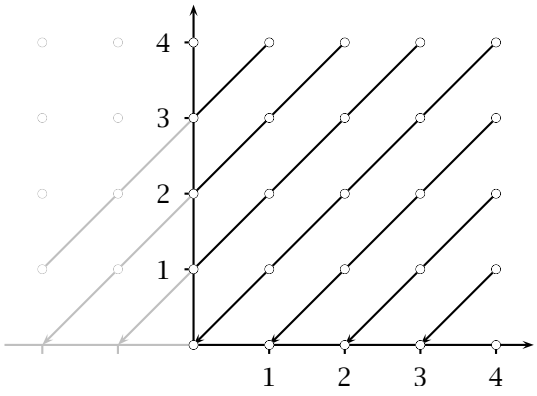
$$\begin{aligned} \nu(x) &= x + \iota(\mathbb{1}) \\ \iota(x) &= -x \end{aligned}$$

ist eine Komplettierung der Peano-Menge $(\mathbb{Z}, \nu) \leftrightarrow (\mathbb{N}, \nu)$.

Weiteres Ziel. Wir wollen $\mathbb{Z} = \mathbb{N} \times \mathbb{N}/\sim$ zu einem Ring machen, indem wir auch die Multiplikation von $\mathbb{N}$ auf $\mathbb{Z}$ fortsetzen. Wir gehen zunächst von $\mathbb{N}$ zu $\mathbb{N}_0 := \mathbb{N} \dot\cup \{0\}$ (größere Peano-Menge) über und betrachten

$$\mathbb{Z} = \mathbb{N}_0 \times \mathbb{N}_0/\sim \overset{(?)}{=} \mathbb{N} \times \mathbb{N}/\sim$$

Veranschaulichung von (?):



Dieselben Klassen, aber jede Äquivalenzklasse hat ein Element mehr (nämlich $(x,0)$ oder $(0,x)$).

Auf $\mathbb{N}_0$ haben $+, \cdot$. Das macht $\mathbb{N}_0$ zu einem kommutativen Halbring mit Null und Eins.

Ausdehnung der Multiplikation von $\mathbb{N}_0$ auf $\mathbb{Z} = \mathbb{N}_0 \times \mathbb{N}_0/\sim$.

Heuristik. Wir brauchen: $(a-b)(c-d) = ac + bd - ad - bc$.

4.1.10 Definition (Multiplikation)**.** *Also definiere die folgende Multiplikation von Paaren:*

$$(a,b) \cdot (c,d) := (ac + bd, ad + bc)$$

Dies ist zunächst eine Operation auf $\mathbb{N}_0 \times \mathbb{N}_0$. Daraus wollen wir eine Operation auf den Äquivalenzklassen machen, vermittels

$$[a,b] \cdot [b,c] := [ac + bd, ad + bc]$$

Problem. Zeige, dass diese Definition repräsentantenunabhängig ist, und dass alle Rechengesetze „kommutativ“, „assoziativ“ und „distributiv“ erfüllt sind. Dies ist rechenaufwendig, siehe [RS05, 6.2].

Um den Rechenaufwand zu reduzieren, gehen

wir zu Matrizen über, und zwar betrachte

$$\begin{array}{c} \mathbb{N}_0^{2\times 2} \text{ Matrizen mit Einträgen aus } \mathbb{N}_0 \\ \cup \\ \mathcal{Z} \leftrightarrow \mathbb{N}_0 \times \mathbb{N}_0 \\ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \leftrightarrow (a,b) \end{array}$$

Damit haben wir unsere Multiplikation (4.1.10) realisiert als Multiplikation von Matrizen:

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix} \cdot \begin{pmatrix} c & d \\ d & c \end{pmatrix} = \begin{pmatrix} ac+bd & ad+bc \\ ad+bc & ad+bc \end{pmatrix}$$

Da ganz allgemein die Multiplikation von Matrizen assoziativ ist, vererbt sich dies auf unsere Multiplikation 4.1.10. Multiplikation ist im Allgemeinen nicht kommutativ. Jedoch in $\mathcal{Z}$ gilt die Kommutativität, wie man sofort nachrechnet (siehe Übung 10.1). Ebenso gilt die Distributivität.

Zwischenergebnis. $\mathcal{Z} \leftrightarrow \mathbb{N}_0 \times \mathbb{N}_0$ ist kommutativer Halbring mit dem Nullelement $\left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right) \leftrightarrow (0,0)$ und dem Einselement $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \leftrightarrow (1,0)$.

Wir müssen aus $\mathcal{Z}$ unser richtiges $\mathbb{Z} = \mathbb{N}_0 \times \mathbb{N}_0/\sim$ machen, indem wir die Äquivalenzrelation nach $\mathcal{Z}$ transportieren. Und dann zeigen, dass die Quotientenmenge $\mathbb{Z} = \mathcal{Z}/\sim$ ein echter Ring ist.

Äquivalenzrelation.

$$(a,b) \sim (c,d) \quad \text{falls} \quad a+d = b+c$$

d.h. $(a,b)+(d,c) = (a+b,b+c)$ gehört zur 0-Klasse.

Für Matrizen betrachte $\mathcal{J} = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \in \mathcal{Z}$. Umtauschen der Einträge entspricht der Multiplikation mit $\mathcal{J}$:

$$\mathcal{J} \cdot \begin{pmatrix} a & b \\ b & a \end{pmatrix} = \begin{pmatrix} b & a \\ a & b \end{pmatrix}$$

Seien $A, B \in \mathcal{Z}$. Deshalb sage

$$A \sim B \quad \text{falls} \quad A + \mathcal{J} \cdot B = \begin{pmatrix} x & x \\ x & x \end{pmatrix}$$

wobei x beliebig ist (entspricht der 0-Klasse).

17. VL
03.01.06

Ausgangspunkt.

- $(\mathbb{N}_0, +, \cdot)$ ist nur ein Halbring $\rightsquigarrow \mathbb{Z}$ = Ring
- $\mathbb{N}_0 \times \mathbb{N}_0 \ni (a,b)$, dieses Paar steht für die Differenz $a-b$. $(a,b) \sim (c,d)$ falls $a+d = b+c$ ist eine Äquivalenzrelation.
- $\mathbb{Z} = (\mathbb{N}_0 \times \mathbb{N}_0)/\sim$ Quotientenmenge, $[a,b]$ Äquivalenzklasse von (a,b).
- $+ : (a,b)+(b,c) = (a+c,b+d)$ vererbt sich auf Äquivalenzklassen.
- $\cdot : (a,b)\cdot(c,d) = ac+bd, ad+bc)$ Multiplikation von Zahlenpaare, da $(a-b)\cdot(c-d) = ac+bd-(ad+bc)$. (4.1.10)

Wir wollen wieder von den Zahlenpaaren zu den Äquivalenzklassen übergehen:

Trick. Wir erweitern unsere Paare zu Matrizen:

$$\begin{array}{c} (a,b) \overset{(*)}{\leftrightarrow} \begin{pmatrix} a & b \\ b & a \end{pmatrix} \\ \mathbb{N}_0 \times \mathbb{N}_0 \leftrightarrow \mathcal{Z} \subset \mathbb{N}_0^{2\times 2} \end{array}$$

Unter $(*)$ entspricht unsere Multiplikation 4.1.10 genau der Multiplikation von Matrizen.

Umschreiben der Äquivalenzrelation 4.1.1. $(a,b) \sim (c,d)$ falls $a+d = b+c$. Wir zeichnen in $\mathbb{N}_0 \times \mathbb{N}_0$ die Teilmenge $\mathcal{O}$ aus:

$$\begin{array}{c} \mathcal{O} = \{(a,a) : a \in \mathbb{N}_0\} \\ \updownarrow \\ \mathcal{O}_{\mathcal{Z}} = \left\{ \begin{pmatrix} a & a \\ a & a \end{pmatrix} : a \in \mathbb{N}_0 \right\} \end{array}$$

Wir können die Relation folgendermaßen ausdrücken:

4.1.11 Definition (Äquivalenzrelation)**.** *Für $a,b,c,d \in \mathbb{N}_0$ und $A, C \in \mathcal{Z}$:*

$$\begin{array}{rcl} (a,b) \sim (c,d) & :\Leftrightarrow & (a,b)+(d,c) \in \mathcal{O} \\ A \sim B & :\Leftrightarrow & A + \mathcal{J}C \in \mathcal{O}_{\mathcal{Z}} \end{array}$$

mit $\mathcal{J} = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ einer Elementarmatrix (bei der Zeilen bzw. Spalten der Einheitsmatrix vertauscht werden).

