Vorschau- und Einstiegskurs für das erste Semester im Mathematik-Studium

K. Ihsberner

Universität Rostock

01.,02.,08.,09.10.2015

Herzlich Willkommen zum Vorschau- und Einstiegskurs!

Organisatorisches

Der Vorkurs geht über vier Tage (01.-02. sowie 08.-09.10.2015) und ist in drei verschiedene Veranstaltungstypen unterteilt (Kurzvorlesungen, Übungen und Tutorien).

- In den Kurzvorlesungen werden grundlegende Themen, die üblicherweise in der Schule zu kurz kommen, aufgegriffen und auf Universitätsniveau erläutert.
- In den Übungen können Sie sich mit den vorgestellten Begriffen durch selbständige Bearbeitung von leichten wie auch etwas anspruchsvolleren Aufgaben vertraut machen.
- In den Tutorien können aufgetretene Verständnisprobleme anhand von Beispielen/Erläuterungen angegangen werden.

Hinweise zum Studium – Aufbau einer Lehrveranstaltung

- Eine mathematische Lehrveranstaltung besteht üblicherweise aus sukzessive aufeinander aufbauenden Vorlesungen sowie begleitenden Übungen sowie gegebenenfalls Tutorien.
- Vorlesungen führen **ständig neues** mathematisches Wissen ein, üblicherweise wird **nichts** wiederholt – dies zu tun liegt in der Verantwortung der Studierenden selbst (Nacharbeiten!).
- **Jede Woche** findet (mindestens) eine Übung statt, in der anhand von Beispielaufgaben neue und alte Begriffe gefestigt werden sollen – für das **obligatorische Hausaufgabenblatt** haben Sie ca. eine Woche zur selbständigen Bearbeitung Zeit.
- In den Tutorien können gezielt Themengebiete vertieft werden, die besonders wichtig bzw. besonders schwer zugänglich sind.

Hinweise zum Studium - Tipps zur Vorlesung

- Fragen Sie den jeweiligen Dozenten, nach welchem Buch oder Skript er sich richtet bzw. nach weiterführender Literatur.
- Bereiten Sie die Vorlesungen vor und nach, versuchen Sie insbesondere, alle Schritte eines Beweises/einer Herleitung nachzuvollziehen. Lernen Sie weiter alle eingeführten Begriffe inklusive mindestens eines Beispiels und eines Gegenbeispiels auswendig und wiederholen Sie diese regelmäßig.
- Besuchen Sie jede Vorlesung – durch Fehlen in bzw. fehlendes Nacharbeiten einer Veranstaltung können – auch schon ab der ersten Woche – große Verständnisprobleme auftreten.
- Besorgen Sie sich eine Übersicht über alle Ihnen noch unbekannten Symbole mit deren Erklärungen (inklusive des griechischen Alphabetes). **Fragen Sie** im Zweifel **sofort nach**, wenn in einer Veranstaltung ein neues Symbol auftaucht.

Aufbau einer Vorlesung – auftretende Module (Bausteine)

- **Axiom** – Aussage, auf deren Richtigkeit man sich einigt.
- **Definition** – klare Festlegung eins Fachbegriffes (Vokabel!)
- **Beispiel** – konkretes Objekt, welches eine Aussage erfüllt.
- **Satz** – Aussage, welche etwa durch Anwendung von Axiomen/Definitionen bewiesen werden muss.
- **Lemma** (Hilfssatz) – Aussage, deren Richtigkeit insbesondere für den Beweis späterer Aussagen benötigt wird.
- **Corollar** (Folgerung) – Aussage, deren Richtigkeit sich direkt als Anwendung eines vorangegangenen Satzes ergibt.

Tipp: Versuchen Sie, während der Vorlesung mitzudenken – dann geht das Mitschreiben viel schneller und ist weniger anstrengend.

Hinweise zum Studium - Tipps zur Übung/zum Übungsblatt

- Bereiten Sie die Übungen vor, in dem Sie zumindest den aktuellen Vorlesungsstoff wiederholen und sich die wichtigsten neu eingeführten Begriffe in Erinnerung rufen.
- Bereiten Sie die Übungen nach, in dem Sie alle bereitgestellten Materialien/Musterlösungen noch einmal durchgehen – fangen Sie erst **danach** an, das Hausaufgabenblatt zu bearbeiten.
- Versuchen Sie, möglichst **jedes** Übungsblatt zu einem möglichst hohen Anteil **selbständig** zu bearbeiten.
- Lassen Sie sich **nicht** entmutigen, wenn Sie die Lösung einer Aufgabe nach zwei Stunden noch nicht heraus haben. Erklären Sie sich gegenseitig Ihre Lösungen/Lösungsansätze – lassen Sie Ihre Kommilitonen kritisch Ihre Lösungswege hinterfragen.

Hinweise zum Studium - Allgemeines

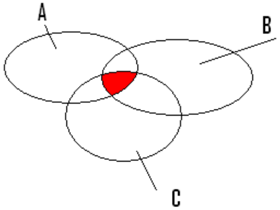
- Nutzen Sie bereits diesen Vorschau- und Einstiegskurs, um Ihre Kommilitonen kennenzulernen und gegebenenfalls schon Lern- bzw. Diskussionsgruppen zu bilden.
- Notieren Sie sich stets alle aufgetretenen Fragen und Probleme, damit wir auf diese in den Übungen und insbesondere in den Tutorien eingehen können.
- Lernen Sie Ihren Fachschaftsrat Sigma (Σ) kennen, er kann im Zweifelsfall vermitteln, falls Sie uns nicht direkt fragen wollen.
- Falls Sie es noch nicht getan haben – holen Sie sich beim IMTZ einen kostenlosen studentischen Email-Account, mit diesem können Sie sich auf der Lernplatform StudIP anmelden.

Und nun Vorsicht – ähm – viel Spaß beim Einstieg!

Programm: 1. Teil – Aussagen, Quantoren und Mengen

In der ersten Kurzvorlesung wollen wir uns mit **Aussagen und Mengen** beschäftigen, allerdings vermutlich auf präzisere Weise, als Sie dies – wenn überhaupt – in der Schule kennengelernt haben.

Dabei wollen wir insbesondere mathematische Symbole aus der Logik und Mengenlehre kennenlernen, welche das Fundament der Sprache der Mathematik bilden.



1.1 Aussagen

Zunächst wollen wir klären, wie man mathematische Aussagen bilden kann.

Variablen, Konstanten, Funktionen, Relationen

In der mathematischen Sprache erlaubt man sich,

- Symbole für **Variablen** (meist $x, y, \ldots$ oder $x_1, x_2, \ldots$)
- Symbole für **Konstanten** (meist $c, d, \ldots$),
- Symbole für n-stellige **Funktionen** (meist $f(\cdot, \ldots, \cdot), g(\cdot, \ldots, \cdot), \ldots$) und
- Symbole für n-stellige **Relationen** (meist $R(\cdot, \ldots, \cdot), S(\cdot, \ldots, \cdot), \ldots$)

zu verwenden.

Terme und grundlegende Aussagen

Mittels dieser Symbole kann man Terme und Aussagen (auch **Formeln** genannt) bilden:

- Jede Variable und jede Konstante ist ein Term.
- Sind $t_1, \dots, t_n$ Terme und ist f eine n-stellige Funktion, so ist auch $f(t_1, \dots, t_n)$ ein Term.
- Sind $t_1, \dots, t_n$ Terme und ist R eine n-stellige Relation, dann ist $R(t_1, \dots, t_n)$ eine Aussage, in der alle vorkommenden Variablen **frei** sind.

Beispiel (Terme)

Seien t_1, t_2 Terme.

- Benutzt man für die zweistelligen Funktionen „plus“ oder „mal“ die Symbole $+$ und $\cdot$, dann sind $+(t_1, t_2)$ und $\cdot(t_1, t_2)$ neue Terme, für die man auch $\boxed{t_1 + t_2}$ und $\boxed{t_1 \cdot t_2}$ schreibt.
- Konkret sind a oder 5 oder $x + 4$ oder $b \cdot (y + 7)$ Terme.

Beispiel (Aussagen)

Seien t_1, t_2 Terme.

- Benutzt man für die zweistelligen Relationen „ist gleich“ und „ist kleiner oder gleich“ die Symbole $=$ und $\leq$, dann sind $= (t_1, t_2)$ und $\leq (t_1, t_2)$ Aussagen, für die man üblicherweise einfach $\boxed{t_1 = t_2}$ und $\boxed{t_1 \leq t_2}$ schreibt.
- Konkret sind $a \leq 11$ oder $x = y + 8$ oder $0 \leq a \cdot a$ Aussagen.

Logische Verknüpfungen von Aussagen

Aus vorhandenen Aussagen kann man mittels logischer Symbole neue Aussagen bilden: Sind A und B Aussagen, dann sind auch

- $A \Longrightarrow B$ („A impliziert B")
- $A \wedge B$ („A und B")
- $A \vee B$ („A oder B")
- $\neg A$ („nicht A")

Aussagen. Abkürzend führt man noch

- $A \Longleftrightarrow B$ („A ist äquivalent zu B")

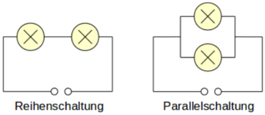
an Stelle von $(A \Longrightarrow B) \wedge (B \Longrightarrow A)$ ein.

Boolesche Logik

Als logische Axiome verlangen wir von jeder Aussage (mit belegten Variablen), dass sie entweder wahr oder falsch ist, und bei Bildung von neuen Aussagen ist deren Gültigkeit durch die folgenden Wahrheitstafeln festgelegt:

A	B	$A \implies B$	$A \wedge B$	$A \vee B$	$\neg A$	$\neg B$	$(\neg A) \vee B$
w	w	w	w	w	f	f	w
w	f	f	f	w	f	w	f
f	w	w	f	w	w	f	w
f	f	w	f	f	w	w	w

In der Technik kann die Aussage $A \wedge B$ mit einer Reihenschaltung und die Aussage $A \vee B$ mit einer Parallelschaltung realisiert werden.



Definition (Tautologie)

Eine Aussage, welche bei beliebiger Belegung der Variablen wahr ist, nennen wir eine **Tautologie**.

Beispiel (Tautologie)

Die Aussage $(A \wedge B) \Longrightarrow A$ ist eine wahre Aussage, egal ob A, B wahre oder falsche Aussagen sind, denn sie besitzt die folgende Wahrheitstabelle

A	B	$A \wedge B$	$(A \wedge B) \Longrightarrow A$
w	w	w	w
w	f	f	w
f	w	f	w
f	f	f	w

Übungsaufgaben

1. Zeigen Sie für beliebige Aussagen A, B und C die Äquivalenzen:
   (a) Doppelte Negation: $\neg(\neg A) \iff A$
   (b) Kommutativgesetz: $A \wedge B \iff B \wedge A$
   $A \vee B \iff B \vee A$
   (c) Assoziativgesetz: $(A \wedge B) \wedge C \iff A \wedge (B \wedge C)$
   $(A \vee B) \vee C \iff A \vee (B \vee C)$
   (d) Distributivgesetz: $(A \wedge B) \vee (A \wedge C) \iff A \wedge (B \vee C)$
   $(A \vee B) \wedge (A \vee C) \iff A \vee (B \wedge C)$
   (e) De Morgansche Regeln: $\neg(A \wedge B) \iff (\neg A) \vee (\neg B)$
   $\neg(A \vee B) \iff (\neg A) \wedge (\neg B)$
2. Zeigen Sie für beliebige Aussagen A, B und C die Äquivalenzen
   (a) Kettenschluss: $(A \Longrightarrow B) \wedge (B \Longrightarrow C) \Longrightarrow (A \Longrightarrow C)$
   (b) Indirekter Beweis: $(\neg B) \Longrightarrow (\neg A) \iff (A \Longrightarrow B)$

1.2 Quantoren

Ist darüber hinaus x eine freie Variable in der Aussage A, so erlaubt man sich auch, mittels der Quantoren $\forall$ und $\exists$ die Aussagen

- $\forall x\colon A(x)$ („für jedes x gilt $A(x)$") und
- $\exists x\colon A(x)$ („es gibt (mindestens) ein x, für das $A(x)$ gilt")

zu bilden, und in diesen ist dann x keine freie Variable mehr, sondern **gebunden**.

