1 Mengen

1.1 Logik

Nur weil Mäuse Vierbeiner sind, heißt es noch lange nicht, dass jeder Vierbeiner eine Maus ist. In diesem kurzen Abschnitt geht es darum, welche Schlussfolgerungen zulässig sind. Außerdem wird einiges an Notation eingeführt.

Aussagen Aussagen sind entweder wahr oder falsch. „Der Dachs ist ein Säugetier“ ist eine wahre Aussage. Auch „Die Eins ist eine negative Zahl“ ist eine Aussage, allerdings eine falsche. Dagegen ist „Kuh über blau“ keine Aussage.

Aussagen können verneint werden: aus „Ich mag Schockolade“ wird etwa „Ich mag Schockolade nicht“. Ist P eine Aussage, so bezeichnet man mit $\neg P$ die verneinte Aussage. Bei der Verneinung von komplexen Aussagen, wie etwa „Ist der Koch blau, dann ist die Suppe versalzen oder die Bohnen sind nicht gar“, muss man vorsichtig sein.

Man kann zwei Aussagen zu einer Aussage zusammenfassen, etwa „Der Eisverkäufer ist da, und ich habe gerade Taschengeld bekommen“, oder „Gibst du mir eins deiner Lollis, so bin ich dein bester Freund„. Die verschiedenen Wege, Aussagen zusammenzufassen, kann man gut mit *Wahrheitstafeln* voneinander unterscheiden. Vier Zusammenfassungsregeln sind:

a) Und $\wedge$ Ich ging einkaufen, und die Sonne schien.

b) Oder $\vee$ Entweder mähe ich den Rasen, oder ich jäte Unkraut – oder beides.

c) Implikation $\Rightarrow$: Wenn es morgen regnet, dann bleibe ich auf jedem Fall zu Hause – aber vielleicht tue ich das sowieso.

d) Äquivalenz $\Leftrightarrow$ Wenn du sofort dein Zimmer aufräumst, dann darfst du eine halbe Stunde fernsehen – sonst aber nicht.

Wahrheitstafeln:

P	Q	$\neg P$	$P \wedge Q$	$P \vee Q$	$P \Rightarrow Q$	$P \Leftrightarrow Q$
F	F	W	F	F	W	W
F	W	W	F	W	W	F
W	F	F	F	W	F	F
W	W	F	W	W	W	W

Beachten Sie: $P \vee Q$ ist nur falsch, wenn P, Q beide falsch sind; und $P \Rightarrow Q$ ist nur falsch, wenn P wahr und Q falsch ist. Die Aussagen $(\neg P) \vee Q$ und $P \Rightarrow Q$ sind sogar äquivalent.

Will man zeigen, dass alle Vierbeiner Mäuse sind, so reicht es nicht aus, um nachzuweisen, dass alle Mäuse Vierbeiner sind. Dagegen ist die Aussage „Alle Vierbeiner sind Mäuse“ äquivalent zur (falschen) Aussage „Alles, was kein Maus ist, ist auch kein Vierbeiner“. In Symbolen ausgedrückt will ich sagen, dass die Folgerung $(P \Rightarrow Q) \Rightarrow (Q \Rightarrow P)$ nicht immer gilt, die Äquivalenz $(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P)$ dagegen schon. Diese beiden Behauptungen lassen sich mit Wahrheitstafeln nachweisen.

P	Q	$P \Rightarrow Q$	$Q \Rightarrow P$	$(P \Rightarrow Q) \Rightarrow (Q \Rightarrow P)$
F	F	W	W	W
F	W	W	F	**F**
W	F	F	W	W
W	W	W	W	W

P	Q	$\neg P$	$\neg Q$	$P \Rightarrow Q$	$\neg Q \Rightarrow \neg P$	$(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P)$
F	F	W	W	W	W	W
F	W	W	F	W	W	W
W	F	F	W	F	F	W
W	W	F	F	W	W	W

Aussageformen und Quantifikatoren Eine Aussageform ist eine Aussage mit einem oder mehreren freien Variablen. Es hängt vom Wert der Variable(n) ab, ob die Aussage wahr oder falsch ist.

Beispiel Schreibt man etwa $P(x)$ für die Aussageform „x ist eine reelle Zahl, die $x^2 - x = 0$ erfüllt“, so ist $P(0)$ eine wahre und $P(3)$ eine falsche Aussage.

Beispiel Schreibt man $Q(x, y)$ für die Aussageform „$xy + 3x = 2$“, so ist $Q(0, 1)$ falsch und $Q(1, -1)$ wahr. Dagegen ist $Q(1, y)$ die Aussageform „y+3 = 2“ mit nur einer Variable.

Gerade machten wir die Aussageform $P(x)$ zu einer Aussage, indem wir den Wert $x = 3$ einsetzen. Man kann aber auch Quantifikatoren benutzen, um aus Aussageformen Aussagen zu machen. Wir benötigen drei Quantifikatoren:

a) $\forall$ „für alle" Beispiel: „$\forall x \colon x^2 \geq 0$“ ist die Aussage, dass jedes x die Ungleichung $x^2 \geq 0$ erfüllt.

b) $\exists$ „es gibt (mindestens) ein“ Beispiel: „$\exists x \colon x$ ist eine ganze Zahl und $x^2 = 2$“ ist die (falsche) Aussage, dass $\sqrt{2}$ eine ganze Zahl ist.

c) $\exists!$ „es gibt genau ein“ Beispiel: „$\exists! x \colon x$ ist eine ganze Zahl und $x^2 = y$“ ist eine Aussageform, die für $y = 0$ wahr ist, aber für $y = 3$ bzw. $y = 4$ falsch ist, denn dort gibt es keine bzw. zwei Möglichkeiten für x.

1.2 Mengen

Wer Mathematik-Vorlesungen besucht, wird mit sehr vielen Definitionen konfrontiert. Eine zufriedenstellende Definition des Mengenbegriffs ist aber nicht dabei, stattdessen wird erwartet, dass man ungefähr weiß, was eine Menge ist. Die vier wichtigsten Punkte:

a) Mengen wurden von Cantor eingeführt. Traditionell gibt man anstelle einer formalen Definition das folgende Zitat wieder:

> *Unter einer ‚Menge' verstehen wir jede Zusammenfassung M von bestimmten wohlunterschiedenen Objecten m unsrer Anschauung oder unseres Denkens (welche die ‚Elemente' von M genannt werden) zu einem Ganzen.* (G. Cantor, 1895)

b) Somit bilden die rationalen Zahlen eine Menge, und die Städte Thüringens mit mehr als 50.000 Einwohnern bilden eine andere.

> *Eine Menge ensteht durch Zusammenfassung von Einzeldingen zu einem Ganzen. Eine Menge ist eine Vielheit, als Einheit gedacht.* (F. Hausdorff, 1927)

c) Allerdings sind manche Zusammenfassungen, die man sich vorstellen kann, – die Zusammenfassung aller Mengen, zum Beispiel – so groß, dass man sie nicht als Mengen durchgehen lassen kann (Stichwort: Russellsche Paradoxon).

d) Dieser Problematik müssen wir uns aber erst dann – wenn überhaupt – stellen, wenn wir im Hauptstudium eine Axiomatische Mengenlehre hören. Denn die Methoden, die wir benutzen, um neue Mengen zu konstruieren, liefern als Ergebnis tatsächlich immer Mengen.

Mengen bestehen aus Elementen. Ist x ein Element der Menge M, so drückt man diese Tatsache durch die Bezeichung $x \in M$ aus. So ist zum Bespiel $1 \in \mathbb{Z}$ aber $\frac{1}{2} \notin \mathbb{Z}$. Eine Menge M heißt *endlich*, wenn sie nur endlich viele Elemente enthält. Deren Anzahl nennt man die *Mächtigkeit* $|M|$.