$\mathcal{J}C$ bedeutet umtauschen der Zeilen bzw. Spalten:

$$C = \begin{pmatrix} c & d \\ d & c \end{pmatrix} \qquad \mathcal{J}C = \begin{pmatrix} d & c \\ c & d \end{pmatrix} = C\mathcal{J}$$

also mit $A = \left(\begin{smallmatrix} a & b \\ b & a \end{smallmatrix}\right)$ und $C = \left(\begin{smallmatrix} c & d \\ d & a \end{smallmatrix}\right)$:

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix} \sim \begin{pmatrix} c & d \\ d & c \end{pmatrix} \text{falls} \begin{pmatrix} a & b \\ b & a \end{pmatrix} + \begin{pmatrix} d & c \\ c & d \end{pmatrix} \in \mathcal{O}_{\mathcal{Z}}$$

4.1.12 Satz. *Die Multiplikation von Matrizen in $\mathcal{Z}$ vererbst sich auf die Quotientenmenge $\mathbb{Z} = \mathcal{Z}/\sim$, d.h.*

$$\begin{matrix} A \sim A' \\ B \sim B' \end{matrix} \quad \Rightarrow \quad AB \sim A'B' \tag{1}$$

Wenn $[A]$ die Äquivalenzklasse von A bezeichnet, dann ist

$$[A] \cdot [B] := [AB]$$

wohldefiniert.

Beweis. □

4.1.13 Satz. *Die Quotientenmenge $\mathbb{Z} = \mathcal{Z}/\sim$ erbt die Operationen $+, \cdot$ und ist bezüglich dieser Operation ein Ring.*

Beweis. □

Zusatzbemerkung. Unsere Ausgangsmenge $\mathbb{N}_0$ ist in $\mathbb{Z}$ eingebettet vermittels

$$a \in \mathbb{N}_0 \begin{cases} \nearrow (a,0) \\ \searrow \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \end{cases} \in \mathbb{Z}$$

Diese Einbettung ist verträglich mit den Operationen $+, \cdot$ (ein Homomorphismus):

Vorteil dieser Konstruktion: Wir bekommen die Operationen auf $\mathbb{Z}$ direkt, ohne Fallunterscheidung.

Rückblende.

$$\mathbb{Z} = \mathbb{N} \dot\cup 0 \dot\cup -\mathbb{N}$$

$$\mathbb{Z} \times \mathbb{Z} \overset{+,\cdot}{\to} \mathbb{Z}$$

Definition durch Fallunterscheidung, mit zusätzlichen Rechnungen, damit alles wie vorgesehen abläuft.

4.1.14 Satz. *Sei R ein beliebiger Ring mit Eins. Dann gibt es genau einen Ringhomomorphismus $\iota_R : \mathbb{Z} \to R$ mit der Eigenschaft $\iota_R(1) = 1_R$.*

Beweis. □

Reflexion. Wir haben aus einem Halbring $(H, +, \cdot)$ einen Ring $(R, +, \cdot)$ konstruiert. Weitgehend unabhängig von der Tatsache, dass zufällig $H = \mathbb{N}$ ist. Die einzige Eigenschaft von H, welche wirklich gebraucht wurde, ist die Kürzungsregel der Addition, d.h.

$$h + h_1 = h + h_2 \quad \Rightarrow \quad h_1 = h_2$$

1. Schritt: $H \times H \ni (a, b)$

$$(a, b) \sim (c, d) \quad \text{falls} \quad a + d = b + c$$

Die Transitivitätseigenschaft kann man nur beweisen, wenn in $(H, +)$ die Kürzungsregel gilt.

4.2 Der Quotientenkörper (Die Konstruktion rationaler Zahlen)

18. VL 09.01.06

Wir nehmen die ganzen Zahlen $\mathbb{Z}$ als gegeben und wollen daraus die rationalen Zahlen $\mathbb{Q}$ konstruieren. Die Konstruktion beruht auf der Kürzungsregel der Multiplikation, d.h.

$$ab = ac \text{ und } a \neq 0 \Rightarrow b = c$$

Wir beginnen mit einem beliebigen Integritätsbereich R = kommutativer nullteilerfreier Ring mit Eins.

4.2.1 Definition (Addition und Multiplikation)**.** *Bilde aus R den größeren Bereich B, bestehend aus allen Paaren $\left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right)$ mit $b \neq 0$. Wir führen für diese Paare eine Addition und eine Multiplikation ein, beruhend auf den Operationen in R:*

$$\begin{pmatrix} a \\ b \end{pmatrix} + \begin{pmatrix} c \\ d \end{pmatrix} := \begin{pmatrix} ad + bc \\ bd \end{pmatrix}$$

b, d beide $\neq 0 \Rightarrow bd \neq 0$, da R nullteilerfrei

$$\begin{pmatrix} a \\ b \end{pmatrix} \cdot \begin{pmatrix} c \\ d \end{pmatrix} := \begin{pmatrix} ac \\ bd \end{pmatrix}$$

Beispiel. $\left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right) + \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right)$

4.2.2 Folgerung (Übertragung der Rechenregeln)**.** *Einige der Rechenregeln übertragen sich von R auf die Operationen in B:*

(i) $+$ *ist assoziativ und kommutativ mit Nullelement* $\binom{0}{1}$.

(ii) $\cdot$ *ist assoziativ und kommutativ mit Einselement* $\binom{1}{1}$.

Fehlanzeigen. In B gibt es kein Distributivgesetz und es gibt im Allgemeinen kein „Negatives“.

$$\binom{a}{b} + \binom{-a}{b} = \binom{0}{b^2} \neq \binom{0}{1}$$
$$\left(\binom{a}{b} + \binom{c}{d}\right) \cdot \binom{e}{f} \neq \binom{a}{b}\binom{e}{f} + \binom{c}{d}\binom{e}{f}$$

4.2.3 Definition und Satz (Äquivalenzrelation)**.** *Wir führen auf B die folgende Relation ein:*

$$\binom{a}{b} \sim \binom{c}{d} \quad \textit{falls} \quad ad = bc$$

Dies ist eine Äquivalenzrelation.

Beweis. □

Notation. Es sei $Q = B/\sim$ die Quotientenmenge. Für die Elemente schreiben wir:

$$\frac{a}{b} := \left[\binom{a}{b}\right] = \text{ Äquivalenzklasse von } \binom{a}{b}$$

In diesem Fall sind die Äquivalenzklassen wirklich Quotienten. Dies ist der Ursprung des Begriff „Quotientenmenge“.

4.2.4 Satz (Repräsentantenunabhängigkeit von $+, \cdot$)**.** *Die Operationen $+, \cdot$ übertragen sich von B auf die Quotientenmenge Q, weil sie repräsentantenunabhängig sind.*

Beweis. □

4.2.5 Satz (Quotientenkörper)**.** $(Q, +, \cdot)$ *ist ein (kommutativer) Körper. Man nennt* $Q = \mathrm{Quot}(R)$ *den Quotientenkörper des Integritätsbereichs R.*

Beweis. □

4.2.6 Folgerung (Einbettung von R in Q)**.** *Wir habe eine natürliche Einbettung $\iota : R \to Q$, nämlich die Abbildung $\iota(a) := \frac{a}{1}$. Diese Abbildung ist verträglich mit den Operationen $+, \cdot$, d.h. ein Homomorphismus von Ringen, und in Q gilt:*

$$\frac{a}{b} = \iota(a) \cdot \iota(b)^{-1}$$

Beweis. □

4.2.7 Hauptbeispiele. (i) $R = \mathbb{Z}$, dann sind $\mathbb{Q} = \mathrm{Quot}(\mathbb{Z})$ die rationalen Zahlen.

(ii) $R = I[X]$ Polynome mit Koeffizienten in einem Integritätsbereich. Dann ist R selbst ein Integritätsbereich.

$$\begin{aligned} a &= a_0 + \cdots + a_n X^n \\ b &= b_0 + \cdots + b_m X^m \\ ab &= \cdots + \underbrace{a_n b_m}_{\neq 0} X^{n+m} \end{aligned}$$

$Q = I(X) := \mathrm{Quot}(I[X])$ ist der Körper der *rationalen Funktionen* mit Koeffizienten in X.