Beispiel (Aussage mit Quantoren)

Ist x ein beliebiger Hund, die Aussage $A(x)$, dass der Hund bellt, und $B(x)$, dass der Hund beißt, so ist $\boxed{\forall x\colon\ (A(x) \Longrightarrow \neg B(x))}$ eine mathematische Formulierung des Sprichwortes

„Hunde, die bellen, beißen nicht."

Logische Axiome für Quantoren

Für Aussagen mit Quantoren verlangt man als logische Axiome die Gültigkeit von

- $(\forall x\colon A(x)) \Longrightarrow A(t)$,
- $A(t) \Longrightarrow (\exists x : A(x))$,
- $\forall x\colon (B \Longrightarrow A(x)) \Longrightarrow (B \Longrightarrow \forall x\colon A(x))$,
- $\forall x\colon (A(x) \Longrightarrow B) \Longrightarrow ((\exists x\colon A(x)) \Longrightarrow B)$,

wobei

- $A(x)$ eine Aussage mit freier Variable x,
- t einen Term und
- B eine Aussage, in der die Variable x nicht vorkommt,

bezeichnet.

Mathematische Theorien und formale Beweise

- Eine mathematische Theorie besteht aus einer wie eben konstruierten Sprache (mit festgelegten Konstanten-, Funktions- und Relationssymbolen), den logischen Axiomen und zusätzlich als gültig betrachteten nicht-logischen Axiomen.
- Ein Beweis einer Aussage innerhalb einer mathematischen Theorie ist eine Aneinanderreihung von Aussagen, von denen jede entweder ein (logisches oder nichtlogisches) Axiom der Theorie ist oder direkt mit Hilfe einer Tautologie aus vorher in der Aneinanderreihung vorkommenden Aussagen hervorgeht.

Hinweis – Erinnerung:

1. Eine Aussage der Form $A \iff B$ beweist man, indem man zuerst $A \implies B$ und dann $B \implies A$ zeigt.
2. Falls A falsch ist, so ist $A \implies B$ stets wahr.

Beispiel (Nicht-logische Axiome)

Für die zweistellige Relation $=$ werden die nicht-logischen Axiome

- $\forall x\colon x = x$ (reflexiv)
- $\forall x\colon \forall y\colon (x = y \Longrightarrow y = x)$ (symmetrisch)
- $\forall x\colon \forall y\colon \forall z\colon ((x = y) \wedge (y = z)) \Longrightarrow x = z$ (transitiv)

gefordert, ohne die $=$ eben nicht viel mit Gleichheit zu tun hätte.
Bem.: Wir werden später weitere aufgrund dieser drei Eigenschaften „Äquivalenzrelationen" genannte Relationen kennenlernen.

Beispiel (Beweis einer Aussage)

Eine Konsequenz der oben genannten Axiome ist beispielsweise die Aussage $\boxed{\forall x\colon \exists y\colon x = y}$. Denn ist x beliebig, folgt mit der Reflexivität $x = x$, also gilt für beliebiges x die Aussage $\exists y\colon x = y$ und somit auch $\forall x\colon \exists y\colon x = y$.

1.3 Mengen

Relationssymbol $\in$

Die Objekte, mit denen man sich in der Mathematik üblicherweise beschäftigt, sind Mengen. Dabei gibt man sich das zweistellige Relationssymbol $\in$ vor, mit dessen Hilfe man Aussagen wie $x \in y$ („x ist Element von y“) formen kann.

- **Wunsch:** Gerne würde man über die Menge aller x sprechen, für die eine bestimmte von der freien Variablen x abhängige Aussage $A(x)$ wahr wird.
- **Aber:** Dies führt zu logischen Widersprüchen, so dass man vorsichtig sein muss.

Wir vereinbaren die Abkürzung $\boxed{x \notin y}$ für die Aussage $\neg(x \in y)$.

Definition

- Ist $A(x)$ eine mathematische Aussage mit freier Variable x, so bezeichnet $\{x \mid A(x)\}$ einen Term mit **gebundener** Variable x, den man die **Ansammlung** (Klasse) aller x, für welche die Aussage $A(x)$ wahr ist, nennt.
- Als grundlegendes nicht-logisches Axiom gibt man sich dann

$$(y \in \{x \mid A(x)\}) \iff A(y)$$

vor, d.h. y ist genau dann ein Element von $\{x \mid A(x)\}$, wenn $A(y)$ gilt.

Gleichheit

Die zweistellige Relation $=$ definiert man mittels $\in$ durch das nicht-logische Axiom

$$x = y \iff \forall z\colon (z \in x \iff z \in y)$$

(Extensionalitätsaxiom).
Zwei Ansammlungen x und y sind also gleich, wenn jedes Element von x auch ein Element von y ist, und umgekehrt.

Beispiel (leere Klasse)

Ein Beispiel für eine Ansammlung (Klasse) ist die leere Klasse (Ansammlung)

$$\emptyset \;:=\; \{x \,|\, x \neq x\} \;:=\; \{x \,|\, \neg(x = x)\},$$

welche durch die Eigenschaft $\forall y\colon\, y \notin \emptyset$ charakterisiert ist.

Das Russelsche Paradoxon

Sei $K := \{x \mid x \notin x\}$, gilt dann $K \in K$ oder $K \notin K$?

Bezeichne $A(x)$ die Aussage $\neg(x \in x)$, dann ist $K = \{x \mid A(x)\}$.

- Wäre $K \in K$, dann müsste $A(K)$ gelten und damit $K \notin K$, Widerspruch.
- Wäre $K \notin K$, dann müsste $\neg A(K)$ gelten und somit $K \in K$, Widerspruch.

Als Ausweg aus diesem Dilemma betrachten wir nur noch spezielle Ansammlungen (Klassen), sogenannte Mengen. Genauer sieht man in der Theorie der Mengen also **nicht jeden Ausdruck der Form** $\{x \mid A(x)\}$ als Menge an, sondern nur noch spezielle Ausdrücke.

Mengen

Beispielsweise

- ist $\{\} := \emptyset$ eine Menge, die **leere Menge** genannt wird,
- ist mit zwei Mengen x, y auch die sogenannte **Paarmenge** $\{x, y\} := \{z \mid (z = x) \vee (z = y)\}$ eine Menge,
- ist mit einer Menge x bei $z \subset x$, d.h., $\forall u\colon\ (u \in z \Longrightarrow u \in x)$, auch z eine Menge (z wird **Teilmenge** von x genannt),
- sind mit zwei Mengen x, y auch

  $x \cup y := \{u \mid u \in x \vee u \in y\}$ (die **Vereinigungsmenge**)

  $x \cap y := \{u \mid u \in x \wedge u \in y\}$ (die **Schnittmenge**)

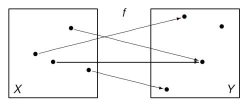
  Mengen,
- ist mit einer Menge x auch $\mathcal{P}(x) := \{z \mid z \subset x\}$ eine Menge, wobei $\mathcal{P}(x)$ die **Potenzmenge** von x genannt wird.

Produktmengen

Ähnlich wie Paarmengen kann man geordnete Paare und damit die (kartesische) **Produktmenge** $M \times N := \{(m,n) \mid m \in M, n \in N\}$ zweier Mengen M, N definieren.

Abbildungen

Eine Abbildung $f\colon M \to N$ kann man mengentheoretisch als eine Teilmenge $R \subset M \times N$ auffassen mit der Eigenschaft



$$\forall x \in M\ \exists!\, y \in N\colon (x,y) \in R\ ,$$

d.h., dass es zu jedem $x \in M$ genau ein $y \in N$ mit $(x,y) \in R$ gibt. Üblicherweise wird R der Graph von f genannt, und das zu $x \in M$ gehörige eindeutige Element $y \in N$ mit $(x,y) \in R$ bezeichnet man mit $f(x)$.

Beispiel (Mengen)

Für die Mengen $A = \{1, 5, 13\}$ und $B = \{13, 17\}$ erhalten wir

- $A \cap B = \{13\}$ und $A \cup B = \{1, 5, 13, 17\}$
- $A \times B = \{(1, 13), (1, 17), (5, 13), (5, 17), (13, 13), (13, 17)\}$
- $B \times A = \{(13, 1), (13, 5), (13, 13), (17, 1), (17, 5), (17, 13)\}$

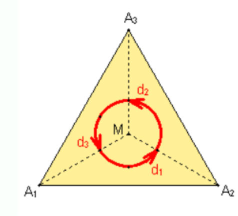
Beispiel (Abbildungen)

Für die Mengen $A = \{1, 2, 4\}$ und $B = \{0, 1, 4, 16\}$ ist etwa

- $R_1 = \{(1, 0), (2, 0), (4, 0)\} \subset A \times B$ der Graph einer Abbildung $f_1 \colon A \to B$, $x \mapsto 0$.
- $R_2 = \{(1, 1), (2, 4), (4, 16)\} \subset A \times B$ der Graph einer Abbildung $f_2 \colon A \to B$.

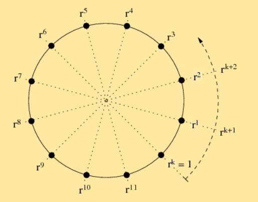
Programm: 2. Teil – Unendliche Mengen, Gruppen und die Uhrzeit

In dieser Kurzvorlesung wollen wir uns mit den naheliegendsten **Zahlenbereichen** beschäftigen.
Ausgehend von den natürlichen Zahlen diskutieren wir erste grundlegende algebraische Strukturen, welche Sie teilweise in der Schule als Rechengesetze oder auch im Alltag kennengelernt haben.



Verknüpfungstafel (Gruppentafel):

∘	i	d_1	d_2
i	i	d_1	d_2
d_1	d_1	d_2	i
d_2	d_2	i	d_1



$$\begin{array}{ccccc} 1 & + & 1 & = & 2 \\ 1 & + & 2 & = & 0 \end{array} \; ?$$

Unendliche Mengen

Die bisher angegebenen Axiome der Mengenlehre garantieren nicht die Existenz einer unendlichen Menge, wie z.B. der Menge der natürlichen Zahlen.
Deswegen fordern wir formell das nicht-logische Axiom

$$\exists x\colon\ (\emptyset \in x \land (\forall y\colon y \in x \Longrightarrow (y \cup \{y\}) \in x))\ ,$$

d.h., wir fordern als Axiom die Existenz einer induktiven Menge, also einer Menge, welche die leere Menge $\emptyset$ enthält und für die mit jedem Element y auch $y \cup \{y\}$ ein Element der Menge ist.