Es gibt im wesentlichen zwei Methoden, eine Menge anzugeben:

a) Man listet alle Elemente auf, etwa $M = \{1, 3, 4, 6\}$ mit $|M| = 4$.

b) Man gibt eine Eigenschaft an, die die Elemente der Menge charakterisiert[1], etwa die unendliche Menge

$$M = \{n \in \mathbb{N} \mid n \text{ ist durch 3 teilbar und } n^2 \text{ hat als letztes Ziffer eine 4}\}\,.$$

[1] Warnhinweis: Die Eigenschaft muss auch dafür sorgen, dass eine Menge tatsächlich entsteht: meistens, indem man nur die Elemente eine bereits bekannten Menge in Betracht zieht. Russells Paradoxon (1901) ist das Erkenntnis, dass $L = \{x \mid x \text{ ist selbst eine Menge, und } x \notin x\}$ keine Menge sein kann.

Einige wichtige Mengen:

$\emptyset$	Die *leere* Menge $\emptyset = \{\}$, die *keine* Elemente enthält.
$\mathbb{N}$	Die Menge $\mathbb{N} = \{1, 2, 3, 4, 5, \ldots\}$ aller natürlichen Zahlen
$\mathbb{N}_0$	Die Menge $\mathbb{N}_0 = \{0, 1, 2, 3, 4, 5, \ldots\}$ aller natürlichen Zahlen einschl. 0
$\mathbb{Z}$	Die Menge $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ aller ganzen Zahlen
$\mathbb{Q}$	Die Menge der rationalen Zahlen
$\mathbb{R}$	Die Menge der reellen Zahlen
$\mathbb{C}$	Die Menge der komplexen Zahlen (kommt noch)

Definition (Gleichheit von Mengen)
Zwei Mengen M, N heißen genau dann gleich, wenn gilt: jedes Element aus M ist gleichzeitig ein Element aus N, und auch umgekehrt. In Symbolen:

$$(M = N) \quad \Longleftrightarrow \quad (\forall x \colon (x \in M) \Leftrightarrow (x \in N)) \,.$$

Beachten Sie hierzu:

- Die Mengen $\{1, 2, 3\}$ und $\{1, 2, 2, 3\}$ sind gleich, denn jedes Element der ersten Menge ist Element der zweiten, und auch umgekehrt. Beide Mengen haben auch genau drei Elemente.
- Dedekind stellte sich eine Menge vor wie einen geschlossenen Sack, der die Elemente der Menge enthält. Stelle ich mir aber einen roten und einen blauen Sack vor, die die gleichen Elemente enthalten, so stellen nach obiger Definition diese beiden Säcke die gleiche Menge dar: die Beschaffenheit des Sacks ist also unerheblich.

Beispiel $\{x \in \mathbb{Z} \mid x^4 - 5x^2 + 4 = 0\} = \{-2, -1, 1, 2\}$.

Eine Menge N heißt eine *Teilmenge* der Menge M, wenn jedes Element von N auch ein Element aus M ist. Bezeichnung: $N \subseteq M$. In Symbolen:

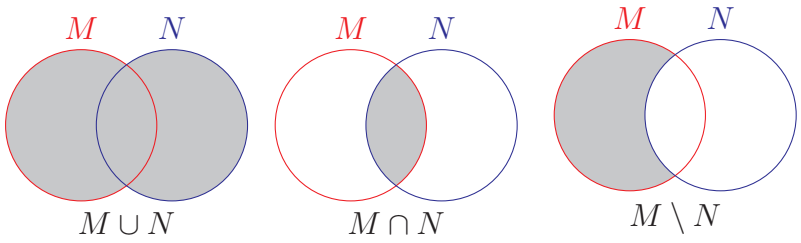
$$(N \subseteq M) \quad \Longleftrightarrow \quad (\forall x \colon (x \in N) \Rightarrow (x \in M)) \,.$$

Somit gilt:

Lemma 1.1. *Es ist genau dann $M = N$, wenn sowohl $N \subseteq M$ als auch $M \subseteq N$ gelten.* ∎

Sind M, N Mengen, so kann man folgende neue Mengen bilden: die *Vereinigung* $M \cup N$, den *Schnitt* $M \cap N$, und die *Differenzmenge* $M \setminus N$. Das geht so:

$$M \cup N = \{x \mid (x \in M) \vee (x \in N)\}$$
$$M \cap N = \{x \mid (x \in M) \wedge (x \in N)\}$$
$$M \setminus N = \{x \in M \mid x \notin N\} \qquad \text{Alternativschreibweise: } M - N.$$



Ist $M \cap N = \emptyset$, so heißen die Mengen M, N *disjunkt*.

Die Potenzmenge $\mathscr{P}(M)$ einer Menge M ist per Definition die Menge aller Teilmengen von M.

$$\mathscr{P}(M) = \{N \colon N \subseteq M\}\,.$$

Definition Sind A, B zwei Mengen, so definiert man das *direkte Produkt* $A \times B$ als die Menge aller *geordnete Paare* (a, b) mit $a \in A$ und $b \in B$. Das Wort „geordnet“ bedeutet, dass z.B. $(1, 2) \neq (2, 1)$.

Allgemeiner definiert man für Mengen $A_1, A_2, \ldots, A_n$ das direkte Produkt

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A_i \text{ für alle } i\}\,.$$

Die Elemente dieses Produkts nennt man (geordnete) n-Tupel[2].

1.3 Abbildungen

Definition Seien X, Y Mengen. Eine *Abbildung* $f \colon X \to Y$ von X nach Y ist eine Vorschrift, die zu jedem Element $x \in X$ genau ein Element $f(x) \in Y$ zuordnet. Man spricht auch von der Abbildung $x \mapsto f(x)$.

Die Menge aller Abbildungen von X nach Y wird mit Y^X oder $\mathrm{Abb}(X, Y)$ bezeichnet.

Beispiele

a) Die Vorschrift „$f(x) = 2x^3 - \sin(x)$“ definiert eine Abbildung $f \colon \mathbb{R} \to \mathbb{R}$.

b) Abbildungen müssen aber keineswegs durch schöne Formel definiert werden. So kann man eine Abbildung $f \colon \{0, 1, 3, 8, 9\} \to \{-1, \pi, e, \frac{1}{2}\}$ durch $f(0) = \pi$, $f(1) = -1$, $f(3) = -1$, $f(8) = \frac{1}{2}$ und $f(9) = -1$ definieren.

c) Die Vorschrift „$f(x) =$ das y mit $y^2 = x$“ definiert aus zwei Gründen keine Abbildung $f \colon \mathbb{R} \to \mathbb{R}$. Erstens wird zu negativen Zahlen wie z.B. -1 keinen Wert $f(x)$ zugeordnet; und zweitens wird zu positiven Zahlen mehr als einen Wert zugeordnet, z.B. $f(1) = 1$ und $f(1) = -1$.

[2]Wenn man später die Mengenlehre axiomatisieren will, stellt man sich die Frage, was für ein Objekt ein geordnetes Paar sein soll. Die heute allgemein akzeptierte Antwort lautet: das geordnete Paar (a, b) ist die Menge $\{\{a\}, \{a, b, \}\}$. Beachten Sie, dass diese Menge im Fall $a = b$ aus nur einem Element besteht.

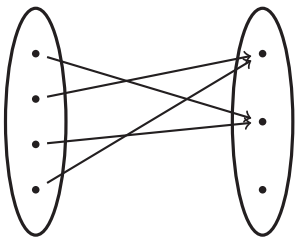
Bemerkung Eine äquivalente Definition lautet so: eine Abbildung $f\colon X \to Y$ ist eine Teilmenge $F \subseteq X \times Y$ mit der folgenden Eigenschaft: zu jedem $x \in X$ gibt es genau ein Element $y \in Y$ derart, dass das Paar (x, y) in F liegt. Es ist dann $y = f(x)$. Da man nicht Y von F ablesen kann, muss man streng genommen auch Y angeben.