Bemerkung. Aus jeder formalen rationalen Funktion $\frac{a_0+a_1X+\cdots+a_nX^n}{b_0+b_1X+\cdots+b_mX^m}$ wird durch Auswerten eine echte Funktion mit Werten in $\mathrm{Quot}(I)$:

$$x \in I \mapsto \frac{a_0 + a_1 x + \cdots + a_n x^n}{b_0 + b_1 x + \cdots + b_m x^m} \in \mathrm{Quot}(I)$$

Bemerkung. Wenn R bereits ein Körper ist, dann folgt $R = \mathrm{Quot}(R)$.

4.2.8 Rechnen mit Brüchen. Man versucht, die Nenner so klein wie möglich zu halten. (Voraussetzung: In R sei $\mathrm{ggT}(a, b)$ wohldefiniert, z.B. $R = \mathbb{Z}$.)

$$\frac{a}{b} = \frac{a/\mathrm{ggT}(a,b)}{b/\mathrm{ggT}(a,b)} = \frac{a_0}{b_0} \quad \text{(reduzierter Bruch)}$$

Man nennt b_0 den Nenner von $\frac{a}{b}$. Der Nenner ist eindeutig bis auf Einheiten $\varepsilon \in R^\times$. (In $\mathbb{Z}$: $\frac{a_0}{b_0} = \frac{-a_0}{-b_0}$. Wenn man fordert, dass der Nenner positiv sein soll, dann hat jede rationale Zahl einen eindeutig bestimmten Nenner.)

Erweitern mit Faktoren: $\frac{a}{b} = \frac{ac}{bc}, c \neq 0, \in R$.

4.2.9 Satz (Eindeutigkeitsaussage)**.** *Der Integritätsbereich R sei ein faktorieller Ring. Dann vererbt sich die eindeutige Zerlegung in Primfaktoren von R auf den Quotientenkörper Q.*

Sei P die Menge aller Primelemente in R, sei S ein Repräsentantensytem für $P/\sim$ ($p_1 \sim p_2 \Leftrightarrow p_1 \mid p_2 \wedge p_2 \mid p_1 \Leftrightarrow p_2 = \varepsilon p_1, \varepsilon \in R^\times$). Dann schreibt sich jedes $x \in Q$ eindeutig in der Form:

$$x = \varepsilon \prod_{p \in S} p^{\nu_p(x)}$$

mit ganzzahligen Exponenten $\nu_p(x)$.

Beweis. □

19. VL
10.01.06

Beispiele.

- $\frac{18}{25} = 2 \cdot 3^2 \cdot 5^{-2}$
- $R = K[X]$ Polynomring über einem Körper, ist faktoriell. $K(X) = \mathrm{Quot}(R) \in f$ ist rationale Funktion. f schreibt sich eindeutig in der Form:
$$f = \varepsilon \prod_{p} p^{\nu_p(f)}$$
mit einer Konstanten $\varepsilon \in K, \neq 0$, wobei p läuft über die irreduziblen und normierten Polynome aus $R = K[X]$. Exponenten $\nu_P(f)$ dürfen auch negativ sein.

4.2.10 Definition und Satz (Ordnung auf $\mathbb{Q}$)**.** *Unser Positivbereich $\mathbb{Q}_+$ ist definiert als die Menge aller Quotienten $\alpha = \frac{a}{b}$ mit $a, b \in \mathbb{N}$. Offensichtlich:*

(i) $0 = \frac{0}{1} \notin \mathbb{Q}_+$

(ii) $\alpha, \beta \in \mathbb{Q}_+ \Rightarrow \alpha + \beta, \alpha \cdot \beta, \alpha \cdot \beta^{-1} \in \mathbb{Q}_+$

(iii) Weiter haben wir (ebenso wie für $\mathbb{Z}$) die Trichotomie:

$$\mathbb{Q} = \mathbb{Q}_+ \dot\cup \{0\} \dot\cup -\mathbb{Q}_+$$

Wir definierten die Ordnung auf $\mathbb{Q}$ durch:

$$\alpha < \beta \quad :\Leftrightarrow \quad \beta - \alpha \in \mathbb{Q}_+$$

Beweis. □

Die Eigenschaften von Q_+ werden dann reflektiert durch die Eigenschaften von $<$. z.B.:

$$\alpha < \beta, \gamma > 0 \quad \Rightarrow \quad \alpha\gamma < \beta\gamma$$

weil $\beta\gamma - \alpha\gamma = \underbrace{(\beta - \alpha)}_{\in \mathbb{Q}_+} \cdot \underbrace{\gamma}_{\in \mathbb{Q}_+}$

4.2.11 Folgerung (Totalordnung)**.** *$\mathbb{Q}$ ist total geordnet, d.h. für je zwei Elemente α, β gilt genau eine der Relationen*

$$\begin{array}{ccc} \alpha < \beta & \alpha = \beta & \beta < \alpha \\ \beta - \alpha \in \mathbb{Q}_+ & \alpha - \beta = 0 & \alpha - \beta \in \mathbb{Q}_+ \end{array}$$

Aber im Gegensatz zu $\mathbb{N}$ ist $\mathbb{Q}_+$ nicht mehr wohlgeordnet[9]

$$Q_+ \subset \{1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots\}$$

ist eine Teilmenge ohne kleinstes Element.

4.2.12 Lemma (Gaußklammer)**.** *Sei $\alpha = \frac{a}{b} \in \mathbb{Q}$. Dann gibt es genau eine ganze Zahl $q \in \mathbb{Z}$ mit*

$$q \le \alpha < q + 1$$

Man schreibt $q = \lfloor \alpha \rfloor$ (α abgerundet auf eine ganze Zahl).

Beweis. □

Beispiel.

$$\lfloor 4{,}81 \rfloor = 4$$
$$\lfloor -4{,}81 \rfloor = -5$$

$-x$ abgerundet ist $-(x$ aufgerundet).

4.2.13 Satz (Darstellung rationaler Zahlen durch Positionssysteme)**.** *Wir geben eine natürliche Zahl $g > 1$ vor (Basiszahl, z.B. $g = 10$). Sei $M_g = \{0, 1, 2, \dots, g-1\}$. Dann können wir jedes $\beta \in \mathbb{Q}_+$ eindeutig entwickeln in der Form*

$$\beta = \sum_{i=-\infty}^{+\infty} b_i g^i \quad \text{mit} \quad b_i \in M_g$$

wobei die Summe nach oben ($i \to \infty$) abbricht.

Beweis. □

Zusatz. Dabei ist $\beta_m := \sum_{-m}^{\infty} b_i g^i \in \frac{1}{g^m}\mathbb{Z}$ die zu β benachbarte Zahl aus dem Raster $\frac{1}{g^m}\mathbb{Z}$, so dass $\beta_m \le \beta$. Unter Benutzung der Gaußklammer können wir also schreiben:

$$\beta_m = \frac{\lfloor g^m \cdot \beta \rfloor}{g^m}$$

[9] In $\mathbb{N}$ bzw. in jeder Teilmenge $M \subset \mathbb{N}$ existiert immer ein eindeutig bestimmtes kleinstes Element.