Die Menge $\mathbb{N}$ der natürlichen Zahlen

- Die Menge $\mathbb{N}$ der natürlichen Zahlen ist der Durchschnitt aller induktiven Mengen, d.h. die kleinste induktive Menge.
- Symbolisch kann man $\mathbb{N}$ als $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \dots\}$ schreiben, aber üblicherweise bezeichnet man die Elemente von $\mathbb{N}$ mit $1 := \emptyset$, $2 := \{\emptyset\}$, $3 := \{\emptyset, \{\emptyset\}\}$, ...
- Durch $s\colon \mathbb{N} \to \mathbb{N}$, $s(y) := y \cup \{y\}$, wird die sogenannte Nachfolgerabbildung auf $\mathbb{N}$ definiert, man schreibt auch kurz $n + 1 := s(n)$.
- Aufgrund der Definition der natürlichen Zahlen als kleinster induktiver Menge kann man Aussagen über natürliche Zahlen von der Form $\forall n \in \mathbb{N}\colon A(n)$ dadurch beweisen, dass man $A(1)$ und $\forall n \in \mathbb{N}\colon (A(n) \implies A(n+1))$ beweist. Dies nennt man einen Beweis der Aussage $\forall n \in \mathbb{N}\colon A(n)$ per Induktion.

Rechnen in $\mathbb{N}$ – Teil 1

- Mittels der Nachfolgerabbildung s kann man $m+n$ als n-malige Anwendung von s auf m definieren und erhält so eine Addition $+\colon \mathbb{N}\times\mathbb{N}\to\mathbb{N}$ mit den Eigenschaften, dass
  - $(k+m)+n = k+(m+n)$ (Assoziativität) und
  - $n+m = m+n$ (Kommutativität)

  für alle $k, m, n \in \mathbb{N}$ gilt.
- Als $(n-1)$-malige Anwendung von $k \mapsto k+m$ auf m erhalten wir analog eine Multiplikation $\cdot\colon \mathbb{N}\times\mathbb{N}\to\mathbb{N}$, $(m,n)\mapsto m\cdot n$ mit den Eigenschaften, dass für alle $k, m, n \in \mathbb{N}$
  - $1\cdot n = n$ (1 ist neutrales Element der Multiplikation),
  - $(k\cdot m)\cdot n = k\cdot(m\cdot n)$ (Assoziativität),
  - $n\cdot m = m\cdot n$ (Kommutativität) und
  - $(k+m)\cdot n = (k\cdot n)+(m\cdot n)$ (Distributivität)

  gilt.

Rechnen in $\mathbb{N}$ – Teil 2

- In gleicher Weise definieren wir als $(n-1)$-malige Anwendung von $k \mapsto k \cdot m$ auf m die *n-te Potenz* $\cdot^{\cdot} : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $(m, n) \mapsto m^n$ mit den Eigenschaften $n^1 = n$ und $k^{m+n} = k^m \cdot k^n$ für alle $k, m, n \in \mathbb{N}$.
- Man schreibt $m < n$, wenn n einer der Nachfolger von m ist, also n durch einfache oder mehrfache Anwendung der Nachfolger-Abbildung erhalten wird (für $m < n$ schreibt man oftmals auch $n > m$).
- Falls $m = n$ oder n einer der Nachfolger von m ist, schreiben wir auch abkürzend $m \leq n$ (analog verwenden wir $\geq$).

Rechnen in $\mathbb{Z}$

- Zu gegebenem $m, n \in \mathbb{N}$ kann man die Gleichung $k + m = n$ für k in $\mathbb{N}$ nur lösen, wenn $m < n$ gilt.
- **Ausweg:** Wir erweitern die Menge $\mathbb{N}$ um
  - ein neutrales Element der Addition, d.h., wir fügen ein Element $e_+ := 0$ hinzu, von dem wir verlangen, dass $\boxed{\forall n \in \mathbb{N} \colon e_+ + n = n + e_+ = n}$ erfüllt ist;
  - inverse Elemente der Addition, d.h., zu jedem Element $n \in N$ fügen wir ein Element $-n$ hinzu, für dass dann $n + (-n) = (-n) + n = e_+$ gilt;

  und setzen auf der Menge $\mathbb{Z} \ := \ \mathbb{N} \cup \{0\} \cup \{-n \mid n \in \mathbb{N}\}$ Addition und Multiplikation in verträglicher Weise fort.
- Die Lösung von $k + m = n$ zu vorgegebenen $m, n \in \mathbb{N}$ schreiben wir dann abkürzend als $k = n - m$ (für $n + (-m)$).

Oftmals haben wir viele Zahlen zu addieren oder zu multiplizieren.

Verwendung des Summen- und Produktzeichens

Sei $m, n \in \mathbb{N}$ mit $m \leq n$ und $a_m, \ldots, a_n$ Zahlen. Dann setzen bzw. vereinbaren wir

$$\sum_{k=m}^{n} a_k := a_m + a_{m+1} + \cdots + a_{n-1} + a_n \,, \qquad \sum_{k=1}^{0} a_k := 0 \,,$$

$$\prod_{k=m}^{n} a_k := a_m \cdot a_{m+1} \cdot \cdots \cdot a_{n-1} \cdot a_n \,, \qquad \prod_{k=1}^{0} a_k := 1 \,.$$

Beispiel

$$\sum_{k=5}^{8} k = 5 + 6 + 7 + 8 = 26, \qquad 5! := \prod_{k=1}^{5} k = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120.$$

Beim letzten Beispiel haben wir bereits verwendet, dass wir uns auf eine einheitliche Darstellung natürlicher Zahlen geeinigt haben.

Darstellung ganzer Zahlen zur Basis $b \in \mathbb{N}$

$$\pm a_n a_{n-1} \ldots a_2 a_1 a_0 := \pm \sum_{k=0}^{n} a_k b^k \quad n \in \mathbb{N}$$

mit Ziffernsymbolen $a_i \in \{0, ..., b-1\}$ für alle $i \in \{0, \ldots, n\}$.

- geläufige Basen sind z.B. 2, 10, 16 (vergleiche Dual-, Dezimal- und Hexadezimalsystem)
- $356 = 3 \cdot 10^2 + 5 \cdot 10^1 + 6 \cdot 10^0$
- $356 = 0x0164 = 1 \cdot 16^2 + 6 \cdot 16^1 + 4 \cdot 16^0$
- oder auch zur Basis 7, $356 = 1 \cdot 7^3 + 0 \cdot 7^2 + 1 \cdot 7^1 + 6 \cdot 7^0$

Definition (Gruppe)

- Eine Menge mit einer assoziativen Operation und einem neutralen Element, in der Inverse existieren, heißt Gruppe.
- Ist die Operation zusätzlich kommutativ, so spricht man von einer kommutativen (oder abelschen) Gruppe.

Beispiel (Gruppen)

- $(\mathbb{Z}, +, 0)$ ist eine kommutative Gruppe,
- $(\mathbb{Z} \setminus \{0\}, \cdot, 1)$ ist keine Gruppe, da für $m \notin \{-1, 1\}$ die Gleichung $m \cdot n = 1$ keine Lösung $n \in \mathbb{Z}$ besitzt.
- Die Gruppe der Drehungen um ein ganzzahliges Vielfaches von 120° (siehe vorne) ist eine Gruppe.
- Die kleinsten Gruppen sind $(\{0\}, +)$ oder $(\{1\}, \cdot)$.

Definition (Teilbarkeit, Primzahl)

- Es heißt $m \in \mathbb{Z}$ Teiler von $n \in \mathbb{Z}$, wenn ein $k \in \mathbb{Z}$ mit $k \cdot m = n$ existiert, man schreibt dann kurz $m|n$ („m teilt n“).
- $p \in \mathbb{N}$ heißt Primzahl, falls $p > 1$ und $n|p \Longrightarrow (n = 1 \vee n = p)$

Theorem

1. *Aus $m \cdot n = 0$ folgt $m = 0$ oder $n = 0$, d.h. $\mathbb{Z}$ ist nullteilerfrei.*
2. *Für jedes $n \in \mathbb{N}$ gilt $1|n$ und $n|n$.*
3. *Jedes $n \in \mathbb{N}$ besitzt eine eindeutige Primfaktorzerlegung, d.h., es gibt eindeutige Primzahlen $p_1, \ldots, p_m$ und Potenzen $i_1, \ldots, i_m \in \mathbb{N}$ mit $\boxed{n = \prod_{k=1}^{m} p_k^{i_k}}$.* (z.B.: $600 = 2^3 \cdot 3^1 \cdot 5^2$)

Programm: 3. Teil – Äquivalenzrelationen und Körper

In dieser Kurzvorlesung wollen wir uns mit der speziellen Identifizierung innerhalb einer Menge mittels Äquivalenzrelationen beschäftigen, durch welche eine Menge vollständig in voneinander separierte Teilmengen aufgeteilt werden kann.

Mit deren Hilfe gelangen wir dann zu einer wichtigen – da in vielen Gebieten der Mathematik benötigten – grundlegenden algebraischen Struktur der sogenannten mathematischen Körper.

Definition (Relation, Äquivalenzrelation)

- Eine Relation R auf einer nichtleeren Menge G ist lediglich eine Teilmenge von $G \times G$.

  Statt $(x, y) \in R$ schreiben wir einfach wieder xRy.
- Eine Relation R auf einer nichtleeren Menge G heißt
  - **reflexiv**, falls $\forall x \in G : xRx$,
  - **symmetrisch**, falls $\forall x \in G : \forall y \in G : \ (xRy \Longrightarrow yRx)$,
  - **transitiv**, falls
  $$\forall x \in G : \forall y \in G : \forall z \in G : \big((xRy \wedge yRz) \Longrightarrow xRz\big).$$
- Eine Relation R auf einer nichtleeren Menge G heißt **Äquivalenzrelation**, wenn sie reflexiv, transitiv und symmetrisch ist.

  Äquivalenzrelationen werden häufig mit $\sim$ oder $\equiv$ bezeichnet.
- Die Mengen $[n]_\sim := \big\{m \in G \bigm| m \sim n\big\}$ nennen wir **Äquivalenzklassen**.

Theorem

Sei $\sim$ eine Äquivalenzrelation auf einer nichtleeren Menge G. Dann gilt $\forall n \in G : \forall m \in G : \left(\neg\left([n]_\sim \cap [m]_\sim = \emptyset\right) \Longrightarrow [n]_\sim = [m]_\sim\right)$

Beispiel (Äquivalenzrelation)

- Wir haben bereits in Teil 1 die Äquivalenzrelation $=$ auf einer beliebigen Menge kennengelernt.
- Zu einem beliebigen, festen $k \in \mathbb{N}$ mit $k > 1$ definiert $m \sim_k n :\Longleftrightarrow k|(m-n)$ eine Äquivalenzrelation auf $\mathbb{Z}$.

  Auf der Menge $\mathbb{Z}_k$ der Äquivalenzklassen (welche hier auch **Restklassen** genannt werden – vergleiche Division mit Rest) $[n]_k := \{m \in \mathbb{Z} \mid m \sim_k n\}$, $n \in \mathbb{Z}$, können wir Addition durch $[m]_k + [n]_k := [m+n]_k$ definieren und Multiplikation durch $[m]_k \cdot [n]_k := [m \cdot n]_k$ mit neutralen Elementen $[0]_k$ und $[1]_k$.