1.4 Verknüpfung; Injektivität & Co.

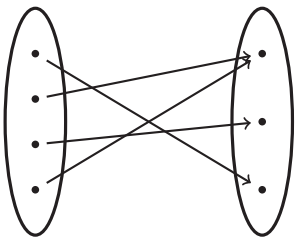
Definition Sind $f\colon X \to Y$ und $g\colon Y \to Z$ Abbildungen, so wird deren *Verknüpfung* $g \circ f\colon X \to Z$ so definiert: für jedes $x \in X$ ist $(g \circ f)(x) = g(f(x))$.

Definition Eine Abbildung $f\colon X \to Y$ heißt

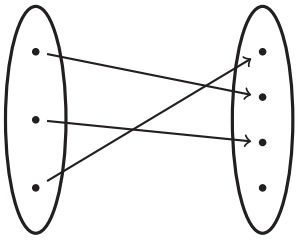
- *injektiv*, wenn keine zwei Elemente von X das gleiche Bild in Y haben, d.h. wenn jedes $y \in Y$ höchstens ein Urbild in X hat;
- *surjektiv*, wenn $\mathrm{Bild}(f) = Y$ gilt, d.h. wenn es zu jedem $y \in Y$ mindestens ein $x \in X$ mit $f(x) = y$ gibt;
- *bijektiv*, wenn sie sowohl injektiv als auch surjektiv ist. Anders gesagt, wenn es zu jedem $y \in Y$ genau ein $x \in X$ gibt mit $f(x) = y$.



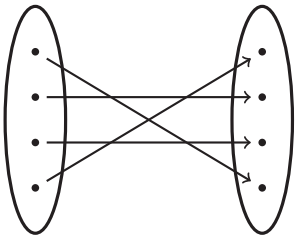
Weder surjektiv noch injektiv



Surjektiv aber nicht injektiv



Injektiv aber nicht surjektiv



Bijektiv

1.5 Erste Erkenntnisse über Abbildungen

Lemma 1.2. *Verknüpfung von Abbildungen ist assoziativ, d.h. sind $f\colon X \to Y$, $g\colon Y \to Z$ und $h\colon Z \to W$ Abbildungen, so sind die Abbildungen $h \circ (g \circ f)$ und $(h \circ g) \circ f\colon X \to W$ gleich.*

Beweis. In jedem $x \in X$ nehmen beide Abbildungen den Wert $h(g(f(x)))$. ∎

Lemma 1.3. *Seien $f\colon X \to Y$ und $g\colon Y \to Z$ Abbildungen.*

a) Ist die Verknüpfung $g \circ f$ injektiv, so muss f injektiv sein.

b) Ist die Verknüpfung $g \circ f$ surjektiv, so muss g surjektiv sein.

Beweis. Hausaufgabe Nr. 10. ∎

Bezeichnung Die *Identitätsabbildung* $\mathrm{Id}_X\colon X \to X$ ist die Abbildung gegeben durch $\forall\, x \in X : \mathrm{Id}_X(x) = x$. Man beachte: Id_X ist bijektiv.

Lemma 1.4. *Sei $f\colon X \to Y$ eine Abbildung. Dann*

a) f bijektiv $\Leftrightarrow$ Es gibt eine Umkehrabbildung *$f^{-1}\colon Y \to X$, die $f \circ f^{-1} = \mathrm{Id}_Y$ und $f^{-1} \circ f = \mathrm{Id}_X$ erfüllt.*

b) Eindeutigkeit von f^{-1}: Sofern f bijektiv ist, gilt: Ist $g\colon Y \to X$ eine Abbildung mit $f \circ g = \mathrm{Id}_Y$ oder $g \circ f = \mathrm{Id}_X$, dann ist $g = f^{-1}$.

Beweis. a): Ist f bijektiv, dann gibt es zu jedem $y \in Y$ genau ein Element $x_y \in X$ mit $f(x_y) = y$. Definieren wir $f^{-1}\colon Y \to X$ durch $f^{-1}(y) = x_y$, so gilt $f \circ f^{-1} = \mathrm{Id}_Y$ sofort, denn $f \circ f^{-1}(y) = f(x_y) = y$. Sei jetzt $x \in X$ und $z = f^{-1}(f(x))$. Es ist $f(z) = f(f^{-1}(f(x))) = (f \circ f^{-1})(f(x)) = f(x)$, denn $f \circ f^{-1} = \mathrm{Id}_Y$. Also $z = x$, denn f ist injektiv. Das heißt, $f^{-1} \circ f = \mathrm{Id}_X$.

Existiert dagegen f^{-1}, so folgt aus Lemma 1.3: Wegen $f \circ f^{-1} = \mathrm{Id}_Y$ ist f surjektiv, und wegen $f^{-1} \circ f = \mathrm{Id}_X$ ist f injektiv.

b): Angenommen f ist bijektiv und $g \circ f = \mathrm{Id}_X$. Dann: Zu jedem $y \in Y$ gibt es wegen f surjektiv ein $x \in X$ mit $f(x) = y$, also

$$g(y) = gf(x) = x = f^{-1}f(x) = f^{-1}(y)\,.$$

Daher $g = f^{-1}$. Ist dagegen $f \circ g = \mathrm{Id}_Y$, dann $fg(y) = y = ff^{-1}(y)$ für alle $y \in Y$, daher $g(y) = f^{-1}(y)$ wegen f injektiv. Wieder gilt $g = f^{-1}$. ∎

1.6 Bild, Einschränkung & Co.

Definition Sei $f\colon X \to Y$ eine Abbildung.

a) Man spricht auch von der Abbildung $x \mapsto f(x)$.

b) Sei $A \subseteq X$ eine Teilmenge. Die *eingeschränkte* Abbildung $f|_A\colon A \to Y$ wird definiert durch $f|_A(x) = f(x)$ für jedes $x \in A$.

c) Ist $A \subseteq X$ eine Teilmenge, so bezeichnet man mit $f(A)$ die *Bildmenge* $f(A) = \{f(x) \mid x \in A\}$ von A. Insbesondere nennt man $f(X)$ das *Bild*[3] von f, es ist also $\text{Bild}(f) = \{f(x) \mid x \in X\}$.

d) Ist $B \subseteq Y$, so definiert man die *Urbildmenge* $f^{-1}(B) \subseteq X$ durch

$$f^{-1}(B) = \{x \in X \mid f(x) \in B\}\,.$$

Ist B die Teilmenge $\{b\}$, die aus einem Element $b \in Y$ besteht, so schreibt man $f^{-1}(b)$ statt $f^{-1}(\{b\})$. Beachten Sie aber, dass $f^{-1}(b)$ kein Element von X ist, sondern eine Teilmenge von X.

Beispiel Sei $f\colon \mathbb{R} \to \mathbb{R}$ die Abbildung $x \mapsto x^2$. Dann

$$\text{Bild}(f) = \mathbb{R}_{\geq 0} \qquad f^{-1}(\{-2, 0, 9\}) = \{-3, 0, 3\}$$
$$f^{-1}(-1) = \emptyset \qquad f^{-1}(4) = \{-2, 2\}\,.$$

1.7 Familien

— Wird nicht vorgelesen —

Man könnte die Geburtstage der Kinder aus der Klasse 1b als eine Menge auffassen. Dies hat aber zwei Nachteile. Erstens erfährt man zwar, dass jemand am 13.8. Geburtstag hat, aber nicht, dass es sich hier um Julie handelt. Zweitens kann zwar die Anzahl der Kinder mit der Anzahl der Geburstage vergleichen, und so feststellen, dass zwei Kinder den gleichen Geburtstag haben muss: aber ob dieser doppelte Geburtstag der 27.3. oder der 4.7. ist, kann man nicht erkennen.

Am besten fasst man die Geburtstage als eine *Familie* auf. Zu einer Familie gehört eine *Indexmenge*, I; in diesem Fall ist I die Menge der Kinder aus der 1b. Eine Familie von Elementen einer Menge M mit Indexmenge I ist eigentlich eine Abbildung $f\colon I \to M$, die man aber als $(m_i)_{i\in I}$ schreibt, wobei $m_i = f(i)$ ist. Zum Beispiel $\text{Geburtstag}_{\text{Julie}} = 13.8$.