Beispiel. Für $g = 10$ und $\beta = \frac{1}{7}$ ergibt sich die Dezimalbruchentwicklung $\beta_m = \frac{\lfloor g^m \beta \rfloor}{g^m}$:

$$\beta_1 = \frac{\lfloor \frac{10}{7} \rfloor}{10} = \frac{1}{10} = 0{,}1$$
$$\beta_2 = \frac{\lfloor \frac{100}{7} \rfloor}{100} = \frac{14}{100} = 0{,}14$$
$$\beta_3 = \frac{\lfloor \frac{1000}{7} \rfloor}{1000} = 0{,}14\ldots$$

Folgerung. *Die Entwicklung bricht genau dann ab, wenn für großes m $\beta = \beta_m$ ein Punkt des Rasters $\frac{1}{g^m}\mathbb{Z}$ ist. Das ist genau dann der Fall, wenn sämtliche Primteiler des Nenners von β in g aufgehen.*

Beweis. □

Beispiel. Für $g = 10$. Die Dezimalbruchentwicklung von $\beta = \frac{a}{b}$ ist genau dann endlich, wenn im Nenner von β nur die Primzahlen 2 und 5 aufgehen. Wenn andere Primzahlen auftreten, ist die Entwicklung unendlich.

Satz. *Die rationalen Zahlen zeichnen sich dadurch, dass die g-Entwicklung, wenn schon nicht endlich, dann aber immer periodisch ist (im Allgemeinen mit Vorperiode).*

Beweis. □

20. VL
16.01.06

4.2.14 Definition und Satz (Eine Bemerkung aus der Gruppentheorie)**.** *Sei G eine endliche kommutative Gruppe mit n Elementen (multiplikativ geschrieben). Als Ordnung $\#g$ eines Elements $g \in G$ bezeichnet man die kleinste ganze Zahl $s \geq 1$, so dass $g^s = 1$ ist. ($s \cdot g = 0$, falls die Gruppenoperation additiv geschrieben ist.)*

Behauptung: Es gilt stets

$$\#g \mid n$$

Beweis. □

4.2.15 Lemma. *Sei $\beta \in \mathbb{Q}_+$ mit*

(i) $0 < \beta < 1$

(ii) Der Nenner c von β ist prim zur Basiszahl g.

Dann ist die g-Entwicklung von β rein periodisch mit der Periode

$$s = \#[g] \in (\mathbb{Z}/c\mathbb{Z})^\times$$

(Gruppe der zu c primen Restklassen). Insbesondere ist die Periode immer ein Teiler von

$$\varphi(c) := \#(\mathbb{Z}/c\mathbb{Z})^\times$$

Beweis. □

Beispiel. Sei $g = 10, \beta = \frac{3}{7}$. Dann ist $c = 7$ prim zu $g = 10$ und $\varphi(c) = 7 - 1 = 6$. Periode der Dezimalbruchentwicklung ist

$$s = \#[10] \in \underbrace{(\mathbb{Z}/7\mathbb{Z})^\times}_{\text{Gruppe der Ordnung 6}}$$

Die Periode ist auf jeden Fall ein Teiler von 6. Andererseits sieht man, dass 6 minimal ist:

$$10^6 \equiv 1 \mod 7$$

Also ist die Periode tatsächlich 6.

4.2.16 Satz. *Sei $\beta \in \mathbb{Q}_+, g \neq 1$ die fixierte Basiszahl. Dann wird die g-Entwicklung von β nach einer gewissen Vorperiode stets periodisch.*

Beweis. □

4.2.17 Satz. *Umgekehrt habe die g-Entwicklung von β die Form: Vorperiode + Periode, dann ist β eine rationale Zahl.*

Beweis. Als Übung 11.1. □

Defekt. Was ist mit denjenigen Zahlen, deren g-Entwicklung niemals periodisch wird? Stichwort: irrationale Zahlen.

4.2.18 Lemma (Ein Beispiel)**.** *Sei $a \in \mathbb{N}$. Dann gilt: Ein $\alpha \in \mathbb{Q}$ mit der Eigenschaft $\alpha^2 = a$ existiert genau dann, wenn a bereits Quadrat einer natürlichen Zahl ist.*

Beweis. □

5 Die reellen Zahlen

5.1 Cauchyfolgen rationaler Zahlen und ihre Eigenschaften

Bisher haben wir $(\mathbb{Q}, <)$ mit $\alpha < \beta$, falls $\beta - \alpha \in \mathbb{Q}_+$ und $\mathbb{Q} = -\mathbb{Q}_+ \dot\cup 0 \dot\cup \mathbb{Q}_+$.

Definition. *(*sgn, $|\circ|$*) Für $x \in \mathbb{Q}$ setzen wir*

$$\operatorname{sgn}(x) := \begin{cases} 1 & \text{falls } x \in \mathbb{Q}_+ \\ 0 & \text{falls } x = 0 \\ -1 & \text{falls } x \in \mathbb{Q}_- \end{cases}$$

$$|x| := \begin{cases} x & \text{falls } x \geq 0 \\ \operatorname{sgn}(x) \cdot x & \text{falls } x < 0 \end{cases}$$

5.1.1 Folgerung (Eigenschaften)**.** *Für den Absolutbetrag rationaler Zahlen gilt:*

$$|xy| = |x||y|$$
$$|x + y| \leq |x| + |y|$$
$$||x| - |y|| \leq |x - y|$$

Beweis. Als Übung 11.2. □

5.1.2 Definition (konvergiert, Cauchyfolge)**.** *(i) Eine Folge $(\alpha_n)_{n\in\mathbb{N}}$ rationaler Zahlen $\alpha_n \in \mathbb{Q}$ konvergiert gegen eine rationale Zahl α, falls zu jeder rationales Zahl $\varepsilon > 0$ ein $N = N(\varepsilon) \in \mathbb{N}$ existiert, so dass*

$$\forall\, n \geq N : |\alpha - \alpha_n| < \varepsilon$$

(ii) Eine Folge $(\alpha_n)_{n\in\mathbb{N}} \subset \mathbb{Q}$ heißt Cauchyfolge (Fundamentalfolge) falls zu jedem $\varepsilon \in \mathbb{Q}_+$ ein $N = N(\varepsilon) \in \mathbb{N}$ existiert, so dass

$$\forall\, n, m \geq N : |\alpha_n - \alpha_m| < \varepsilon$$

Idee. Die Cauchy-Folgen sind „im wesentlichen“ die reellen Zahlen.

5.1.3 Satz (Konvergenzkriterium)**.** *Konvergiert $(\alpha_n)_{n\in\mathbb{N}} \subset \mathbb{Q}$ gegen $\alpha \in \mathbb{Q}$, dann ist (α_n) eine Cauchyfolge.*

Beweis. □

Bemerkung. Also: Konvergente Folgen $\subseteq$ Cauchyfolgen. Der Begriff $|\alpha_n - \alpha_{n+1}| < \varepsilon$, $\forall\, n \geq N$ wäre aber zu weit gefasst, weil dann $a_n = \sum_{i=1}^{n} \frac{1}{i}$ eine zulässige Folge wäre, die ist aber divergent.

5.1.4 Satz. *Sei $(a_n)_{n\in\mathbb{N}} \subset \mathbb{Q}$ eine monoton wachsende (bzw. fallende) Folge, und nach oben (bzw. unten) beschränkt, d.h. $\forall\, n : a_n \leq s$ (bwz. $a_n \geq s$) für ein $s \in \mathbb{Q}$. Dann ist (a_n) eine Cauchyfolge.*

Beweis. Als Übung 11.3. □

21. VL
17.01.06

5.1.5 Satz. *Sei $(a_n)_{n\in\mathbb{N}} \subset \mathbb{Q}$ eine Cauchyfolge, welche nicht gegen eine gegebene Zahl $b \in \mathbb{Q}$ konvergiert. Dann existiert immer eine Schranke $N \in \mathbb{N}$, so dass*

$$\begin{aligned} \textit{entweder:} \quad & \forall\, n > N : a_n > b \\ \textit{oder:} \quad & \forall\, n > N : a_n < b \end{aligned}$$

Schreibweise. Sei $(a_n)_{n\in\mathbb{N}}$ ein Cauchyfolge, $b \in \mathbb{Q}_+$ und $b \neq \lim(a_n)_{n\in\mathbb{N}}$. Schreibe:

$$b > (a_n)_{n\in\mathbb{N}} \quad \text{falls} \quad \forall i > N : b > a_i$$
$$b < (a_n)_{n\in\mathbb{N}} \quad \text{falls} \quad \forall i > N : b < a_i$$

5.1.6 Folgerung. *Jede Cauchyfolge, welche nicht konvergiert teilt $\mathbb{Q}$ in zwei Teilmengen:*

$$\mathbb{Q} = A \dot\cup B$$

wobei

$$A = \{b \in \mathbb{Q} : b < (a_n)_{n\in\mathbb{N}}\}$$
$$B = \{b \in \mathbb{Q} : b > (a_n)_{n\in\mathbb{N}}\}$$

Dann folgt: $\forall\, a \in A, b \in B : a < b$.