Definition (Körper)

Jede nichtleere Menge $\mathbb{K}$ mit zwei assoziativen Operationen $+\colon \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ und $\cdot\colon \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ und mit neutralen Elementen $0 \neq 1$, für welche $(\mathbb{K}, +, 0)$ und $(\mathbb{K} \setminus \{0\}, \cdot, 1)$ abelsche Gruppen sind und das Distributivgesetz gilt, nennt man einen Körper.

Beispiel (zyklische Gruppen und endliche Körper)

- Für jedes $k \in \mathbb{N} \setminus \{1\}$ ist $(\mathbb{Z}_k, +, [0]_k)$ eine abelsche Gruppe.
- Für $k = 12$ entspricht dies genau unserer verwendeten Uhrzeigerarithmetik, denn da 5 sowie 17 bei Division durch 12 den Rest 5 lassen, sagen wir zu beiden Zeiten, es ist 5 Uhr.
- Ist $k = p$ eine Primzahl, so ist auch $(\mathbb{Z}_p \setminus \{[0]_p\}, \cdot, [1]_p)$ eine abelsche Gruppe und $\mathbb{Z}_p$ mit beiden Verküpfungen ein Körper.

  Da $\mathbb{Z}_p = \{[0]_p, [1]_p, \dots, [p-1]_p\}$ nur endlich viele Elemente besitzt, sprechen wir von einem endlichen Körper.

Beispiel ($\mathbb{Z}_6$ - Teil 1)

- Rechnen wir in $\mathbb{Z}_6$, d.h., fassen wir ganze Zahlen, welche bei Division durch 6 denselben Rest $n \in \{0, 1, 2, 3, 4, 5\}$ lassen, zu Äquivalenzklassen $[n]_6$ zusammen, so erhalten wir folgende Operationstabellen für die Addition und Multiplikation

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

und

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

denn da 8 und 2 denselben Rest bei Division durch 6 lassen, ist etwa $[2]_6 \cdot [4]_6 = [8]_6 = [2]_6$. Jedoch besitzen die Elemente $[2]_6$, $[3]_6$ und $[4]_6$ jeweils kein multiplikatives Inverse in $\mathbb{Z}_6$.

In einem Körper besitzt jedes Element außer 0 ein multiplikatives Inverses, d.h., zu jedem $k \in \mathbb{K}$ existiert ein $x \in \mathbb{K}$ mit $k \cdot x = 1$.

Beispiel ($\mathbb{Z}_6$ - Teil 2)

- Da $(\mathbb{Z}_6 \setminus \{[0]\}, \cdot, 1)$ keine abelsche Gruppe ist, kann $\mathbb{Z}_6$ mit der betrachteten Multiplikation **kein Körper** sein.
- Insbesondere haben wir hier $[2]_6 \cdot [3]_6 = [0]_6$, obwohl weder $[2]_6 = [0]_6$ noch $[3]_6 = [0]_6$ gilt (denn sowohl 2 als auch 3 lassen einen Rest $\neq 0$ bei Division durch 6).

Theorem (Nullteilerfreiheit von Körpern)

Für Körper $\mathbb{K}$ *gilt* $\forall s, t \in \mathbb{K}\colon \ \big(s \cdot t = 0 \Longrightarrow \big[(s = 0) \vee (t = 0)\big]\big).$

Beweis: Angenommen, $s \cdot t = 0$ und $s \neq 0$, dann $\exists s^{-1} \neq 0$ und es folgt

$$t \ = \ 1 \cdot t \ = \ (s^{-1} \cdot s) \cdot t \ = \ s^{-1} \cdot (s \cdot t) \ = \ s^{-1} \cdot 0 \ = \ 0 \,.$$

Beispiel (Endliche Körper)

- Ein Körper muss wegen der Forderung $0 \neq 1$ mindestens zwei Elemente enthalten.
- Somit ist $\mathbb{Z}_2$ der kleinste Körper, denn $[1]_2$ hat sich selbst als (multiplikatives und additives) Inverse wegen

  $$[1]_2 \cdot [1]_2 = [1]_2$$

  (das Produkt zweier ungerader Zahlen bleibt ungerade) und

  $$[1]_2 + [1]_2 = [0]_2$$

  (die Summe zweier ungerader Zahlen ist eine gerade Zahl).
- Ebenso ist $\mathbb{Z}_7$ ein Körper. In $\mathbb{Z}_7$ ist $[3]_7$ das multiplikative Inverse von $[5]_7$, denn es gilt $[3]_7 \cdot [5]_7 = [1]_7$, und das additive Inverse von $[4]_7$, denn es gilt $[3]_7 + [4]_7 = [0]_7$.

Rationale Zahlen $\mathbb{Q}$

- In den ganzen Zahlen $\mathbb{Z}$ besitzt zu vorgegebenem $m, n \in \mathbb{Z}$ die Gleichung $k \cdot m = n$ im allgemeinen keine Lösung.
- Dieser Mangel lässt sich beheben, indem wir mit Hilfe der ganzen Zahlen die Menge der Äquivalenzklassen

$$\mathbb{Q} \;:=\; \left\{ \left[\frac{p}{q}\right]_{\sim} \;\middle|\; p \in \mathbb{Z},\; q \in \mathbb{Z},\; q \neq 0 \right\}$$

  mit der Äquivalenzrelation $\frac{p}{q} \sim \frac{\tilde{p}}{\tilde{q}} :\Longleftrightarrow p \cdot \tilde{q} = \tilde{p} \cdot q$ betrachten.
- Daraus folgt Erweitern/Kürzen $\boxed{\frac{p}{q} \sim \frac{p \cdot z}{q \cdot z}}$ für alle $z \in \mathbb{Z} \setminus \{0\}$.
- Der Einfachheit halber schreiben wir wieder $=$ statt $\sim$ und lassen die eckigen Klammern wieder weg.

Rechnen in $\mathbb{Q}$: Seien $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$ gegeben.

1. Definieren wir auf $\mathbb{Q}$ eine Addition durch $\boxed{\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}}$, so ist $0 = \frac{0}{1}$ das neutrale Element und $\frac{-a}{b}$ das Inverse von $\frac{a}{b}$.
2. Definieren wir auf $\mathbb{Q}$ die Multiplikation durch $\boxed{\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}}$, so ist $1 = \frac{1}{1}$ das neutrale Element und $\frac{b}{a}$ invers zu $\frac{a}{b}$ $(a \neq 0)$.
   Die aus der Schule bekannten Doppelbrüche sind also nichts anderes als Multiplikation mit dem Inversen:
   $$\boxed{\frac{\frac{a}{b}}{\frac{c}{d}} = \frac{a}{b} \cdot \frac{d}{c} = \frac{a \cdot d}{b \cdot c}}.$$
3. Der Einfachheit halber schreiben wir z statt $\frac{z}{1}$ für alle $z \in \mathbb{Z}$.
   Daher ist die oben eingeführte Addition sowie Multiplikation auf $\mathbb{Q}$ eine Fortsetzung der Operationen auf $\mathbb{Z}$.

Beispiel (der unendliche Körper $\mathbb{Q}$ der rationalen Zahlen)

- $(\mathbb{Q}, +, 0)$ und $(\mathbb{Q} \setminus \{0\}, \cdot, 1)$ sind abelsche Gruppen, und das Distributivgesetz gilt.

  Also ist $\mathbb{Q}$ mit diesen beiden Verknüpfungen ein Körper.

  Wir sprechen in diesem Fall von einem unendlichen Körper, da $\mathbb{Q}$ unendlich viele Elemente besitzt.
- Für $b, c \in \mathbb{Q}$, $b \neq 0$, hat die Gleichung $a \cdot b = c$ eine eindeutige Lösung $a \in \mathbb{Q}$, nämlich $a = \frac{c}{b}$.

Programm: 4. Teil – Angeordnete Körper

In dieser Kurzvorlesung wollen wir die algebraische Struktur Körper mit einer **Anordnung** versehen.

Ausgehend von der Frage, ob $\mathbb{Q}$ „lückenlos“ ist, motivieren wir, warum wir die reellen Zahlen benötigen.

Mit den zuvor vorgestellten **Anordnungsaxiomen** können wir nun die aus der Schule bekannten Intervalle einführen, welche wiederum Lösungsmengen von Ungleichungen sein können.

Abschließend erinnern wir an die Nullstellenbestimmung quadratischer Polynome und an die der schriftlichen Division verwandte **Polynomdivision**.

Wiederholung/Ausblick:

- Bisher haben wir Mengen und Operationen auf einigen von ihnen kennengelernt.
- Falls letztere gewisse Eigenschaften besitzen, haben wir diesen Objekten Namen wie Gruppe oder Körper gegeben.
- Jetzt interessiert uns, ob die einzelnen Elemente einer Menge zueinander in irgendeiner Beziehung stehen. Dazu greifen wir wiederum auf spezielle Relationen zurück.
- Eine zweistellige Relation R auf einer nichtleeren Menge M ist eine Teilmenge $R \subset M \times M$, wobei wir anstelle von $(x, y) \in R$ üblicherweise kurz xRy schreiben.
- Kennengelernt haben wir bisher schon die Äquivalenzrelationen $=$ und $\sim_k$.
- Nun wollen wir Relationen kennenlernen, die etwas über die Anordnungsmöglichkeit einer Menge aussagen.

Definition (Ordnungsrelation)

Eine Relation $\preceq$ auf $M \neq \emptyset$ heißt Ordnungsrelation, falls gilt

- $\forall x \in M\colon x \preceq x$ (Reflexivität)
- $\forall x, y, z \in M\colon \big((x \preceq y \wedge y \preceq z) \Longrightarrow x \preceq z\big)$ (Transitivität)
- $\forall x, y \in M\colon \big((x \preceq y \wedge y \preceq x) \Longrightarrow x = y\big)$ (Antisymmetrie)

Eine Ordnungsrelation $\preceq$ auf $M \neq \emptyset$ heißt total, falls für beliebige $x, y \in M$ stets $x \preceq y$ oder $y \preceq x$ gilt, also je zwei Elemente aus M vergleichbar sind (man sagt auch: in Relation zueinander stehen).

Beispiel

- Auf der Potenzmenge $\mathcal{P}(\Omega)$ ist $\subseteq$ eine Ordnungsrelation.
- Auf $\mathbb{N}$, $\mathbb{Z}$ und $\mathbb{Q}$ ist $\leq$ eine totale Ordnungsrelation.

Mittels totaler Ordnung können wir angeordnete Körper definieren.

Definition

Ein Körper $(\mathbb{K}, +, \cdot)$ heißt angeordnet, wenn auf $\mathbb{K}$ eine totale Ordnungsrelation $\preceq$ gegeben ist, die sich mit den Körperoperationen $+$ und $\cdot$ in folgendem Sinn verträgt:

1. $\forall x, y, z \in \mathbb{K}\colon \big(x \preceq y \Longrightarrow x + z \preceq y + z\big)$
2. $\forall x, y \in \mathbb{K}\colon \big(0 \preceq x \wedge 0 \preceq y \Longrightarrow 0 \preceq x \cdot y\big)$

Beispiel

- $\mathbb{Q}$ bildet mit den üblichen Operationen $+$ und $\cdot$ und der Ordnungsrelation $\leq$ einen angeordneten Körper.
- $\mathbb{Z}_2$ kann nicht angeordnet werden, denn gäbe es eine totale Ordnung $\preceq$ auf $\mathbb{Z}_2$ mit obigen beiden Eigenschaften, so folgte aus $[0]_2 \preceq [1]_2$ nach Addition von $[1]_2$ auch $[1]_2 \preceq [0]_2$ und mit der Antisymmetrie dann auch $[0]_2 = [1]_2$, Widerspruch.