Es gibt auch Familien von Mengen, eine typische Schreibweise wäre $(A_i)_{i\in I}$. Zum Beispiel könnte A_i die Menge der AGs sein, die Kind i besucht: etwa

$$A_{\text{Nils}} = \{\text{Badminton}, \text{Hockey}, \text{Schach}\}\,.$$

Liegt eine Familie von Mengen vor, so kann man die Vereinigung und den Schnitt aller Mengen in der Familie bilden:

$$\bigcup\{A_i \mid i \in I\} = \bigcup_{i\in I} A_i = \{x \mid \exists i \in I\colon x \in A_i\}$$
$$\bigcap\{A_i \mid i \in I\} = \bigcap_{i\in I} A_i = \{x \mid \forall i \in I\colon x \in A_i\}$$

Im obigen Beispiel ist $\bigcup\{A_i \mid i \in I\}$ die Menge aller AGs, die von irgendeinem Kind aus der 1b besucht werden, und $\bigcap_{i\in I} A_i$ ist die (vermutlich leere) Menge aller AGs, die jedes Kind aus der 1b besucht.

[3] Auf Englisch *Image*

1.8 Äquivalenzrelationen

Wir führen Relationen ein. Die wichtigsten Relationen sind Äquivalenzrelationen (etwa „Peter und Sabine haben den gleichen Geburtstag“) sowie Ordnungsrelationen (etwa „Jena hat weniger Einwohner als Erfurt“).

Definition Sei X eine Menge. Eine (binäre) *Relation* auf X ist eine Teilmenge $R \subseteq X \times X$. Sind $x, y \in X$, so schreibt man meistens $x \; R \; y$ anstelle von $(x, y) \in R$. Somit ist $x \; R \; y$ eine Aussage, und deshalb entweder wahr oder falsch.

Eine Relation heißt

- *reflexiv*, falls $x \; R \; x$ gilt für jedes $x \in X$.
- *symmetrisch*, falls $x \; R \; y$ genau dann gilt, wenn $y \; R \; x$ gilt.
- *transitiv*, falls $x \; R \; z$ aus $x \; R \; y$ und $y \; R \; z$ folgt.

Eine *Äquivalenzrelation* ist eine Relation, die reflexiv, symmetrisch und transitiv ist. Typischerweise bezeichnet man eine Äquivalenzrelation mit $\sim$, also $x \sim y$ anstelle von $x \; R \; y$.

Beispiele

- X = alle Städte Deutschlands: Relation „liegt im gleichen Bundesland als“ ist eine Äquivalenzrelation.
- X = die Kinder aus der 6b: Relation „hat den gleichen Geburtstag als“ ist eine Äquivalenzrelation.
- $X = \mathbb{R}^3$ mit $(u_1, u_2, u_3) \; R \; (v_1, v_2, v_3) \;\Leftrightarrow$ stimmen an mindestens *zwei* Stellen übereinstimmen: *keine* Äquivalenzrelation, denn reflexiv und symmetrisch, aber wegen

  $$(1,1,1) \; R \; (1,1,2) \qquad (1,1,2) \; R \; (1,2,2) \qquad (1,1,1) \not R \; (1,2,2)$$

  nicht transitiv.

Definition Ist $\sim$ eine Äquivalenzrelation auf der Menge X, so nennt man die Menge $[x] = [x]_\sim = \{y \in X \mid y \sim x\}$ die *Äquivalenzklasse* eines Elements $x \in X$.

Lemma 1.5. *Sei $\sim$ eine Äquivalenzrelation auf der Menge X. Dann ist $x \in [x]$ für jedes $x \in X$, wegen Reflexivität. Außerdem sind für $x, y \in X$ folgende drei Aussagen äquivalent:*

a) $x \sim y$

b) $[x] \cap [y] \neq \emptyset$.

c) $[x] = [y]$

Beweis. Wir führen den *Ringschluss* a) ⇒ b) ⇒ c) ⇒ a).

a) ⇒ b): Ist $x \sim y$, dann $x \in [y]$. Wegen Reflexivität ist aber $x \in [x]$. Also $x \in [x] \cap [y]$.

b) ⇒ c): Wegen b) gibt es ein $z \in [x] \cap [y]$. Ist $w \in [x]$, dann $w \sim x$. Wegen $z \in [x]$ ist $z \sim x$, also $x \sim z$ wegen Symmetrie. Aus $w \sim x$ und $x \sim z$ folgt $w \sim z$ wegen Transitivität. Aufgrund von $z \in [y]$ gilt $z \sim y$, also $w \sim y$ wegen Transitivität, also $w \in [y]$. Wir haben gezeigt, dass $[x] \subseteq [y]$. Analog folgt $[y] \subseteq [x]$, also $[y] = [x]$.

c) ⇒ a): Es ist $x \underset{\text{reflexiv}}{\in} [x] \underset{\text{c)}}{=} [y]$, also $x \sim y$. ∎

Bemerkung Somit stellen die Äquivalenzklassen von $\sim$ eine *Partition* der Menge X dar, d.h. X ist die Vereinigung von disjunkten, nichtleeren Äquivalenzklassen.

Definition Ist $\sim$ eine Äquivalenzrelation auf der Menge X, so bezeichnet man mit $X/\sim$ die Menge aller Äquivalenzklassen: $X/\sim = \{[x] \mid x \in X\}$.

Beispiel Auf $X =$ die zwölf Monate ist „gleich lang“ eine Äquivalenzrelation[4].

$$\begin{aligned} X/\sim &= \{[\text{Januar}], [\text{Februar}], [\text{April}]\} \\ &= \left\{ \begin{array}{l} \{\text{Januar}, \text{März}, \text{Mai}, \text{Juli}, \text{August}, \text{Oktober}, \text{Dezember}\}, \\ \{\text{Februar}\}, \{\text{April}, \text{Juni}, \text{September}, \text{November}\} \end{array} \right\}. \end{aligned}$$

Lemma 1.6. *Sei $\sim$ eine Äquivalenzrelation auf der Menge X. Sei $f\colon X \to Y$ eine Abbildung mit folgender Eigenschaft:*

$$\textit{Für alle } x, x' \in X \textit{ mit } x \sim x' \textit{ gilt } f(x) = f(x').$$

Dann definiert die Vorschrift $\bar{f}([x]) := f(x)$ eine Abbildung $\bar{f}\colon X/\sim \to Y$.

Beweis. Wir müssen zeigen, dass $\bar{f}$ wohldefiniert ist, also repräsentantenunabhängig. Ist $[x] = [x']$, dann $x \sim x'$, also $f(x) = f(x')$, weshalb $\bar{f}([x]) = \bar{f}([x'])$ gilt, wie erwünscht. ∎

[4]Sofern wir das Problem – wegen Schaltjahren – mit Reflexivität in Bezug auf Februar übersehen.

2 Gruppen

Ein Körper ist ein zulässiger Skalarenbereich. In einem Körper kann man addieren, subtrahieren, multiplizieren und dividieren. Der Körperbegriff wird schrittweise aufgebaut; zuerst kommen Gruppen und Ringe.

2.1 Der Gruppenbegriff

Definition Eine Gruppe $G = (G, *)$ besteht aus einer Menge G und einer Operation $*\colon G \times G \to G$ mit den folgenden drei Eigenschaften:

(G1) Assoziativität: $x * (y * z) = (x * y) * z$ für alle $x, y, z \in G$.

(G2) Neutrales Element: Es gibt $e \in G$, so dass $x * e = e * x = x$ für jedes $x \in G$.

(G3) Inversen: Zu jedem $x \in G$ gibt es $x' \in G$ mit $x * x' = e = x' * x$.

Eine Gruppe G heißt *abelsch*, falls $x * y = y * x$ gilt für alle $x, y \in G$. Die *Ordnung* von G ist $|G|$:= Anzahl der Elemente von G. Ist $|G|$ endlich, so heißt G eine *endliche* Gruppe.