5.1.7 Satz (Beschränktheit der Cauchyfolgen)**.** *Jede Cauchyfolge ist beschränkt, d.h. finde ein $s \in \mathbb{Q}_+$, so dass*

$$(a_n)_{n\in\mathbb{N}} \subset [-s, s]$$

Beweis. □

5.1.8 Definition (Dedekindscher[10] Schnitt)**.** *Eine Teilmenge S von $\mathbb{Q}_+$ heißt (Dedekindscher) Schnitt, falls die folgende Eigenschaften hat:*

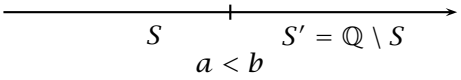
(i) $S \neq \emptyset, S \neq \mathbb{Q}$

(ii) $\forall\, a \in S, b \in S' := \mathbb{Q} \setminus S$ gilt $a < b$.

(iii) S enthält kein größtes Element, d.h. $\forall\, x \in S$ existiert ein $y \in S$ mit $y > x$.

[10] Richard DEDEKIND 1831-1916: Braunschweig, Göttingen, Zürich

Anschaulich. Ein Dedekindscher Schnitt S ergibt eine Partition von $\mathbb{Q}$:



Folgerung. *Jede Cauchyfolge ergibt einen Dedekindschen Schnitt: Gegeben sie eine Cauchy-Folge $(a_n)_{n\in\mathbb{N}}$. Es gibt zwei Fälle zu unterscheiden:*

(i) $(a_n)_{n\in\mathbb{N}}$ *konvergiert gegen eine rationale Zahl a. In diesem Fall sei*

$$S := \{x \in \mathbb{Q} : x < a\}$$
$$S' = \{x \in \mathbb{Q} : x \geq a\}$$

(ii) $(a_n)_{n\in\mathbb{N}}$ *konvergiert nicht. Dann sei*

$$S = \{a \in \mathbb{Q} : a < (a_n)_{n\in\mathbb{N}}\}$$

5.1.9 Definition und Satz (Summe und Produkte von Cauchyfolgen)**.** *Seien $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}} \subset \mathbb{Q}$ zwei Cauchyfolgen. Dann definiere:*

$$(a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}} := (a_n + b_n)_{n\in\mathbb{N}}$$
$$-(a_n)_{n\in\mathbb{N}} := (-a_n)_{n\in\mathbb{N}}$$
$$(a_n)_{n\in\mathbb{N}} \cdot (b_n)_{n\in\mathbb{N}} := (a_n \cdot b_n)_{n\in\mathbb{N}}$$

Das Ergebnis ist wieder eine Cauchyfolge.

Beweis. □

5.1.10 Satz. *Sei $(a_n)_{n\in\mathbb{N}}$ eine Cauchyfolge, die nicht gegen 0 konvergiert. Dann existiert ein $s \in \mathbb{Q}_+$ und ein $N \in \mathbb{N}$ mit*

$$\forall\, n > N : |a_n| \geq s$$

Beweis. □

Ergänzung. Genauer findet man s, N sodass entweder

(i) $a_n \geq s$ für alle $n > N$, oder

(ii) $a_n \leq -s$ für alle $n > N$.

Diese präzisere Fassung bei der Definition positiver reeller Zahlen benötigt man in Abschnitt 5.3. Man muss dort zeigen dass die Definition der Positivität unabhängig ist von der Wahl der Cauchyfolge, welche eine reelle Zahl definiert.

Betrachtet man *äquivalente* Cauchyfolgen, dann ist aber klar: Entweder genügen beide der Eigenschaft (i), oder beide genügen der Eigenschaft (ii).

5.1.11 Folgerung (Das Inverse)**.** *Sei $(a_n)_{n\in\mathbb{N}}$ eine Cauchyfolge mit den Eigenschaften*

(i) $\forall\, n : a_n \neq 0$

(ii) $(a_n)_{n\in\mathbb{N}}$ *konvergiert nicht gegen* 0.

Dann ist auch $(a_n^{-1})_{n\in\mathbb{N}}$ eine Cauchyfolge.

Beweis. □

5.2 Definition der reellen Zahlen

Definition. *Es sei $\mathcal{F}$ die Menge aller Cauchyfolgen $(a_n)_{n\in\mathbb{N}} \subset \mathbb{Q}$ rationaler Zahlen.*

5.2.1 Satz. *Die Menge $\mathcal{F}$ ist ein kommutativer Ring mit Einselement.*

(i) $(a_n)_{n\in\mathbb{N}} \pm (b_n)_{n\in\mathbb{N}} := (a_n \pm b_n)_{n\in\mathbb{N}}$

(ii) $(a_n)_{n\in\mathbb{N}} \cdot (b_n)_{n\in\mathbb{N}} := (a_n b_n)_{n\in\mathbb{N}}$

(iii) Nullfolge: $O_{\mathcal{F}} := (0)_{n\in\mathbb{N}} = (0,0,\dots)$

(iv) Einsfolge: $1_{\mathcal{F}} := (1)_{n\in\mathbb{N}} = (1,1,\dots)$

Es sei $\mathcal{F}_0$ die Menge aller Cauchy-Folgen, welche gegen Null konvergieren. Dann ist $\mathcal{F}_0$ ein Ideal im Ring $\mathcal{F}$.

Beweis. □

5.2.2 Definition und Satz (Körper der reellen Zahlen)**.** *Der Faktorring*

$$\mathbb{R} := \mathcal{F}/\mathcal{F}_0$$

(Ring aller Cauchyfolgen modulo Ideal der Nullfolgen) ist wohldefiniert und bildet einen Körper, den wir als den Körper der reellen Zahlen bezeichnen.

Beweis. □

22. VL
23.01.06

5.2.3 Satz (Einbettung von $\mathbb{Q}$ in $\mathbb{R}$)**.** *Wir betrachten zwei Abbildungen:*

$$\Delta : \mathbb{Q} \to \mathcal{F}$$
$$q \mapsto \Delta q := (q, q, q, \dots) \text{ konstante Folge}$$
$$\lim : \mathcal{F} \to \mathbb{R} = \mathcal{F}/\mathcal{F}_0$$
$$(a_n)_n \mapsto \lim a_n := [(a_n)_n] \text{ Äquivalenzklasse!}$$

Beide Abbildungen sind offensichtlich Homomorphismen von Ringen, d.h. vertragen sich mit $+, \cdot$. Die Hintereinanderausführung

$$\iota := \lim \circ \Delta : \mathbb{Q} \to \mathbb{R}$$

ist ein Homomorphismus (von Ringen) von $\mathbb{Q}$ in den Körper $\mathbb{R}$. Die Abbildung ι ist injektiv.

Beweis. □

Bemerkung. Seien K und L zwei Körper (insbesondere Ringe), und sei $\phi : K \to L$ ein Ringhomomorphismus. Da es in einem Körper keine echten Ideale gibt, folgt aus dem Homomorphiesatz 3.6.8, dass die Abbildung ϕ entweder identisch 0 oder injektiv sein muss. Im zweiten Fall folgt dann aus 3.6.7(ii), dass $\phi(1) = 1$, und wegen uneingeschränkter Ausführbarkeit der Division auch

$$\phi(a^{-1}) = \phi(a)^{-1} \quad \forall\, a \neq 0, \in K$$

sein muss.