Weitere Eigenschaften des mittels $\leq$ angeordneten Körpers $\mathbb{Q}$

Wir vereinbaren die Schreibweisen $x < y$ für $x \leq y \wedge x \neq y$ und $y \geq x$ für $x \leq y$ sowie $y > x$ für $x < y$. Dann gelten:

- $\forall x \in \mathbb{Q}\colon\ (x \leq 0 \iff -x \geq 0)$
- $\forall x, y, z \in \mathbb{Q}\colon\ (x \leq y \wedge z \leq 0 \Longrightarrow x \cdot z \geq y \cdot z)$
- $\forall x \in \mathbb{Q}\colon x^2 \geq 0$
- $\forall x \in \mathbb{Q}\colon\ \left(x > 0 \Longrightarrow \frac{1}{x} > 0\right)$
- $\forall x, y \in \mathbb{Q}\colon\ \left(y \geq x \wedge x > 0 \Longrightarrow \frac{1}{x} \geq \frac{1}{y}\right)$
- $\forall x, y \in \mathbb{Q}\colon\ \left(x \leq y \Longrightarrow x \leq \frac{x+y}{2} \wedge \frac{x+y}{2} \leq y\right)$

Lückenlosigkeit von $\mathbb{Q}$?

Es stellt sich nun die Frage, ob „zwischen zwei rationalen Zahlen nur rationale Zahlen liegen“.

Die Antwort lautet: Nein !

$\sqrt{2} \notin \mathbb{Q}$

Die Gleichung $x = \frac{2}{x}$ besitzt keine (positive) Lösung in $\mathbb{Q}$, denn: Angenommen, wir könnten zwei teilerfremde Zahlen $p, q \in \mathbb{N}$ finden, so dass

$$\frac{p}{q} = \frac{2}{\frac{p}{q}} \iff p^2 = 2q^2$$

Demzufolge wäre p^2 gerade. Da das Produkt ungerader Zahlen nicht gerade sein kann, müsste auch p gerade sein. Also gäbe es eine natürliche Zahl $k \in \mathbb{N}$ mit $p = 2 \cdot k$ und daher

$$4k^2 = 2q^2 \iff 2k^2 = q^2 \ .$$

Dies bedeutete aber, dass q^2 und somit auch q gerade wäre, Widerspruch zur Teilerfremdheit!

Ausweg

Diese bereits Pythagoras bekannte „Lückenhaftigkeit“ von $\mathbb{Q}$ wird durch das sogenannte Vollständigkeitsaxiom behoben, welches wir in einigen Wochen im Zusammenhang mit Folgen und Reihen kennenlernen werden. Durch Hinzunehmen der sogenannten irrationalen Zahlen erhalten wir den Körper/die Menge der reellen Zahlen $\mathbb{R}$, die wir mit Schulwissen bisher nur als (endliche/ unendliche, periodische/nichtperiodische) Dezimalbrüche kennen.

Wir definieren nun die folgenden (lückenlosen) reellen Intervalle

$$
\begin{aligned}
[a,b] &:= \{x \in \mathbb{R} \mid a \le x \ \wedge\ x \le b\} && \text{(abgeschlossenes Intervall)}\\
]a,b[&:= \{x \in \mathbb{R} \mid a < x \ \wedge\ x < b\} && \text{(offenes Intervall)}\\
]a,b] &:= \{x \in \mathbb{R} \mid a < x \ \wedge\ x \le b\} && \text{(links halboffenes Intervall)}\\
[a,b[&:= \{x \in \mathbb{R} \mid a \le x \ \wedge\ x < b\} && \text{(rechts halboffenes Intervall)}
\end{aligned}
$$

Beispielsweise sind Lösungsmengen von Ungleichungen oftmals Intervalle bzw. Vereinigungen von Intervallen.

Beispiel (Lösen einer Ungleichung)

Die Ungleichung $(x-2)^2 < 9$ ist äquivalent zu $x^2 - 4x - 5 < 0$, d.h. zu $(x-5)(x+1) < 0$. Somit ist die Lösungsmenge $L =]-1, 5[$. Hierbei brauchten wir die Nullstellen eines Polynoms.

Definition (Polynom)

Ein Polynom vom Grad $n \in \mathbb{N}_0$ über einem Körper $\mathbb{K}$ mit Koeffizienten $a_0, \ldots, a_n \in \mathbb{K}, a_n \neq 0_{\mathbb{K}}$, besitzt die Gestalt

$$p(x) \; := \; \sum_{k=0}^{n} a_k x^k \; = \; a_n x^n + a_{n-1} x^{n-1} + \ldots a_2 x^2 + a_1 x + a_0 \; .$$

Dem Nullpolynom $p_0 \colon x \mapsto 0$ ordnet man den Grad $-\infty$ zu.

Beispiel (Polynome kleineren Grades)

1. Konstanten a_0 mit $a_0 \in \mathbb{K} \setminus \{0_{\mathbb{K}}\}$ sind Polynome 0. Grades.
2. Lineare Polynome $a_0 + a_1 x$ mit $a_1 \neq 0_{\mathbb{K}}$ sind 1. Grades.
3. Für $a_2 \neq 0_{\mathbb{K}}$ heißt $a_0 + a_1 x + a_2 x^2$ quadratisches Polynom.
4. Für $a_3 \neq 0_{\mathbb{K}}$ heißt $a_0 + a_1 x + a_2 x^2 + a_3 x^3$ kubisches Polynom.
5. Für $a_4 \neq 0_{\mathbb{K}}$ heißt $a_0 + a_2 x^2 + a_4 x^4$ biquadratisches Polynom.

Nullstellen sind die Elemente der Lösungsmenge L von $p(x) = 0$.

Definition (Nullstelle eines Polynoms)

- Wir sagen, ein Polynom $p(x)$ besitzt über einem Körper $\mathbb{K}$ eine **Nullstelle** a, wenn $p(a) = 0$ und $a \in \mathbb{K}$ gilt.
- Ist a eine Nullstelle eines Polynoms $q(x)$, dann nennen wir a eine **mehrfache Nullstelle** von $p(x) = (x - a)q(x)$.

Beispiel (Nullstellen von Polynomen über $\mathbb{K} = \mathbb{R}$)

1. Für $p_0 \colon x \mapsto 0$ ist $L = \mathbb{K}$ für die Gleichung $p_0(x) = 0$.
2. Für konstante Polynome $\neq 0$ ist $L = \emptyset$ von $p(x) = 0$.
3. Für die Gleichung $a_0 + a_1 x = 0$ mit $a_1 \neq 0$ ist $L = \{-a_0 a_1^{-1}\}$.
4. Für Polynome ungeraden Grades ist $L \neq \emptyset$. (Übungsaufgabe!)
5. Für die Gleichung $a_0 + a_1 x + a_2 x^2$ mit $a_2 \neq 0$ kann die Lösungsmenge null, ein oder zwei Elemente enthalten.

Binomische Formeln und Co.

- Ausmultiplizieren liefert
$$\begin{aligned} (a \pm b)^2 &= a^2 \pm 2ab + b^2 \\ a^2 - b^2 &= (a+b)(a-b) \end{aligned}$$
- Ist $p(x)$ ein Polynom mit $\deg(p(x)) = n$ und $p(u) = 0$, dann existiert ein $q(x)$ mit $\deg(q(x)) = n - 1$, $p(x) = (x - u)q(x)$.
- Sind u und v Nullstellen von $x^2 + ax + b$, so gelten $b = uv$ und $-a = u + v$ wegen $(x-u)(x-v) = x^2 - (u+v)x + uv$.

Nullstellen quadratischer Polynome

Ob ein (normiertes) quadratisches Polynom $x^2 + px + q$ Nullstellen über $\mathbb{R}$ besitzt, überprüfen wir mittels quadratischer Ergänzung:

$$x^2 + px + q = 0 \iff \underbrace{x^2 + 2 \cdot \frac{p}{2}x + \frac{p^2}{4}}_{=\left(x+\frac{p}{2}\right)^2} = \underbrace{\frac{p^2}{4} - q}_{=:D(\text{iskriminante})}$$

Im Fall $D \geq 0$ folgt die bekannte p-q-Formel $x_{1,2} = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}$

Beispiel (Spezialfall: Polynomdivision ohne Rest)

$$\begin{array}{rrrrl}
(x^3 & +2x^2 & -x & -2) & : (x-1) = x^2 + 3x + 2 \\
-(x^3 & -x^2) & & & \\
\hline
 & 3x^2 & -x & & \\
 & -(3x^2 & -3x) & & \\
\hline
 & & 2x & -2 & \\
 & & -(2x & -2) & \\
\hline
 & & & 0 &
\end{array}$$

Polynomdivision ohne Rest, falls eine Nullstelle bekannt.

Am letzten Beispiel sehen wir, dass für eine Nullstelle a von $p(x)$ per Polynomdivision durch $(x-a)$ ein Polynom kleineren Grades erhalten werden kann, dessen Nullstellen folglich auch Nullstellen von $p(x)$ sein müssen. Wegen $x^2+3x+2=(x+2)(x+1)$ folgt für das letzte Beispiel $x^3+2x^2-x-2 \ = \ (x-1)(x+2)(x+1)$.

Im Allgemeinen ist das Ergebnis einer Polynomdivision jedoch nicht wieder ein Polynom, sondern eine sogenannte **rationale Funktion**.

Beispiel (Allgemeiner Fall: Polynomdivision mit Rest)

$$\begin{array}{rrrrl}
(x^3 & +2x^2 & -\ x & -1) & :(x-1) \ = \ x^2+3x+2+\frac{1}{x-1} \\
-(x^3 & -\ x^2) & & & \\
\hline
 & 3x^2 & -\ x & & \\
 & -(3x^2 & -3x) & & \\
\hline
 & & 2x & -1 & \\
 & & -(2x & -2) & \\
\hline
 & & & 1 &
\end{array}$$

Polynomdivision mit Rest, da 1 keine Nullstelle.

Beispiel (Polynomdivision mit Rest $\Longrightarrow$ gebrochen rationaler Teil)

$$
\begin{array}{rrrrrl}
(x^5 & +2x^4 & +\ 3x^3 & -68x^2) & & \quad : (x^2-4x+4) \\
-(x^5 & -4x^4 & +\ 4x^3) & & & \\
\hline
 & 6x^4 & -\ \ x^3 & -68x^2 & & \\
 & -(6x^4 & -24x^3 & +24x^2) & & \\
\hline
 & & 23x^3 & -92x^2 & & \\
 & & -(23x^3 & -92x^2 & +92x) & \\
\hline
 & & & & -92x &
\end{array}
$$

$$
= \ x^3 + 6x^2 + 23x - \boxed{\frac{92x}{x^2-4x+4}}
$$

Programm: 5. Teil – Polynome und Vektorräume

In dieser Kurzvorlesung wollen wir uns sinnvolle Verknüpfungen auf der Menge aller Polynome über x von höchstens n-tem Grad anschauen.

Insbesondere wollen wir herausstellen, was diese Menge – zusammen mit diesen Verknüpfungen – mit dem $\mathbb{R}^{n+1}$ gemein hat.