Beispiele a) $G = \mathbb{Z}$ mit $x * y = x + y$. Es ist $e = 0$, $x' = -x$. Abelsch. Analog sind auch $(\mathbb{Q}, +)$ und $(\mathbb{R}, +)$ abelsch.

b) $G = \mathbb{R}^\times = \{x \in \mathbb{R} \mid x \neq 0\}$ mit $x * y = xy$ (Multiplikation). Es ist $e = 1$, $x' = \frac{1}{x}$.

c) Die *triviale* Gruppe $G = \{e\}$, mit $e * e = e$. Neutrales Element e, und $e' = e$.

d) Die Menge $G = \{+1, -1\}$, mit Multiplikation. Es ist $e = 1$, $x' = \frac{1}{x} = x$. Eine endliche Gruppe: $|G| = 2$.

e) Die symmetrische Gruppe S_n oder $\mathrm{Sym}(\Omega)$, s. unten. Wichtig für Kombinatorik (einschl. Kartenspiele), und für die Determinante (Kapitel 11). Bereits S_3 ist nichtabelsch.

f) Siehe Kapitel 13: Die *Matrizengruppen* GL_n, SL_n, $O(n)$, $SO(n)$, $U(n)$ und $SU(n)$ sind wichtig für Geometrie und Physik.

Lemma 2.1. *Sei G eine Gruppe.*

a) Es gibt in G genau ein neutrales Element e.

b) Zu jedem $x \in G$ gibt es genau ein Inverses $x' \in G$. Dieses nennt man daher x^{-1}.

c) Seien $a, b \in G$. Dann ist die Gleichung $a * x = b$ eindeutig lösbar für $x \in G$; und $y * a = b$ ist eindeutig lösbar für y.

d) Es ist $(x * y)^{-1} = y^{-1} * x^{-1}$ *für alle* $x, y \in G$.

e) Für jedes $x \in G$ *gilt* $(x^{-1})^{-1} = x$.

f) Es ist $e^{-1} = e$.

Beweis. a),b): Hausaufgabe Nr. 14.
c): Fall $a * x = b$: eine Lösung ist $x = a' * b$, denn

$$a * (a' * b) = (a * a') * b = e * b = b\,.$$

Es gibt keine weitere Lösung, denn ist x eine Lösung, dann aus $a * x = b$ folgt

$$a' * b = a' * (a * x) = (a' * a) * x = e * x = x\,.$$

Der Beweis für $y * a = b$ ist recht analog, die Lösung ist $y = b * a'$.
d): Nach c) reicht es zu zeigen: $(x * y) * (y^{-1} * x^{-1}) = e$. Assoziativität:

$$\begin{aligned}(x * y) * (y^{-1} * x^{-1}) &= ((x * y) * y^{-1}) * x^{-1} \\ &= (x * (y * y^{-1})) * x^{-1} = (x * e) * x^{-1} = x * x^{-1} = e\,.\end{aligned}$$

e): Folgt aus c), denn $x^{-1} * (x^{-1})^{-1} = e = x^{-1} * x$.
f): Folgt nach c) aus $e * e = e$. ∎

2.2 Permutationen und die symmetrische Gruppe

Für eine beliebige Menge Ω erklärt man die *symmetrische Gruppe* $\mathrm{Sym}(\Omega)$ als die Menge aller Bijektionen von Ω nach sich selbst.

$$\mathrm{Sym}(\Omega) = \{f\colon \Omega \to \Omega \mid f \text{ ist eine Bijektion}\}\,.$$

Dies ist eine Gruppe bezüglich Verküpfung: $f * g = f \circ g$. Die Identitätsabbildung $\mathrm{Id}\colon \Omega \to \Omega$ ist das neutrale Element, die Umkehrfunktion ist das Inverse. Die Elemente von $\mathrm{Sym}(\Omega)$ nennt man *Permutationen* von Ω.

Häufig beschäftigt man sich mit dem Fall $\Omega = \{1, 2, 3, \ldots, n\}$. In diesem Fall schreibt man einfach S_n für die symmetrische Gruppe $\mathrm{Sym}(\Omega)$.

Zykelschreibweise für Permutationen

Definition Für $r \geq 2$ heißt die Permutation $\sigma \in S_n$ ein *r-Zykel*, wenn es paarweise verschiedene Elemente $x_1, \ldots, x_r \in \{1, \ldots, n\}$ gibt mit

$$\sigma(x_i) = x_{i+1} \text{ für } 1 \leq i < r \qquad \sigma(x_r) = x_1 \qquad \sigma(x) = x \text{ sonst}$$

Schreibweise: $\sigma = (x_1\ x_2\ x_3\ \ldots\ x_r)$.

Beispiele a) In S_4 ist $(1\ 2\ 4) = (2\ 4\ 1) = (4\ 1\ 2)$ die Permutation

$$1 \mapsto 2 \qquad 2 \mapsto 4 \qquad 3 \mapsto 3 \qquad 4 \mapsto 1$$

b) Einen 2-Zykel nennt man eine *Transposition*. Die Transposition $(1\ 3) \in S_4$ ist die Permutation

$$1 \mapsto 3 \qquad 2 \mapsto 2 \qquad 3 \mapsto 1 \qquad 4 \mapsto 4$$

c) Zykel $(x_1\ x_2\ x_3\ \ldots\ x_r)$ und $(y_1\ y_2\ \ldots\ y_s)$ heißen *disjunkt*, falls kein x_i ein y_j ist. So sind $(1\ 2\ 5)$ und $(3\ 4\ 6)$ disjunkt, aber $(1\ 2\ 5)$ und $(3\ 4\ 5)$ sind nicht disjunkt.

d) Disjunkte Zykel kommutieren miteinander, z.B. in S_6 ist $(1\ 2\ 5)(3\ 4\ 6) = (3\ 4\ 6)(1\ 2\ 5)$ die Permutation

$$1 \mapsto 2 \qquad 2 \mapsto 5 \qquad 3 \mapsto 4 \qquad 4 \mapsto 6 \qquad 5 \mapsto 1 \qquad 6 \mapsto 3\,.$$

Dagegen kommutieren die nicht-disjunkten Permutationen $(1\ 2)$ und $(1\ 3)$ nicht miteinander:

$$(1\ 2)(1\ 3) = (1\ 3\ 2) \qquad\qquad (1\ 3)(1\ 2) = (1\ 2\ 3)\,.$$

Das erste Produkt bildet 2 nach 1 ab, das zweite bildet 2 nach 3 ab. Somit sind die Produkte tatsächlich nicht gleich – und die Gruppe S_n ist nicht-abelsch für alle $n \geq 3$.

e) $(1\ 2\ 3\ 4\ 5\ 6)^{-1} = (1\ 6\ 5\ 4\ 3\ 2)$.

f) Die Permutation $\sigma \in S_6$ gegeben durch

$$1 \mapsto 3 \qquad 2 \mapsto 5 \qquad 3 \mapsto 1 \qquad 4 \mapsto 6 \qquad 5 \mapsto 2 \qquad 6 \mapsto 4$$

ist kein Zykel, lässt sich aber ein Produkt von paarweise disjunkten Zykeln schreiben: $\sigma = (1\ 3)(2\ 5)(4\ 6)$.