Dies trifft insbesondere auf $\iota : \mathbb{Q} \to \mathbb{R}$ zu.

5.2.4 Folgerung. *Sei $\alpha = \lim a_n \in \mathbb{R}$. Dann ist α genau dann von der Form $\alpha = \iota(q)$, wenn die Folge $(a_n)_n$ gegen die rationale Zahl q konvergiert.*

Beweis. □

5.3 Die Ordnungsrelation

5.3.1 Definition und Satz (positiv, $\mathbb{R}_+$)**.** *Sei $\alpha = \lim a_n \in \mathbb{R} = \mathcal{F}/\mathcal{F}_0$. Dann nennen wir α positiv, d.h. $\alpha \in \mathbb{R}_+$, in folgenden Fällen:*

(i) $\alpha = \iota(q)$, d.h. $(a_n)_n \to q$ mit $q \in \mathbb{Q}_+$.

(ii) α ist irrational und oberhalb einer Schranke N sind alle $a_n > 0$ (für $n > N$).

Beweis. Insbesondere ist hier zu zeigen, dass die Definition der Positivität von α unabhängig ist von der Wahl der Cauchyfolge mit der wir α repräsentieren. □

5.3.2 Folgerung (für Dedekind-Schnitte)**.** *Die Abbildung*

$$\textit{Cauchyfolge } (a_n) \mapsto \textit{ Dedekind-Schnitt } S$$

hängt nur von der Äquivalenzklasse der Cauchyfolge ab, d.h. wir bekommen eine Abbildung

$$\mathbb{R} \ni \alpha \mapsto S \in \textit{ Schnitt}$$

Beweis. □

5.3.3 Folgerung (Eigenschaften von $\mathbb{R}_+$)**.** *Wenn $\alpha, \beta \in \mathbb{R}_+$, dann sind auch $\alpha + \beta, \alpha \cdot \beta, \alpha : \beta := \alpha \cdot \beta^{-1}, \beta^{-1} \in \mathbb{R}_+$.*

Beweis. □

5.3.4 Folgerung (Trichotomie)**.** *Für alle $\alpha \in \mathbb{R}$ gilt entweder $\alpha \in \mathbb{R}_+$, oder $\alpha = 0$ oder $-\alpha \in \mathbb{R}_+$.*

$$\mathbb{R} = \mathbb{R}_+ \dot\cup\, 0 \,\dot\cup -\mathbb{R}_+$$

Beweis. □

5.3.5 Definition und Satz (Ordnung)**.**

$$\alpha > \beta \quad :\Leftrightarrow \quad \alpha - \beta \in \mathbb{R}_+$$

Aus den Eigenschaften von $\mathbb{R}_+$ folgen Eigenschaften der Ordnung, z.B.

$$\alpha > \beta > \gamma \quad \Rightarrow \quad \alpha > \gamma \qquad \text{(Transitivität)}$$

Aus der Trichotomie folgt: Für je zwei Zahlen α, β gilt stets: Entweder

$$\alpha < \beta \quad \textit{oder} \quad \alpha = \beta \quad \textit{oder} \quad \beta < \alpha$$

Damit ist $\alpha \leq \beta$ eine Totalordnung auf $\mathbb{R}_+$.

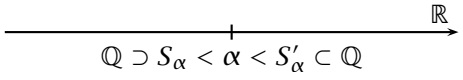
Beweis. □

5.3.6 Folgerung. *Die Abbildung $\mathbb{R} \ni \alpha \mapsto S_\alpha \in$ Schnitt ist injektiv.*

Beweis. □

23. VL
24.01.06

Anschaulich. Wenn man α als Punkt des Zahlenstrahls auffasst, dann ist S_α die Menge aller *rationaler* Punkte links von α. Man kann sich den Schnitt auch als Paar vorstellen, bestehend aus S_α und dem Komplement $S'_\alpha = \mathbb{Q} - S_\alpha$.



5.3.7 Definition und Satz (Gaußklammer für $\mathbb{R}$)**.** *Jedes $\alpha \in \mathbb{R}$ bestimmt eindeutig eine ganze Zahl $\lfloor \alpha \rfloor \in \mathbb{Z}$, so dass $\lfloor \alpha \rfloor \leq \alpha < \lfloor \alpha \rfloor + 1$.*

Beweis. □

5.4 Der Absolutbetrag und Konvergenz

5.4.1 Definition ($|\cdot|$, sgn)**.** *Für $\alpha \in \mathbb{R} = \mathcal{F}/\mathcal{F}_0$ setzen wir*

$$|\alpha| := \begin{cases} \alpha & \text{falls } \alpha \geq 0 \\ -\alpha & \text{falls } \alpha < 0 \end{cases}$$

und für $\alpha \neq 0$

$$\operatorname{sgn}(\alpha) := \begin{cases} 1 & \text{falls } \alpha > 0 \\ -1 & \text{falls } \alpha < 0 \end{cases}$$

5.4.2 Satz. *Es sei $\alpha = \lim a_n \in \mathbb{R}$. Dann gilt:*

$$|\lim a_n| = \lim |a_n|$$

Beweis. □

5.4.3 Folgerung. *(i) Für $\mathbb{Q} \ni q \mapsto \iota(q) = \lim \Delta q \in \mathbb{R}$ gilt*

$$|\iota(q)|_{\mathbb{R}} = \iota(|q|_{\mathbb{Q}})$$

(ii) Der Absolutbetrag reeller Zahlen hat die üblichen Eigenschaften:

$$\begin{aligned} |\alpha| = 0 \quad &\Leftrightarrow \quad \alpha = 0 \\ |\alpha\beta| &= |\alpha||\beta| \\ |\alpha + \beta| &\leq |\alpha| + |\beta| \\ ||\alpha| - |\beta|| &\leq |\alpha - \beta| \end{aligned}$$

Beweis. □

5.4.4 Definition (Konvergenz und Cauchyfolge in $\mathbb{R}$)**.** *Eine Folge reeller Zahlen $(\alpha_n)_n$ konvergiert gegen $\alpha \in \mathbb{R}$, falls zu jeden $\varepsilon \in \mathbb{R}_+$ ein $N = N(\varepsilon) \in \mathbb{N}$ existiert, so dass*

$$\forall\, n > N : |\alpha - \alpha_n| < \varepsilon$$

$(\alpha_n)_n$ heißt Cauchyfolge, falls zu jedem $\varepsilon \in \mathbb{R}_+$ ein $N = N(\varepsilon) \in \mathbb{N}$ existiert, so dass

$$\forall\, n, m > N : |\alpha_n - \alpha_m| < \varepsilon$$

Bemerkung. Es genügt immer, sich auf $\varepsilon \in \mathbb{Q}_+$ zu beschränken, weil zu jedem $\varepsilon \in \mathbb{R}_+$ man ein $\varepsilon' \in \mathbb{Q}_+$ findet mit $\varepsilon' < \varepsilon$.

Nächstes Ziel. Unser rein formal definierter Limes $\alpha = \lim_n a_n$ kann jetzt als echter Limes interpretiert werden.

5.4.5 Satz. *Es sei $\alpha \in \mathbb{R}$ und es sei $(a_n)_n$ eine Folge rationaler Zahlen. Dann ist folgendes äquivalent:*

(i) $(a_n)_n$ ist Cauchyfolge und $\alpha = \lim_n(a_n)$ im formalen Sinne (Äquivalenzklasse der Cauchyfolge).

(ii) Die Folge $(\iota(a_n))_n \subset \mathbb{R}$ konvergiert (im Sinne von 5.4.4) gegen $\alpha \in \mathbb{R}$.