Daran anknüpfend führen wir daraufhin den abstrakten Begriff des **Vektorraumes** ein, welcher allgemein – um seine im Gegensatz zu anderen mathematischen Räumen besondere algebraische Struktur deutlich hervorzuheben – auch **linearer Raum** genannt wird.

- In der letzten Woche haben wir bereits gewisse mathematische Strukturen – etwa eine Gruppe oder einen Körper – kennengelernt. Diese zeichneten sich allein durch ihre definierenden Eigenschaften aus.
- In dieser Woche wollen wir uns einem weiteren mathematischen Objekt nähern, welches uns während des Studiums immer wieder begegnen wird.
- Wir erinnern uns zunächst, dass ein Polynom vom Grad $n \in \mathbb{N}_0$ über einem Körper $\mathbb{K}$ mit Koeffizienten $a_0, \ldots, a_n \in \mathbb{K}, a_n \neq 0_{\mathbb{K}}$, die Gestalt

$$p_n(x) \; := \; \sum_{k=0}^{n} a_k x^k \; = \; a_n x^n + a_{n-1} x^{n-1} + \ldots a_2 x^2 + a_1 x + a_0$$

besitzt. Dabei haben wir die Nullabbildung $p_0 : x \mapsto 0$ als **Nullpolynom** bezeichnet und ihm den Grad $-\infty$ zugeordnet.

Π_n – Menge aller Polynome vom Grad $\leq n$

- Sei $(\mathbb{K}, +, \cdot)$ ein beliebiger Körper. Wir betrachten die Menge

$$\Pi_n \ := \ \left\{ p(x) \;\middle|\; p(x) = \sum_{k=0}^{n} a_k x^k, a_k \in \mathbb{K}, k = 0, \ldots, n \right\} \ .$$

- Auf dieser Menge Π_n definieren wir für beliebige $p, \tilde{p} \in \Pi_n$ eine **additive Verknüpfung** $\oplus \colon \Pi_n \times \Pi_n \to \Pi_n$ durch

$$(p, \tilde{p}) \mapsto p(x) \oplus \tilde{p}(x) \ := \ \sum_{k=0}^{n} (a_k + \tilde{a}_k) x^k \ .$$

- Desweiteren betrachten wir für beliebige $\alpha \in \mathbb{K}$ und beliebige $p \in \Pi_n$ eine weitere Verknüpfung $\bullet \colon \mathbb{K} \times \Pi_n \to \Pi_n$, definiert durch

$$(\alpha, p) \mapsto \alpha \bullet p(x) \ := \ \sum_{k=0}^{n} (\alpha \cdot a_k) x^k \ .$$

Theorem

Die Struktur $(\Pi_n, \oplus)$ *ist eine abelsche Gruppe.*

Beweis:

1. Die Verknüpfung $\oplus\colon \Pi_n \times \Pi_n \to \Pi_n$ ist sowohl assoziativ als auch kommutativ, da dies durch $(\mathbb{K}, +)$ vererbt wird.
2. Es existiert ein neutrales Element, nämlich das Nullpolynom p_0, bei dem alle Koeffizienten $a_k = 0$ sind.
3. Zu jedem $p \in \Pi_n$ existiert ein $-p \in \Pi_n$, welches genau die Koeffizienten $-a_k$ besitzt, so dass

$$p(x) \oplus (-p(x)) \;=\; \sum_{k=0}^{n} (a_k + (-a_k))x^k \;=\; \sum_{k=0}^{n} 0 \cdot x^k \;=\; p_0 \;.$$

∎

Weitere Eigenschaften

Die Verknüpfung $\bullet\colon \mathbb{K} \times \Pi_n \to \Pi_n$ auf der abelschen Gruppe $(\Pi_n, \oplus)$ besitzt die Eigenschaften

1. $\forall p \in \Pi_n\colon 1_{\mathbb{K}} \bullet p(x) \; = \; \sum_{k=0}^{n} (1_{\mathbb{K}} \cdot a_k) x^k \; = \; \sum_{k=0}^{n} a_k x^k \; = \; p(x)$
2. $\forall \alpha, \beta \in \mathbb{K}\colon \forall p \in \Pi_n\colon$
$$\begin{aligned} (\alpha \cdot \beta) \bullet p(x) \; &= \; \sum_{k=0}^{n} ((\alpha \cdot \beta) \cdot a_k) x^k \; = \; \sum_{k=0}^{n} (\alpha \cdot (\beta \cdot a_k)) x^k \\ &= \; \alpha \bullet (\beta \bullet p(x)) \end{aligned}$$
3. Analog gelten $\forall \alpha, \beta \in \mathbb{K}$ und $\forall p, q \in \Pi_n$
$$\begin{aligned} (\alpha + \beta) \bullet p(x) \; &= \; (\alpha \bullet p(x)) \oplus (\beta \bullet p(x)) \; , \\ \alpha \bullet (p(x) \oplus q(x)) \; &= \; (\alpha \bullet p(x)) \oplus (\alpha \bullet q(x)) \; . \end{aligned}$$

Diese Eigenschaften haben wir bereits einmal woanders gesehen:

Beispiel

Auf den Mengen $\mathbb{R}^2 := \mathbb{R} \times \mathbb{R}$ und $\mathbb{R}^3 := \mathbb{R} \times \mathbb{R} \times \mathbb{R}$ kennen wir die komponentenweisen Additionen

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} := \begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 \end{pmatrix} \quad \text{bzw.} \quad \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} := \begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 \\ x_3 + y_3 \end{pmatrix}$$

und die komponentenweisen Multiplikationen mit einem sogenannten Skalaren

$$\alpha \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} := \begin{pmatrix} \alpha \cdot x_1 \\ \alpha \cdot x_2 \end{pmatrix} \quad \text{bzw.} \quad \alpha \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} := \begin{pmatrix} \alpha \cdot x_1 \\ \alpha \cdot x_2 \\ \alpha \cdot x_3 \end{pmatrix} ,$$

welche eben analoge Eigenschaften besitzen.

Somit lohnt es sich, diese Struktur in einer Definition festzuhalten:

Definition (Vektorraum)

Sei $(\mathbb{K}, +, \cdot)$ ein Körper und $(V, \oplus)$ eine abelsche Gruppe. Weiter gäbe es eine äußere Verknüpfung $\bullet : \mathbb{K} \times V \to V$ mit

1. $\forall v \in V \colon 1_{\mathbb{K}} \bullet v = v$ (Einselement)
2. $\forall \alpha, \beta \in \mathbb{K}\ \forall v \in V \colon (\alpha \cdot \beta) \bullet v \ = \ \alpha \bullet (\beta \bullet v)$ (Assoziativität)
3. $\forall \alpha, \beta \in \mathbb{K}\ \forall v \in V \colon (\alpha + \beta) \bullet v \ = \ (\alpha \bullet v) \oplus (\beta \bullet v)$

   und

   $\forall \alpha \in \mathbb{K}\ \forall v, w \in V \colon \alpha \bullet (v \oplus w) \ = \ (\alpha \bullet v) \oplus (\alpha \bullet w)$

   (Distributivität)

Dann heißt V ein linearer Raum oder Vektorraum über $\mathbb{K}$ (kurz $\mathbb{K}$-Vektorraum).

Üblicherweise bezeichnen wir die Elemente eines linearen Raumes als **Vektoren** und die Verknüpfung $\bullet$ als skalare Multiplikation.

Beispiel (($\mathbb{K}$-)Vektorräume)

- Sei Π_2 die Menge der Polynome höchstens zweiten Grades über einem beliebigen (endlichen oder unendlichen) Körper $\mathbb{K}$. Nach einem vorangegangenen Theorem ist $(\Pi_2, +)$ mit
$$(a_2x^2 + a_1x + a_0) \ + \ (b_2x^2 + b_1x + b_0) \\ := \ (a_2 + b_2)x^2 + (a_1 + b_1)x + (a_0 + b_0)$$
eine abelsche Gruppe, welche mit
$$\alpha \cdot (a_2x^2 + a_1x + a_0) \ := \ (\alpha \cdot a_2)x^2 + (\alpha \cdot a_1)x + (\alpha \cdot a_0)$$
zu einem $\mathbb{K}$-Vektorraum wird.
- Im Fall $\mathbb{K} = \mathbb{R}$ kann man obigen Vektorraum durch die eineindeutige (und mit den Verknüpfungen sogar verträgliche) Zuordnung $\Pi_2 \ni a_2x^2 + a_1x + a_0 \mapsto (a_0, a_1, a_2) \in \mathbb{R}^3$ mit dem uns aus der Schule bekannten $\mathbb{R}$-Vektorraum $\mathbb{R}^3$ identifizieren.

Programm: 6. Teil – Lineare Abbildungen und Gleichungssysteme

In dieser Kurzvorlesung wollen wir uns weiter um Vektorräume kümmern, den Begriff der **Dimension** sinnvoll einführen sowie sogenannte **lineare Abbildungen** auf Vektorräumen und ihre Eigenschaften betrachten.

Weiterhin werden wir auf sogenannte **lineare Gleichungssysteme** stoßen, welche einerseits mit Hilfe von Matrizen und dem Skalarprodukt auf dem $\mathbb{R}^n$ in prägnanter Form darstellbar sind und welche andererseits mit Hilfe des sogenannten **Gauß-Algorithmus** schnell gelöst werden.

Um über die Dimension eines linearen Raumes sprechen zu können, benötigen wir zunächst den Begriff einer Basis.

Definition (Linearkombination, linear unabhängig, Basis)

Sei V ein beliebiger $\mathbb{K}$-Vektorraum und $v_1, \ldots, v_n \in V$ Vektoren.

1. Unter einer **Linearkombination** der Vektoren $v_1, \ldots, v_n \in V$ verstehen wir einen Vektor
$$\sum_{k=1}^{n} \alpha_k v_k \qquad \text{mit} \qquad \alpha_1, \ldots, \alpha_n \in \mathbb{K} \ .$$
2. Eine Menge $\{v_k \mid k = 1, \ldots, n\}$ heißt **linear unabhängig**, wenn für jede Linearkombination mit $\sum \alpha_k v_k = 0_V$ schon $a_k = 0$ für alle $k = 1, \ldots, n$ folgt.
3. Eine linear unabhängige Menge $\{v_k \mid k = 1, \ldots, n\}$ heißt **Basis** von V, wenn sich jedes Element von V als (sogar eindeutige) Linearkombination der v_k schreiben lässt.

Theorem

- *Jeder Vektorraum hat eine Basis.*
- *Jede Basis des $\mathbb{R}$-Vektorraumes $\mathbb{R}^n$ besitzt genau n Elemente.*

Die letzte Aussage liefert die Motivation, den Begriff der **Dimension eines Vektorraumes** an der Anzahl der Elemente einer beliebigen Basis des jeweiligen Raumes festzumachen.