Lemma 2.2. *Jede Permutation $\sigma \in S_n$ lässt sich schreiben als ein Produkt von paarweise disjunkten Zykeln. Von der Reihenfolge der Faktoren abgesehen, ist diese Zerlegung eindeutig.*

Beispiel Während des Beweises rechnen wir das Beispiel $\sigma \in S_{10}$ geben durch

$$\begin{array}{lllll} 1 \mapsto 9 & 2 \mapsto 2 & 3 \mapsto 7 & 4 \mapsto 3 & 5 \mapsto 1 \\ 6 \mapsto 8 & 7 \mapsto 10 & 8 \mapsto 6 & 9 \mapsto 5 & 10 \mapsto 4 \end{array}$$

Beweis. Betrachten wir die Folge 1, $\sigma(1)$, $\sigma^2(1)$, ... Da diese unendliche Folge Werte in der endlichen Menge $\{1, 2, \ldots, n\}$ annimmt, muss es Wiederholungen geben. Sei $\sigma^r(1)$ der erste Wert, der bereits einmal vorkam: Das heißt, $1, \sigma(1), \ldots, \sigma^{r-1}(1)$ sind paarweise verschieden, und $\sigma^r(1) = \sigma^s(1)$ für ein $1 \leq s \leq r-1$. Aber dann $\sigma^{r-s}(1) = \sigma^0(1) = 1$, also nach Wahl von r muss $s = 0$ sein: Also $\sigma^r(1) = 1$, und σ operiert auf der Menge $\{1, \sigma(1), \ldots, \sigma^{r-1}(1)\}$ als der r-Zykel $(1\ \sigma(1)\ \sigma^2(1)\ \cdots\ \sigma^{r-1}(1))$ – bzw. 1 wird durch σ gar nicht bewegt im Falle $r = 1$.

Jetzt streichen wir die Zahlen $1, \sigma(1), \ldots, \sigma^{r-1}(1)$. Sei a die kleinste Zahl, die übrig bleibt. Jetzt machen wir das gleiche für die Folge $a, \sigma(a), \sigma^2(a), \ldots$, und machen dann weiter, bis alle Zahlen abgearbeitet sind.

Eindeutigkeit: Sei $b \in \{1, \ldots, n\}$ beliebig, und sei r die kleinste Zahl mit $\sigma^r(b) = b$. Wie oben im Fall $b = 1$ sind $b, \sigma(b), \ldots, \sigma^{r-1}(b)$ paarweise verschieden, und der r-Zykel $(b\ \sigma(b)\ \cdots\ \sigma^{r-1}(b))$ muss in jeder Zykelzerlegung von σ vorkommen. ∎

2.3 Gruppenhomomorphismen und das Vorzeichen

Definition Seien G, H Gruppen. Eine Abbildung $f\colon G \to H$ heißt ein *Homomorphismus*, falls $f(x * y) = f(x) * f(y)$ gilt für alle $x, y \in G$.

Lemma 2.3. *Ist $f\colon G \to H$ ein Homomorphismus, dann*

$$f(e_G) = e_H \qquad\qquad \forall\, g \in G : f(g^{-1}) = [f(g)]^{-1}\,.$$

Beweis. Hausaufgabe Nr. 15. ∎

Beispiele a) $f\colon \mathbb{Z} \to \mathbb{Z}$, $f(n) = 2n$.

b) Die Exponentialfunktion $\exp\colon (\mathbb{R}, +) \to (\mathbb{R}^\times, \times)$, $x \mapsto e^x$: Ein Homomorphismus, denn $e^{x+y} = e^x \cdot e^y$.

c) Das Vorzeichen einer Permutation.

Definitionsversuch (problematisch) Jede Permutation lässt sich schreiben als ein Produkt von Transpositionen (Beweis später). Ist σ das Produkt von N Transpositionen, dann definiert man das Vorzeichen $\varepsilon(\sigma)$ durch $\varepsilon(\sigma) := (-1)^N$.

Warum problematisch? Wie können wir wissen, dass es keine Permutation σ gibt, die sich sowohl als Produkt von fünf Transpositionen als auch als Produkt von sechsunddreißig Permutationen schreiben lässt? Dann wäre $\varepsilon(\sigma)$ nicht wohldefiniert, denn $(-1)^5 = -1$ und $(-1)^{36} = +1$.

Stattdessen verwendet man die folgende, hochgradig nicht anschauliche Definition. Ihr einziger Vorteil ist, dass sie den Wert von $\varepsilon(\sigma)$ zweifelsfrei festlegt: aber um Eigenschaften nachzuweisen und Rechenregeln herzuleiten, ist einiges an Arbeit erforderlich.

Definition Das *Vorzeichen* $\varepsilon(\sigma)$ einer Permutation $\sigma \in S_n$ ist

$$\varepsilon(\sigma) := \prod_{1 \le i < j \le n} \frac{\sigma(j) - \sigma(i)}{j - i}\,.$$

Beispiel In S_3:

$$\varepsilon(1\ 2\ 3) = \frac{3-2}{2-1} \cdot \frac{1-2}{3-1} \cdot \frac{1-3}{3-2} = \frac{1}{1} \cdot \frac{-1}{2} \cdot \frac{-2}{1} = +1$$
$$\varepsilon(1\ 3) = \frac{2-3}{2-1} \cdot \frac{1-3}{3-1} \cdot \frac{1-2}{3-2} = \frac{-1}{1} \cdot \frac{-2}{2} \cdot \frac{-1}{1} = -1\,.$$

Lemma 2.4. *Sei $n \ge 1$ und $\sigma \in S_n$.*

a) Es ist $\varepsilon(\sigma) = (-1)^N$ für

$$N = \textit{Anzahl der Paare } i, j \textit{ mit } i < j \textit{ und } \sigma(i) > \sigma(j)\,.$$

b) Für $\sigma, \tau \in S_n$ ist $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$.

Bei der Berechnung des Vorzeichens helfen:

c) Ist $\sigma \in S_n$ eine Transposition*, d.h. ein 2-Zykel, so ist $\varepsilon(\sigma) = -1$.*

d) Ist $\sigma \in S_n$ ein r-Zykel, dann ist $\varepsilon(\sigma) = (-1)^{r-1}$.

Beispiel $(1\ 4\ 7\ 2\ 9\ 11)(3\ 10\ 5)(6\ 8)$ hat Vorzeichen $(-1)^{6-1} \cdot (-1)^{3-1} \cdot (-1)^{2-1} = (-1) \cdot 1 \cdot (-1) = +1$.

Beweis. a): Jedes Paar $i < j$ kommt einmal als $j - i$ im Nenner und einmal als $\pm(j - i)$ im Zähler: $+$ falls $\sigma^{-1}(j) > \sigma^{-1}(i)$ und $-$ sonst.

b): Wegen $\dfrac{\sigma(j) - \sigma(i)}{j - i} = \dfrac{\sigma(i) - \sigma(j)}{i - j}$ hängt $\dfrac{\sigma(j) - \sigma(i)}{j - i}$ nur vom *ungeordneten* Paar i, j ab. Also

$$\begin{aligned}\varepsilon(\sigma\tau) &= \prod_{\substack{\text{ungeordnete} \\ \text{Paare } i \ne j}} \frac{\sigma\tau(j) - \sigma\tau(i)}{j - i} \\ &= \prod_{\substack{\text{ungeordnete} \\ \text{Paare } i \ne j}} \left(\frac{\sigma\tau(j) - \sigma\tau(i)}{\tau(j) - \tau(i)}\right) \cdot \prod_{\substack{\text{ungeordnete} \\ \text{Paare } i \ne j}} \left(\frac{\tau(j) - \tau(i)}{j - i}\right)\,.\end{aligned}$$

Aber $\displaystyle\prod_{\substack{\text{ungeordnete} \\ \text{Paare } i \ne j}} \left(\frac{\sigma\tau(j) - \sigma\tau(i)}{\tau(j) - \tau(i)}\right) = \prod_{\substack{\text{ungeordnete} \\ \text{Paare } i \ne j}} \left(\frac{\sigma(j) - \sigma(i)}{j - i}\right)$, weshalb

$$\varepsilon(\sigma\tau) = \prod_{\substack{\text{ungeordnete} \\ \text{Paare } i \ne j}} \left(\frac{\sigma(j) - \sigma(i)}{j - i}\right) \cdot \prod_{\substack{\text{ungeordnete} \\ \text{Paare } i \ne j}} \left(\frac{\tau(j) - \tau(i)}{j - i}\right) = \varepsilon(\sigma)\varepsilon(\tau)\,.$$

c): Es gibt also $i < j$ mit $\sigma(i) = j$, $\sigma(j) = i$ und $\sigma(\ell) = \ell$ sonst. Die Anzahl der Paare in a) ist also ungerade: das Paar i, j, sowie die beiden Paare i, ℓ und ℓ, j für jedes $i < \ell < j$.

d): $(x_1\ x_2\ \ldots\ x_r) = (x_1\ x_r)(x_1\ x_2\ \ldots\ x_{r-1})$. Ergebnis folgt per Induktion über r nach b) und c). ∎

Korollar 2.5. *a) Das Vorzeichen ist ein Gruppenhomomorphismus* $\varepsilon\colon S_n \to (\{+1, -1\}, \times)$.

b) Jede Permuation $\sigma \in S_n$ *lässt sich als ein Produkt von Transpositionen schreiben. Ist* σ *das Produkt von* N *Transpositionen, dann* $\varepsilon(\sigma) = (-1)^N$.