Beweis. □

5.4.6 Satz (Vollständigkeitssatz)**.** *Der Körper $\mathbb{R}$ ist vollständig, d.h. jede Cauchyfolge reeller Zahlen konvergiert gegen eine reelle Zahl.*

Beweis. □

5.5 Unendliche Positionsbrüche

24. VL
30.01.06

Fixiere Basiszahl $g > 1, \in \mathbb{N}$. Ziffernsystem $M_g = \{0, 1, \ldots, g-1\}$. Sei $(a_n)_n \subset M_g$ eine Folge von Ziffern, alle $a_n \in M_g$. Bilde dazu die Folge

$$A_n := \sum_{i=1}^{n} a_i g^{-i} = \frac{a_1}{g} + \frac{a_2}{g^2} + \frac{a_3}{g^3} + \cdots$$

5.5.1 Satz. *Die Partialsummenfolge $(A_n)_n$ ist monoton wachsend und nach oben beschränkt, also eine Cauchyfolge rationaler Zahlen.*

Beweis. □

5.5.2 Definition (Positionsbruch)**.** *Wir schreiben dafür*

$$\alpha = \sum_{i=i}^{\infty} a_i g^{-i}$$

5.5.3 Bemerkung. Es gilt

$$\sum_{i=1}^{\infty} \frac{g-1}{g^i} = \lim_n \left(1 - \frac{1}{g^n}\right) = 1$$

Das ergibt eine Zweideutigkeit, nämlich wenn $\sum_{i=1}^{\infty} a_i g^{-i}$ die Eigenschaft hat $a_m < g - 1$ und $a_i = g - 1 \forall\, i > m$:

$$\sum_{i=1}^{\infty} a_i g^{-i} = \sum_{i=1}^{m-1} a_i g^{-i} + \frac{a_{m+1}}{g^m}$$

Definition. *Der Positionsbruch $\alpha = \sum_{i=1}^{\infty} a_i g^{-i}$ heißt zulässig, falls es kein m gibt, so dass $a_n = g-1 \forall\, n > m$.*

5.5.4 Satz (Eindeutige Darstellung)**.** *Jede reelle Zahl α, $0 \leq \alpha < 1$, besitzt eine eindeutige Darstellung als zulässiger Positionsbruch $\alpha = \sum_{i=1}^{\infty} a_i g^{-i}$.*

Beweis. □

Zusatz. Ist α eine beliebige reelle Zahl, dann erhält man die Positionsbruchentwicklung aus der Zerlegung

$$\alpha = [\alpha] + (\alpha - [\alpha])$$

in den ganzen Anteil und einen Rest der zwischen 0 und 1 liegt.

5.6 Beschränkte Zahlenmengen und Axiomatisierung der reellen Zahlen

5.6.1 Definition (Obere, untere Schranke)**.** *Eine Menge $\mathcal{M}$ reeller Zahlen heißt nach oben beschränkt, falls ein $s \in \mathbb{R}$ existiert, so dass $\alpha \leq s \forall\, \alpha \in \mathcal{M}$. s heißt dann obere Schranke von $\mathcal{M}$. Entsprechend: untere Schranke.*

5.6.2 Lemma. *Sei S die Menge aller oberer Schranken von $\mathcal{M}$. Ist $(s_n)_n$ eine konvergente Folge oberer Schranken, dann ist auch $s = \lim_n s_n$ ein obere Schranke für $\mathcal{M}$.*

Beweis. □

5.6.3 Satz. *Sei $\mathcal{M}$ eine nichtleere, nach oben beschränkte Teilmenge von $\mathbb{R}$. Dann gibt es unter den oberen Schranken von $\mathcal{M}$ eine kleinste Schranke s_0, d.h. s_0 = obere Schranke von $\mathcal{M}$ mit $s_0 \leq s \forall\, s$.*

Beweis. □

5.6.4 Satz (Variante)**.** *Sei $\mathcal{M}$ eine nichtleere, nach unten beschränkte Teilmenge von $\mathbb{R}$. Dann gibt es unter den unteren Schranken eine größte.*

Beweis. 5.6.3 und 5.6.4 sind äquivalent: ersetze $\mathcal{M}$ durch $-\mathcal{M}$. □

Definition (Häufungspunkt)**.** *$\mathcal{M} \subset \mathbb{R}$ sei eine unendliche Menge. $\alpha \in \mathbb{R}$ heißt Häufungspunkt von $\mathcal{M}$, falls zu jedem $\varepsilon > 0$ unendliche viele $\beta \in \mathcal{M}$ mit $|\alpha - \beta| < \varepsilon$ existieren.*

5.6.5 Satz. *Sei $\mathcal{M}$ unendliche Menge in $\mathbb{R}$. Dann ist folgendes äquivalent:*

(i) $\mathcal{M}$ hat einen Häufungspunkt.

(ii) Es gibt eine konvergente Folge $(\alpha_n)_n$ von Zahlen aus $\mathcal{M}$, welche nicht stabilisiert. (Stabilisierend: alle $\alpha_n = \alpha_{n+1}$ für $n > N$.)

Beweis. □

5.6.6 Satz (Bolzano-Weierstraß)**.** *Sei $\mathcal{M}$ unendliche Menge reeller Zahlen und $\mathcal{M} \subseteq [\alpha, \beta]$. Dann hat $\mathcal{M}$ einen Häufungspunkt $h \in [\alpha, \beta]$.*

Beweis. □

25. VL
31.01.06

5.6.7 Satz (Umkehrsatz)**.** *Wenn jede nichtleere, nach oben beschränkte Teilmenge ein Supremum (kleinste obere Schranke) hat, dann muss jede Cauchyfolge konvergieren.*

Beweis. □

5.6.8 Definition und Satz (Axiomatische Einführung von $\mathbb{R}$)**.**

(A1) $\mathbb{R}$ ist ein Körper mit $1 \neq 0$ (also ein echter Körper).

(A2) $\mathbb{R}$ besitzt einen Positivbereich $\mathbb{R}_+$, so dass

a) Trichotomie: $\mathbb{R} = \mathbb{R}_+ \dot\cup\, 0 \,\dot\cup -\mathbb{R}_+$

b) $\mathbb{R}_+$ ist abgeschlossen bezüglich $+$ und $\cdot$.

(A3) Jede nichtleere nach oben beschränkte Teilmenge von $\mathbb{R}$ hat ein Supremum. (äquivalent: Infimumeigenschaft)

Behauptung: Dieses $\mathbb{R}$ ist das von uns konstruierte.

Beweis. □

Weitere Schritte in der Analysis.

(i) Stetigkeitsbegriff reeller Funktionen.

(ii) Eigenschaften: f, g stetig $\Rightarrow c \cdot f, f+g, f \cdot g, f/g$ (dort, wo g keine Nullstelle hat) wieder stetig.

$f(x) = x$ stetig $\Rightarrow$ alle Polynome und alle rationalen Funktionen sind stetig (Nenner beachten).

(iii) Zwischenwertsatz und Existenz der Umkehrfunktion. f stetig und echt monoton $\Rightarrow$ Umkehrfunktion g stetig und echt monoton, d.h. $f(g(x)) = g(f(x)) = x$.

Anwendung auf Zahlen. Betrachte $f(x) = x^n$ für $n \in \mathbb{Z}, n \neq 0$ ist stetig und echt monoton. Also existiert die Umkehrfunktion $g(x) = \sqrt[n]{x}$.

Damit können wir für jedes $\alpha > 0$ und jedes $r = \frac{a}{b} \in \mathbb{Q}$ auch

$$\alpha^r = \sqrt[b]{\alpha^a} = \left(\sqrt[b]{\alpha}\right)^a$$

eindeutig bilden.

Sei β = reell = Limes einer Cauchyfolge rationaler Zahlen $(q_n)_n$. Alle α^{q_1} sind bereits erklärt und bilden wieder eine Cauchyfolge. Also ist

$$\alpha^\beta := \lim_n (\alpha^{q_n})$$

für $\alpha > 0, \beta \in \mathbb{R}$ wohldefiniert.

Betrachte die Funktion ($\alpha > 0$)

$$\mathbb{R} \ni x \mapsto \alpha^x \in \mathbb{R}$$

Diese Funktion ist stetig und monoton. Daher existiert eine eindeutig bestimmte Umkehrfunktion $\log_\alpha$.