Beispiel (Endlich-dimensionale Vektorräume der Dimension $n \in \mathbb{N}$)

Der $\mathbb{R}^n$ ist n-dimensional, denn für jedes Element $v \in \mathbb{R}^n$ gilt

$$\begin{pmatrix} v_1 \\ v_2 \\ v_3 \\ \vdots \\ v_n \end{pmatrix} = v = \sum_{k=1}^{n} v_k \mathbf{e}_k = v_1 \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + v_2 \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + v_3 \begin{pmatrix} 0 \\ 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} + \ldots + v_n \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}.$$

Beispiel (Π_∞ – ein unendlich-dimensionaler Vektorraum)

- Aus der Primfaktorzerlegung eines Polynoms wissen wir, dass Polynome auch miteinander multipliziert werden können.
- Wegen $\deg(p(x) \cdot q(x)) = \deg(p(x)) + \deg(q(x))$ kann die Multiplikation von Polynomen aus Π_n im Fall $n > 0$ keine Abbildung $\cdot\colon \Pi_n \times \Pi_n \to \Pi_n$ sein.
- Aufgrund der Eigenschaft $\forall n \in \mathbb{N}_0\colon \Pi_n \subset \Pi_{n+1}$ wird durch
$$\Pi_\infty := \bigcup_{n\in\mathbb{N}_0} \Pi_n$$
genau die Menge aller Polynome beschrieben.
- Mit einer geeignet fortgesetzten Addition und skalaren Multiplikation bildet Π_∞ einen unendlich-dimensionalen Vektorraum, da jede Basis einer an der Vereinigung beteiligten Menge Π_n auch linear unabhängig in Π_∞ ist.

Auf linearen Räumen betrachten wir häufig lineare Abbildungen.

Definition (Eigenschaften linearer Abbildungen)

1. Eine Abbildung $A\colon \mathbb{R}^n \to \mathbb{R}^m$ heißt **linear**, wenn

$$\forall \lambda, \mu \in \mathbb{R}\colon \forall v, w \in \mathbb{R}^n\colon A(\lambda v + \mu w) \;=\; \lambda A(v) \;+\; \mu A(w)$$

2. Eine lineare Abbildung $A\colon \mathbb{R}^n \to \mathbb{R}^m$ heißt
   - **injektiv** $:\iff \forall v, w \in \mathbb{R}^n\colon\; (A(v) = A(w) \implies v = w)$;
   - **surjektiv** $:\iff \forall y \in \mathbb{R}^m\colon \exists v \in \mathbb{R}^n\colon A(v) = y$;
   - **bijektiv** $:\iff$ A injektiv und surjektiv.
3. Die Menge $\left\{ v \in \mathbb{R}^n \;\middle|\; Av = 0_{\mathbb{R}^m} \right\}$ heißt **Kern** von A.

Beispiel

- Ein Spezialfall linearer Abbildungen $A\colon \mathbb{R}^1 \to \mathbb{R}^1$ sind Geraden durch den Nullpunkt, also Funktionen $x \mapsto ax$ mit $a \in \mathbb{R}$.

Im Fall $a \neq 0$ ist die lineare Abbildung $x \mapsto ax$ bijektiv.

Beispiel (Lineare Abbildungen nach $\mathbb{R}$)

Mit der Schreibweise des sogenannten Transponierens

$$v^{\mathrm{T}} := \begin{pmatrix} v_1 & v_2 & \dots & v_{n-1} & v_n \end{pmatrix}$$

können wir die durch

$$v^{\mathrm{T}} w = \begin{pmatrix} v_1 & v_2 & \dots & v_{n-1} & v_n \end{pmatrix} \begin{pmatrix} w_1 \\ w_2 \\ \dots \\ w_{n-1} \\ w_n \end{pmatrix} := \sum_{k=1}^{n} v_k w_k$$

definierte Verknüpfung $\cdot \colon \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$, welche auch Innenprodukt oder **Skalarprodukt** auf dem $\mathbb{R}^n$ genannt wird, verwenden, um lineare Abbildungen $A \colon \mathbb{R}^n \to \mathbb{R}$ durch $x \mapsto v^{\mathrm{T}} x$ darzustellen.

Im Fall $v \neq 0$ ist die lineare Abbildung $x \mapsto v^{\mathrm{T}} x$ surjektiv.

Die allgemeine lineare Abbildung $A\colon \mathbb{R}^n \to \mathbb{R}^m$ kann mittels m fester Zeilenvektoren $v_1^{\mathrm{T}}, \ldots, v_m^{\mathrm{T}}$ dargestellt werden als

$$x := \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} v_{11} & \dots & v_{1n} \\ \vdots & \ddots & \vdots \\ v_{m1} & \dots & v_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} v_1^{\mathrm{T}} \\ \vdots \\ v_m^{\mathrm{T}} \end{pmatrix} x := \begin{pmatrix} v_1^{\mathrm{T}} x \\ \vdots \\ v_m^{\mathrm{T}} x \end{pmatrix}$$

Beispiel (Endomorphismen ($n = m$))

- $x := \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} 4 & 2 \\ 3 & 8 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 4x_1 + 2x_2 \\ 3x_1 + 8x_2 \end{pmatrix}$
- $x := \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \mapsto \begin{pmatrix} 4 & 2 & 1 \\ 3 & 8 & 7 \\ 1 & 2 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 4x_1 + 2x_2 + x_3 \\ 3x_1 + 8x_2 + 7x_3 \\ x_1 + 2x_2 + x_3 \end{pmatrix}$

- Wie wir eben gesehen haben, können wir eine lineare Abbildung vom $\mathbb{R}^n$ in den $\mathbb{R}^m$ mit Hilfe des **Matrix** genannten Schemas

$$A := \begin{pmatrix} v_{11} & \cdots & v_{1n} \\ \vdots & \ddots & \vdots \\ v_{m1} & \cdots & v_{mn} \end{pmatrix}$$

  darstellen sowie deren Wirkungsweise durch m Skalarprodukte ausdrücken. Diese als **Matrix-Vektor-Multiplikation** Ax bezeichnete Operation kann auf die Multiplikation AB zweier zueinander passender Matrizen A und B erweitert werden. Dabei muss A soviele Spalten besitzen, wie B Zeilen hat.
- Die Menge aller bijektiven linearen Abbildungen $A\colon \mathbb{R}^n \to \mathbb{R}^n$ bzw. eine spezielle Menge sog. quadratischer Matrizen bildet mit der Matrizenmultiplikation eine nichtkommutative Gruppe.

Definition (Bild einer Abbildung)

Für eine lineare Abbildung $A\colon V \to W$ zwischen Vektorräumen V und W sei $\mathrm{Bild}(A) := \{w \in W \mid \exists v \in V\colon A(v) = w\}$ das **Bild**.

Die Fragestellung, ob ein Element im Bild einer linearen Abbildung vorkommt, ist äquivalent zur Frage nach der Lösbarkeit des linearen Gleichungssystems $Ax = b$ zu einer festen rechten Seite b.

Beispiel (Lösungsstrategie – Vielfache von Zeilen addieren)

$$\begin{aligned} 2x + 3y &= 1 \\ 6x + 4y &= 8 \end{aligned} \quad \overset{\text{2.Zeile}-3\cdot\text{1.Zeile}}{\Longleftrightarrow} \quad \begin{aligned} 2x + 3y &= 1 \\ -5y &= 5 \end{aligned}$$

Aus dieser Dreiecksgestalt können wir nun von unten nach oben die Lösung $y = -1$ sowie $x = 2$ ablesen. Mittels Verwendung von Matrizen vermeidet man das „Mitschleppen“ der Variablen.

Programm: 7. Teil – Komplexe Zahlen und Abstandsbegriffe

In dieser Kurzvorlesung wollen wir uns – ausgehend vom Vektorraum $\mathbb{R}^2$ – ein Beispiel für einen nicht angeordneten Körper anschauen, über dem ausnahmslos alle Polynome als ein Produkt von ausschließlich sogenannten Linearfaktoren $(x - a)$ darstellbar sind.

Desweiteren betrachten wir Abstandsbegriffe, welche – besonders in der Analysis – grundlegend für viele andere mathematische Objekte sind.

Wir betrachten die Menge $\mathbb{R}^2$ mit den beiden Verknüpfungen $\oplus, \otimes \colon \mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}^2$, welche definiert seien durch

$$\begin{pmatrix} a \\ b \end{pmatrix} \oplus \begin{pmatrix} c \\ d \end{pmatrix} := \begin{pmatrix} a+c \\ b+d \end{pmatrix}, \qquad \begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} := \begin{pmatrix} ac-bd \\ ad+bc \end{pmatrix}.$$

Theorem

1. *Es ist $(\mathbb{R}^2, \oplus, \otimes)$ ein Körper.* **Diesen nennen wir** $\mathbb{C}$.
2. *Es gilt* $\begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -1 \\ 0 \end{pmatrix}$.

Kürzen wir den Vektor $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ mit i ab und identifizieren wir die reellen Zahlen r mit den Vektoren $\begin{pmatrix} r \\ 0 \end{pmatrix}$, so lässt sich jedes Element eindeutig als $a + \mathrm{i}b$ mit $a, b \in \mathbb{R}$ schreiben. Es folgt also $\mathrm{i}^2 = -1$.

Die Verknüpfung $\otimes$ kann als eine spezielle Matrix-Vektor-Multiplikation aufgefasst werden, denn es ist

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

wobei wegen $\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} a^2 + b^2 & 0 \\ 0 & a^2 + b^2 \end{pmatrix}$

die auftretenden Matrizen bis (falls $(a, b) \neq (0, 0)$) auf den positiven Faktor $\sqrt{a^2 + b^2} > 0$ orthogonal (d.h., falls das multiplikative Inverse einer Matrix mit ihrer Transponierten übereinstimmt) sind und daher die Multiplikation mit einer komplexen Zahl als eine Drehstreckung bzw. Drehstauchung interpretiert werden kann.

Fazit: Wir können somit bei quadratischen Gleichungen im Fall einer negativen Diskriminante nun doch Lösungen finden . . .

Einen sinnvollen Längenbegriff für Vektoren, d.h. die Elemente eines Vektorraumes, kann man mit Hilfe einer Norm definieren.

Definition (Norm)

Sei V ein ($\mathbb{R}$-)Vektorraum. Eine Norm auf V ist eine Abbildung $\|.\| \; : \; V \to \mathbb{R}$ mit

1. $\forall v \in V \colon \|v\| = 0 \iff v = 0_V$ (Definitheit)
2. $\forall \alpha \in \mathbb{K} \; \forall v \in V \colon \|\alpha \cdot v\| = |\alpha| \cdot \|v\|$ (Homogenität)
3. $\forall v, w \in V \colon \|v + w\| \leq \|v\| + \|w\|$ (Dreiecksungleichung)

Die Nichtnegativität einer Norm folgt wieder aus den Eigenschaften

$$0 \overset{(1)}{=} \|0_V\| \overset{\substack{(V,+)\\ \text{Gruppe}}}{=} \|v + (-v)\| \overset{(3)}{\leq} \|v\| + \|-v\| \overset{(2)}{=} 2\|v\| \Longrightarrow 0 \leq \|v\|$$

Beispiel

Einige Normen sind uns aus der Schule wohlbekannt, nämlich einerseits auf $\mathbb{R}$ die durch die Betragsfunktion

$$|\cdot|\colon \mathbb{R} \to \mathbb{R}, \qquad |x| := \begin{cases} x\,, & x \geq 0 \\ -x\,, & x < 0 \end{cases}$$

definierte Norm und andererseits auf $\mathbb{R}^2 := \mathbb{R} \times \mathbb{R}$ bzw. $\mathbb{R}^3$ die euklidische Norm

$$\|\cdot\|_2\colon \mathbb{R}^2 \to \mathbb{R}, \qquad \|\mathbf{x}\|_2 = \|(x_1, x_2)\|_2 \;:=\; \sqrt{x_1^2 + x_2^2}$$

bzw.

$$\|\cdot\|_2\colon \mathbb{R}^3 \to \mathbb{R}, \qquad \|\mathbf{x}\|_2 = \|(x_1, x_2, x_3)\|_2 \;:=\; \sqrt{x_1^2 + x_2^2 + x_3^2}\,.$$

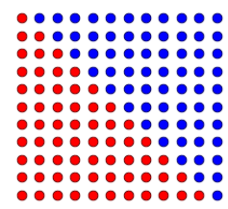
Programm: 8. Teil – Was ich noch zu sagen hätte . . .