Beweis. a): Folgt aus Lemma 2.4 a) und b).

b): Nach der Zykelschreibweise ist jede Permutation ein Produkt von Zykeln. Nach dem Beweis von Lemma 2.4 d) ist jeder Zykel ein Produkt von Transpositionen. Die zweite Aussage folgt aus a) und Lemma 2.4 c). ∎

3 Ringe und Körper

3.1 Ringe

Definition Ein *Ring* $R = (R, +, \cdot)$ besteht aus einer Menge R zusammen mit Abbildungen $+\colon R \times R \to R$, $(x, y) \mapsto x+y$ und $\cdot\colon R \times R \to R$, $(x, y) \mapsto x \cdot y = xy$, die die folgenden Bedingungen erfüllen:

(R1) $(R, +)$ ist eine abelsche Gruppe. Das neutrale Element nennen wir 0_R.

(R1) Multiplikation $\cdot$ ist assoziativ: $(xy)z = x(yz)$.

(R3) Distributivgesetze: $x(y + z) = xy + xz$ und $(x + y)z = xz + yz$ für alle $x, y, z \in R$.

(R4) Eins: Multiplikation $\cdot$ hat ein neutrales Element $1 = 1_R$, das *Einselement*.

Der Ring heißt *kommutativ*, falls $xy = yx$ gilt für alle $x, y \in R$.

Beispiele a) $\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}$ sind Ringe bezüglich der üblichen Addition und Multiplikation.

b) Ist R ein Ring und $n \geq 1$, so ist die Menge $M_n(R)$ aller $n \times n$-Matrizen über R ein Ring bezüglich Matrixaddition und -multiplikation (s. unten). $M_2(\mathbb{R})$ ist nicht kommutativ, denn

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad \text{aber} \quad \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

c) Der Nullring $R = \{0\}$ mit $0 + 0 = 0 \cdot 0 = 0$ ist ein Ring, mit $1_R = 0_R = 0$.

d) Die Menge $\mathbb{R}[X]$ aller Polynome mit Koeffizienten aus $\mathbb{R}$ ist ein Ring, denn man kann Polynome addieren und multiplizieren.

Lemma 3.1. *Sei R ein Ring. Dann:*

a) Es gibt nur ein Einselement in R.

b) $\forall\, x \in R \qquad 0 \cdot x = x \cdot 0 = 0.$

c) $\forall\, x, y \in R \qquad x \cdot (-y) = (-x) \cdot y = -(xy).$

d) $(-1)^2 = 1.$

Beweis. a): Sind $1_a, 1_b$ zwei Einselemente, dann ist einerseits $1_a \cdot 1_b = 1_a$, denn 1_b ist ein Einselement; andererseits ist $1_a \cdot 1_b = 1_b$, denn 1_a ist ein Einselement. Also ist $1_a = 1_a \cdot 1_b = 1_b$.

b): Wegen $0+0=0$ gilt $0\cdot x=(0+0)\cdot x=0\cdot x+0\cdot x$. Zieht man $0\cdot x$ von beiden Seiten ab, so folgt $0\cdot x=0$. Analog zeigt man $x\cdot 0=0$.

c): Für $x\cdot(-y)=-(xy)$ reicht es zu zeigen: $xy+x\cdot(-y)=0$. Aber $xy+x(-y)=x(y+(-y))=x\cdot 0=0$. Analog zeigt man $(-x)y=-(xy)$.

d): Nach Lemma 2.1 c) reicht es zu zeigen: $(-1)^2+(-1)=0$. Dies ist auch der Fall, denn

$$(-1)^2+(-1)=(-1)\cdot(-1)+1\cdot(-1)=((-1)+1)\cdot(-1)=0\cdot(-1)=0\,. \quad \blacksquare$$

3.2 Matrizen

Hier ist eine (3×2)-Matrix mit Einträgen aus $\mathbb{R}$: $\begin{pmatrix} 1 & 2 \\ 4 & -7 \\ 0,5 & \pi \end{pmatrix}$.

Definition Sei R ein Ring und n,m ganze Zahlen ≥ 1. Eine $(m\times n)$-Matrix mit Einträgen aus R besteht aus mn Elemente von R, aufgestellt in m Zeilen und n Spalten.

Ist A eine solche Matrix, so bezeichnet man mit A_{ij} der Eintrag an der Stelle (i,j), d.h. in der $i$ten Zeile und der $j$ten Spalte.

Beispiel Für $A=\begin{pmatrix} 1 & 3 & 7 & 4 \\ 3 & 1 & 2 & 9 \\ 8 & 0 & 7 & 3 \end{pmatrix}$ ist $A_{23}=2$.

Bezeichnung Die Menge der $(m\times n)$-Matrizen mit Einträgen aus R werden wir mit $R^{m\times n}$ bezeichnen. Besonders wichtig ist der Fall $m=n$, man schreibt $M_n(R)$ für $R^{n\times n}$. Eine Matrix heißt *quadratisch*, wenn die Anzahl der Zeilen und der Spalten gleich sind.

Matrixaddition und -multiplikation Für Matrizen $A,B\in R^{m\times n}$ wird die Summe $A+B\in R^{m\times n}$ definiert durch $(A+B)_{ij}=A_{ij}+B_{ij}$ für alle i,j.

Beispiel $\begin{pmatrix} 1 & 2 & 4 \\ 2 & 5 & 7 \end{pmatrix}+\begin{pmatrix} 0 & 3 & 1 \\ 1 & 1 & 1 \end{pmatrix}=\begin{pmatrix} 1 & 5 & 5 \\ 3 & 6 & 8 \end{pmatrix}$.

Sind $A\in R^{m\times n}$ und $B\in R^{n\times p}$ Matrizen, so wird das Produkt $AB\in R^{m\times p}$ definiert durch

$$(AB)_{ik}=A_{i1}B_{1k}+A_{i2}B_{2k}+A_{i3}B_{3k}+\cdots+A_{in}B_{nk}=:\sum_{j=1}^{n}A_{ij}B_{jk}\,.$$

Beispiel

$$\begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix} \begin{pmatrix} 0 & 2 & 4 \\ 1 & 3 & 5 \end{pmatrix} = \begin{pmatrix} 1\cdot 0+0\cdot 1 & 1\cdot 2+0\cdot 3 & 1\cdot 4+0\cdot 5 \\ 3\cdot 0+1\cdot 1 & 3\cdot 2+1\cdot 3 & 3\cdot 4+1\cdot 5 \end{pmatrix}$$
$$= \begin{pmatrix} 0 & 2 & 4 \\ 1 & 9 & 17 \end{pmatrix}.$$

Bemerkung Beachten Sie: das Produkt AB ist nur dann definiert, wenn A die gleiche Anzahl von Spalten hat, wie B Zeilen hat.

Die *Einheitsmatrix* $E_n \in M_n(R)$ ist gegeben durch $(E_n)_{ij} = \delta_{ij} = \begin{cases} 1 & i = j \\ 0 & \text{sonst} \end{cases}$.

Lemma 3.2. *a) Matrixmultiplikation ist assoziativ.*

b) Für $A \in R^{m\times n}$ gilt $A \cdot E_n = A$. Für $B \in R^{n\times p}$ gilt $E_n \cdot B = B$.