6 p-adische Zahlen

6.1 Ganze p-adische Zahlen

Grundgedanke. Sei p eine fixierte Primzahl. Dann nennen wir zwei ganze Zahlen *dicht* beieinander, falls ihre Differenz durch eine hohe Potenz von p teilbar ist.

	gewöhnliche Metrik	p-adische Metrik
Cauchy-Folgen	$\lvert x_m - x_n\rvert < \varepsilon$ $\forall m, n > N$	Für alle n ist $x_{n-1} - x_n$ durch p^n teilbar: $x_{n-1} \equiv x_n \mod p^n$
Nullfolgen $\mathcal{F}_0$	$\lvert x_n\rvert \leq \varepsilon$ $\forall n > N$	Für alle n ist x_{n-1} durch p^n teilbar $x_{n-1} \equiv 0 \mod p^n$

6.1.1 Lemma ($\mathcal{F}^p$ ist ein Ring)**.** *Die Menge $\mathcal{F}^p$ der p-adischen Cauchy-Folgen $(x_n)_{n=0}^\infty$ von ganzen Zahlen ist ein Ring bezüglich komponentenweiser Addition und Multiplikation.*

$$\begin{aligned} &\textit{Nullelement:} && \Delta 0 = (0,0,0,\dots) \\ &\textit{Einselement:} && \Delta 1 = (1,1,1,\dots) \end{aligned}$$

Beweis. Sei $x = (x_n)_n$ und $y = (y_n)_n \in \mathcal{F}^p$, also für alle $n \in \mathbb{N}$

$$x_{n-1} \equiv x_n \mod p^n \quad y_{n-1} \equiv y_n \mod p^n$$

Dann ist auch für alle $n \in \mathbb{N}$:

$$\begin{aligned} x_{n-1} + y_{n-1} &\equiv x_n + y_n \mod p^n \\ y_{n-1} \cdot y_{n-1} &\equiv x_n \cdot y_n \mod p^n \end{aligned}$$

Also $x + y, x \cdot y \in \mathcal{F}^p$. Assoziativität, Kommutativität und Distributivität vererben sich, damit ist $\mathcal{F}^p$ ein Ring. □

6.1.2 Folgerung. *Die Menge $\mathcal{F}_0^p$ der p-adischen Nullfolgen bildet ein Ideal im Ring $\mathcal{F}^p$.*

Beweis. Beschreibung von $\mathcal{F}_0^p$: $\mathcal{F}_0^p \subset \mathcal{F}^p \subset \mathbb{Z}^{\mathbb{N}_0}$:

$$x_{n-1} \equiv 0 \mod p^n \quad \forall n \geq 1$$

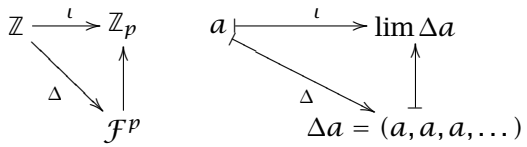
Also für $x \in \mathcal{F}_0^p$:

$$\begin{aligned} x &= (t_0 p, t_1 p^2, t_2 p^3, t_3 p^4, \dots) \\ &= \underbrace{(t_0, t_1, \dots)}_{\in \mathbb{Z}^{\mathbb{N}_0}} \cdot (p, p^2, p^3, \dots) \end{aligned}$$

$\mathcal{F}_0^p \subset \mathbb{Z}^{\mathbb{N}_0}$ ist also ein Hauptideal mit Erzeugendem $(p, p^2, p^3, \dots)$ und erst recht ein Ideal in $\mathcal{F}^p$. □

6.1.3 Definition. *Der Ring $\mathbb{Z}_p$ der ganzen p-adischen Zahlen ist definiert als $\mathbb{Z}_p := \mathcal{F}^p/\mathcal{F}_0^p$, d.h. $x \sim y \Leftrightarrow x - y \in \mathcal{F}_0^p$.*

6.1.4 Lemma (Einbettung von $\mathbb{Z}$)**.** *Wir betten $\mathbb{Z}$ folgendermaßen ein:*



Notation wie gehabt: Wenn $(x_n)_n \in \mathcal{F}^p$, schreibe $\lim x_n$ für die Äquivalenzklasse dieser Folge in $\mathbb{Z}_p$.

Behauptung: Die Abbildung $\iota : \mathbb{Z} \to \mathbb{Z}_p$ ist ein injektiver Ringhomomorphismus.

Beweis. Genügt zu zeigen: $\ker(\iota) = 0$. $\iota(a) = 0 \in \mathbb{Z}_p$ bedeutet $\Delta a \sim$ Nullfolge, d.h. $\Delta a \in \mathcal{F}_0^p$. $\Delta a = (a, a, a, \dots)$ bedeutet $p^n \mid a \forall n \in \mathbb{N}$. Dies geht nur, wenn $a = 0$ ist. □

6.1.5 Beispiel. Wir wollen $\sqrt{2}$ in $\mathbb{Z}_7$ berechnen. D.h.: Löse $\alpha^2 = \iota(2)$ in $\mathbb{Z}_7$. Es ist $\alpha = \lim x_n$, also $(x_n^2) - \Delta 2 \in \mathcal{F}_0^7$, d.h.

$$x_{n-1}^2 - 2 \equiv 0 \mod 7^n \quad \forall n \in \mathbb{N}$$

Beginne mit $n = 1$:

$$x_0^2 \equiv 2 \mod 7$$

Nimm $x_0 = 3$.

Induktionsvoraussetzung: Gegeben sei x_{n-1}, so dass

$$x_{n-1}^2 \equiv 2 \mod 7^n$$

Suche $x_n \in \mathbb{Z}$ mit

$$x_n^2 \equiv 2 \mod 7^{n+1} \qquad (*)$$

Wir brauchen auch

$$x_{n-1} \equiv x_n \mod 7^n$$

denn $(x_n)_n$ soll Cauchy-Folge sein. Ansatz:

$$x_n \equiv x_{n-1} + t_n 7^n \mod 7^{n+1}$$
$$x_n^2 \equiv x_{n-1}^2 + 2x_{n-1}t_n 7^n \mod 7^{n+1}$$

Gehe mit diesem Ansatz in $(*)$ und versuche t_n zu finden.

$$\frac{x_{n-1}^2 - 2}{7^n} \equiv -2x_{n-1}t_n \mod 7$$

Da $(x_0, x_1, ..., x_{n-1})$ schon der Anfang einer Cauchyfolge ist, gilt:

$$-2x_{n-1} \equiv -2x_0 = 1 \mod 7$$

also

$$t_n \equiv \frac{x_{n-1}^2 - 2}{7^n} \mod 7$$

leistet das Verlangte.

6.2 Der Körper der p-adischen Zahlen

Wir haben gesehen, dass $\mathbb{Z}_p$ ein nullteilerfreier Ring ist, sogar faktoriell. Also können wir Quotienten bilden.

Literatur

[Koc04] KOCH, HELMUT: *Einführung in die Mathematik. Hintergründe der Schulmathematik*. Springer, Berlin, 2004. ISBN: 3-540-20391-5. Besonders für Kapitel 2 und 5 des Skripts.

[Lan04] LANDAU, EDMUND: *Grundlagen der Analysis (Das Rechnen mit ganzen, rationalen, irrationalen, komplexen Zahlen.)*. Heldermann Verlag, 2004. ISBN: 3-88538-111-7. Dies ist der Klassiker: Landau erstellte als erster einen „keinen Schluss auslassenden Aufbau der Arithmetik der reellen und komplexen Zahlen von der axiomatischen Einführung der natürlichen Zahlen aus zum einzigen Gegenstand“ und entwickelt damit das Fundament auf der die Analysis aufgebaut werden kann. Es erschien 1930 in der Akademische Verlagsgesellschaft, Leipzig.

[Leu96] LEUTBECHER, ARMIN: *Zahlentheorie. Eine Einführung in die Algebra*. Springer, Berlin, 1996. ISBN: 3-540-58791-8.

[RS05] REISS, KRISTINA und GERALD SCHMIEDER: *Basiswissen Zahlentheorie. Eine Einführung in Zahlen und Zahlbereiche*. Springer, Berlin, 2005. ISBN: 3-540-21248-5.

Index