Bisher haben wir Beweise von formalen Aussagen mittels Erstellung von Wahrheitstabellen sowie Beweise von Summenformeln oder Teilbarkeitsregeln über vollständige Induktion kennengelernt. Oftmals helfen uns aber auch geometrische Anschauungen.

Zum Abschluss soll es noch mal um Polynome und Abbildungen gehen – und was wir noch so alles mit Ihnen im ersten Semester anstellen wollen.

Zum Auftakt – Beweis ohne Worte

Die Summe der n ersten natürlichen Zahlen ist $\frac{n(n+1)}{2}$,



wie man dem Bild „entnehmen“ kann. Desweiteren wird deutlich, warum man die Zahlen

$$\Delta_n := \frac{n(n+1)}{2}$$

auch **Dreieckszahlen** nennt.

1. Können Sie einen analogen „Beweis“ ohne Worte dafür finden, dass die Summe zweier aufeinanderfolgender Dreieckszahlen eine Quadratzahl ist ?
2. Können Sie einen analogen „Beweis“ ohne Worte dafür finden, dass die Summe der n ersten ungeraden Zahlen genau n^2 ist ?

Gebrochen rationale Funktionen

Für Polynome $p(x)$, $q(x)$ mit $\deg(q(x)) = m > n = \deg(p(x))$ heißt eine Funktion der Gestalt

$$r(x) = \frac{p(x)}{q(x)} = \frac{a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0}{b_m x^m + \ldots + b_1 x + b_0} = \frac{\sum_{k=0}^{n} a_k x^k}{\sum_{j=0}^{m} b_j x^j}$$

gebrochen rationale Funktion (vgl. Polynomdivision mit Rest).

Oft können rationale Funktionen vereinfacht werden. Besitzen p und q eine gemeinsame reelle Nullstelle a, so ist der Linearfaktor $(x - a)$ durch Polynomdivision von $p(x)$ und $q(x)$ abzuspalten (vgl. Kürzen in $\mathbb{Q}$). Sind $p(x)$ und $q(x)$ teilerfremd, ist manchmal eine weitere Vereinfachung mittels Partialbruchzerlegung erreichbar.

Definition

Sei $n \in \mathbb{N}$ und $0 < k \leq n$. Eine Nullstelle a eines Polynoms $p(x)$ vom Grad n heißt k-fach, falls es ein Polynom $q(x)$ vom Grad $n-k$ mit $p(x) = (x-a)^k q(x)$ und $q(a) \neq 0$ gibt.

Beispiel ($q(x)$ besitzt nur verschiedene reelle einfache Nullstellen)

$$\frac{x+17}{x^2-x-12} \implies q(x) = x^2 - x - 12 = (x+3)(x-4)$$

$$\overset{\text{Ansatz}}{\implies} \boxed{\frac{A}{x+3} + \frac{B}{x-4}} = \frac{(A+B)x + 3B - 4A}{x^2-x-12}$$

$$\overset{\substack{\text{Koeffizienten-}\\ \text{vergleich}}}{\implies} \left.\begin{array}{rcr} A+B & = & 1 \\ 3B-4A & = & 17 \end{array}\right\} \implies \left\{\begin{array}{lr} A = & -2 \\ B = & 3 \end{array}\right.$$

$$\implies \frac{x+17}{x^2-x-12} = -\frac{2}{x+3} + \frac{3}{x-4}$$

Beispiel ($q(x)$ besitzt nur eine reelle mehrfache Nullstelle)

$$\frac{x^2-7x+15}{(x-2)^3} \overset{\text{Ansatz}}{\Longrightarrow} \boxed{\frac{A}{x-2}+\frac{B}{(x-2)^2}+\frac{C}{(x-2)^3}}$$

$$= \frac{Ax^2+(B-4A)x+4A-2B+C}{(x-2)^3}$$

$$\overset{\substack{\text{Koeffizienten-}\\ \text{vergleich}}}{\Longrightarrow} \left.\begin{aligned} A &= 1 \\ B-4A &= -7 \\ 4A-2B+C &= 15 \end{aligned}\right\} \Longrightarrow \begin{cases} A = & 1 \\ B = & -3 \\ C = & 5 \end{cases}$$

$$\Longrightarrow \quad \frac{x^2-7x+15}{(x-2)^3} = \frac{1}{x-2} - \frac{3}{(x-2)^2} + \frac{5}{(x-2)^3}$$

Definition (Grenzwert einer Folge, Stetigkeit einer Funktion)

1. Eine Folge $(x_n)_{n\in\mathbb{N}}$ heißt konvergent gegen a, falls es zu jedem $\varepsilon > 0$ ein $N \in \mathbb{N}$ gibt, so dass für alle $n \in \mathbb{N}$ aus $n > N$ auch $|x_n - a| < \varepsilon$ folgt. Dann heißt a der Grenzwert von $(x_n)_{n\in\mathbb{N}}$, wir schreiben

$$\boxed{\lim_{n\to\infty} x_n = a\ .}$$

2. Eine Funktion $f\colon [c,d] \to \mathbb{R}$ heißt stetig in $a \in [c,d]$, falls es zu jedem $\varepsilon > 0$ ein $\delta > 0$ gibt, so dass für alle $x \in [c,d]$ aus $|x - a| < \delta$ auch $|f(x) - f(a)| < \varepsilon$ folgt. Wir schreiben

$$\boxed{\lim_{x\to a} f(x) = f(a)\ ,}$$

denn für jede Folge $(x_n)_{n\in\mathbb{N}}$ mit a als Grenzwert ist dann auch die Folge $(f(x_n))_{n\in\mathbb{N}}$ konvergent mit Grenzwert $f(a)$.

Typische Übungsaufgaben aus dem ersten Semester

1. Zeigen Sie für konvergente Folgen $(a_n)_{n\in\mathbb{N}}$ und $(b_n)_{n\in\mathbb{N}}$ die Rechenregeln
$$\lim_{n\to\infty}(a_n \pm b_n) = \left(\lim_{n\to\infty} a_n\right) \pm \left(\lim_{n\to\infty} b_n\right)$$
und
$$\lim_{n\to\infty}(a_n \cdot b_n) = \left(\lim_{n\to\infty} a_n\right) \cdot \left(\lim_{n\to\infty} b_n\right)$$
2. Bestimmen Sie die Grenzwerte
$$\text{(i)}\ \frac{2n^3+n^2-5}{(n+1)^3} \quad \text{(ii)}\ \sqrt{n^2-3}-\sqrt{n^2+3} \quad \text{(iii)}\ \sqrt[n]{4^n+5^n}$$
3. Zeigen Sie die Stetigkeit von konstanten und linearen Funktionen sowie die Stetigkeit von Summen, Produkten und Hintereinanderausführungen stetiger Funktionen.
4. Zeigen Sie die Unstetigkeit von nichtkonstanten Treppenfunktionen.

Definition (Differenzierbarkeit einer Funktion)

Eine Funktion $f:]c,d[\to \mathbb{R}$ heißt differenzierbar in $a \in]c,d[$, falls es ein $b \in \mathbb{R}$ gibt und für jedes $\varepsilon > 0$ ein $\delta > 0$ existiert, so dass für alle $h \neq 0$ aus $|h| < \delta$ auch $\left|\frac{f(a+h)-f(a)}{h} - b\right| < \varepsilon$. Wir schreiben

$$\boxed{\lim_{h\to 0} \frac{f(a+h)-f(a)}{h} \; = \; b \; =: \; f'(a)}$$

Ist f in jedem $a \in]c,d[$ differenzierbar, so nennen wir die Funktion $x \mapsto f'(x)$ die Ableitung von f und f differenzierbar.

Beispiel

1. Für $f: x \mapsto 0$ ist $f': x \mapsto 0$ die Ableitung.
2. Für $n \in \mathbb{N}$ und $f: x \mapsto x^n$ ist $f': x \mapsto nx^{n-1}$ die Ableitung.

Definition (Stammfunktion)

Sei $f\colon\ ]a,b[\to\mathbb{R}$ und es existiere eine differenzierbare Funktion $F\colon\ ]a,b[\to\mathbb{R}$ mit $F'(x)=f(x)$ für alle $x\in\,]a,b[$, dann heißt F eine Stammfunktion von f.

Beispiel

1. Für $f\colon x\mapsto 0$ sind $F\colon x\mapsto 0$ und $F_c\colon x\mapsto c$ für ein beliebiges $c\in\mathbb{R}$ Stammfunktionen.
   Stammfunktionen sind somit nicht eindeutig. Aus der Eindeutigkeit und Linearität (Übungsaufgaben) des Grenzwertes folgt aber, dass sich zwei Stammfunktionen maximal um eine additive Konstante unterscheiden.
2. Für $n\in\mathbb{N}$ und $f\colon x\mapsto x^n$ ist $F\colon x\mapsto \frac{1}{n+1}x^{n+1}$ eine Stammfunktion.

- Stammfunktionen von f werden oftmals als **Newton-Integral** sowie mit $\int f(x)dx$ bezeichnet.
- Das Newton- und das über Riemann-Summen eingeführte Riemann-Integral verfolgen unterschiedliche Zugänge, stimmen aber etwa auf dem linearen Raum der stetigen Funktionen $C([a,b],\mathbb{R}) \;=\; \{f : [a,b] \to \mathbb{R} \mid f \text{ stetig}\}$ überein.
- Die partielle Integration erhalten wir durch Integrieren der **Produktregel**:

$$\begin{aligned}\big(u(x)v(x)\big)' \;&=\; u'(x)v(x) + u(x)v'(x)\\ \Longrightarrow u(x)v(x) - \int u(x)v'(x)dx \;&=\; \int u'(x)v(x)dx\end{aligned}$$

- Sei F eine Stammfunktion von f. Die Substitutionsregel erhalten wir durch Integrieren der **Kettenregel**:

$$\begin{aligned}(F\circ\varphi)'(x) \;&=\; (F'\circ\varphi)(x)\cdot\varphi'(x)\\ \Longrightarrow (F\circ\varphi)(x) \;&=\; \int (f\circ\varphi)(x)\cdot\varphi'(x)dx\end{aligned}$$

Keine Angst vor der Mathematik !

- Das Schöne am Studium der Mathematik ist, dass wir sprichwörtlich „bei Null“ anfangen (können)
- Hilfreiche Voraussetzungen sind lediglich:
  - Fähigkeit zum abstrakten Denken und Freude daran
  - gesunder Menschenverstand (sprich: logisches Schlussfolgern)
  - räumliche Vorstellungskraft/Muster erkennen
  - Fleiß und Frustationstoleranz (sehr wichtig)

Warum lohnt sich ein Mathematik-Studium ?

Die wichtigste Qualifikation, die Sie aus dem Studium mitnehmen (werden/sollen) und welche Arbeitgeber an Mathematikerinnen und Mathematikern so sehr schätzen, ist die Fähigkeit, Probleme zu analysieren und Sachverhalte präzise zu beschreiben.

Wir wünschen Ihnen einen guten Einstieg ins Studium!