Beweis. a): Sei $A \in R^{m\times n}$, $B \in R^{n\times p}$ und $C \in R^{p\times q}$. Für $1 \le i \le m$ und $1 \le \ell \le q$ ist

$$[(AB)C]_{i\ell} = \sum_{k=1}^{p} (AB)_{ik} C_{k\ell} = \sum_{k=1}^{p} \left(\sum_{j=1}^{n} A_{ij} B_{jk} \right) C_{k\ell} = \sum_{j=1}^{n} \sum_{k=1}^{p} A_{ij} B_{jk} C_{k\ell}$$
$$= \sum_{j=1}^{n} A_{ij} \left(\sum_{k=1}^{p} B_{jk} C_{k\ell} \right) = \sum_{j=1}^{n} A_{ij} (BC)_{j\ell} = [A(BC)]_{i\ell}\,.$$

b): Selber nachrechnen. ∎

Auf ähnlicher Weise zeigt man, dass Matrixaddition und -multiplikation die Distributivgesetze erfüllen. Somit ist $M_n(R)$ ein Ring, mit Einselement E_n.

3.3 Körper

Definition Ein *Körper* k ist ein kommutativer Ring, die zwei weiteren Begindungen erfüllt:

(K1) In k gilt $1 \neq 0$.

(K2) $\forall\, x \in R$ gilt: Ist $x \neq 0$, dann gibt es $y \in R$ mit $xy = 1$.
Man schreibt dann $x^{-1} = y$.

Alternative Fassung der Definition Ein *Körper* k ist ein kommutativer Ring derart, dass $k^\times := k \setminus \{0\}$ eine Gruppe[5] bezüglich Multiplikation ist.

[5] Notwendigerweise abelsch, da der Ring kommutativ ist.

In einem Körper gelten genau die Regeln, die man von Skalaren erwartet.

Beispiele a) $\mathbb{R}$ und $\mathbb{Q}$ sind Körper.

b) Die komplexen Zahlen bilden einen Körper $\mathbb{C}$ (s. unten).

c) $\mathbb{Z}$ ist kein Körper, denn 2 liegt in $\mathbb{Z}$ aber $\frac{1}{2}$ nicht.

d) Der Nullring $\{0\}$ ist kein Körper, denn in diesem Fall gilt $1 = 0$.

e) $M_2(\mathbb{R})$ ist kein Körper, denn Matrixmultiplikation ist nicht kommutativ.

f) Die Menge $\{0, 1\}$ bildet einen Körper, genannt $\mathbb{F}_2$, mit Addition und Multiplikation gegeben durch

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

g) Die Menge $\{0, 1, 2\}$ bildet einen Körper, genannt $\mathbb{F}_3$, mit Addition und Multiplikation gegeben durch

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

3.4 Der Körper $\mathbb{C}$ der komplexen Zahlen

Definition Der Körper $\mathbb{C}$ der komplexen Zahlen besteht aus der Menge $\mathbb{R}^2$, zusammen mit der üblichen komponentenweise Addition

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

und mit der folgenden Multiplikationsregel:

$$(a, b)(c, d) := (ac - bd, ad + bc)\,. \qquad (*)$$

Bezeichnung Ist $z = (a, b) \in \mathbb{C}$, so nennt man a bzw. b den reellen Teil $\Re(z)$ bzw. den imaginären Teil $\Im(z)$ von z. Durch $|z| := \sqrt{a^2 + b^2}$ wird der Betrag von z definiert. Man schreibt $i = (0, 1) \in \mathbb{C}$ und identifiziert $a \in \mathbb{R}$ mit $(a, 0) \in \mathbb{C}$. Dann $ib = (0, 1)(b, 0) = (0, b)$, also gilt

$$a + ib = (a, b)\,.$$

Mit dieser Schreibweise lautet die Multiplikationsregel:

$$(a + ib)(c + id) = (ac - bd) + i(ad + bc)\,. \qquad (**)$$

Insbesondere gilt $i^2 = -1$.

Lemma 3.3. $\mathbb{C}$ *ist tatsächlich ein Körper.*

Beweis. Offensichtlich ist $(\mathbb{R}^2, +)$ eine abelsche Gruppe. Wir definieren eine Abbildung $M\colon \mathbb{C} \to M_2(\mathbb{R})$ wie folgt: Für $z = (a, b) \in \mathbb{C}$ ist

$$M(z) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

Da man a und b von der ersten Spalte von $M(z)$ ablesen kann, ist die Abbildung M injektiv.

Das gute an dieser Abbildung M ist, dass sie sich mit Addition und Multiplikation verträgt: das heißt, für $w = (c, d)$ ist

$$\begin{aligned} M(z) + M(w) &= \begin{pmatrix} a & -b \\ b & a \end{pmatrix} + \begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \begin{pmatrix} a+c & -(b+d) \\ b+d & a+c \end{pmatrix} = M(z+w) \\ M(z)M(w) &= \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \cdot \begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \begin{pmatrix} ac-bd & -(ad+bc) \\ ad+bc & ac-bd \end{pmatrix} = M(zw)\,. \end{aligned}$$

Da die Matrixmultiplikation assoziativ ist, ist auch die komplexe Multiplikation assoziativ: sind $z, w, v \in \mathbb{C}$, dann

$$\begin{aligned} M((zw)v) = M(zw)M(v) &= (M(z)M(w))M(v) \\ &= M(z)(M(w)M(v)) = M(z)M(wv) = M(z(wv))\,. \end{aligned}$$

Auf der gleichen Weise zeigt man, dass die Distributivgesetze erfüllt werden. Dass $(a, b)(c, d) = (c, d)(a, b)$ gilt, sieht man aus der Multiplikationsregel (*). Das Einselement ist $(1, 0)$, das Nullelement ist $(0, 0)$. Man rechnet nach, dass jedes $z \neq 0$ ein Inverses z^{-1} hat:

$$(a, b)^{-1} = \left(\frac{a}{a^2 + b^2}, -\frac{b}{a^2 + b^2} \right).$$

Somit ist $\mathbb{C}$ tatsächlich ein Körper. ∎

Bezeichnung Für $z = (a, b)$ wird die komplex konjugierte komplexe Zahl $\bar{z}$ durch $\bar{z} = (a, -b)$ definiert. Das heißt, für $a, b \in \mathbb{R}$ ist $\overline{a + bi} = a - bi$.

Lemma 3.4. *Seien $z, w \in \mathbb{C}$. Dann*

a) $\overline{z + w} = \bar{z} + \bar{w}$.

b) $\overline{zw} = \bar{z} \cdot \bar{w}$.

c) Es ist $z \in \mathbb{R}$ genau dann, wenn $z = \bar{z}$.

d) $z \cdot \bar{z} = |z|^2$. *Für $z \neq 0$ gilt also* $z^{-1} = \frac{\bar{z}}{|z|^2}$.

Beweis. a), b): Hausaufgabe Nr. 25.

c): $z = (a, b)$ liegt genau dann in $\mathbb{R}$, wenn $b = 0$ gilt. Dies ist genau dann der Fall, wenn $b = -b$ gilt, d.h. wenn $(a, b) = (a, -b)$ gilt.

d): Es ist $(a, b)(a, -b) = (a^2 + b^2, 0)$. Diese komplexe Zahl wird mit $a^2 + b^2 \in \mathbb{R}$ identifiziert. ∎

Beispiel $$\frac{1+3i}{2-i} = \frac{(1+3i)(2+i)}{(2-i)(2+i)} = \frac{-1+7i}{2^2+1} = -\frac{1}{5} + \frac{7}{5}i.$$

4 Vektorräume

4.1 Der Vektorraum-Begriff

Definition Sei k ein Körper. Ein *k-Vektorraum* $V = (V, +, \cdot)$ besteht aus

- einer Menge V,
- einer *Vektoraddition* $V \times V \to V$, $(v, w) \mapsto v + w$, und
- einer *Skalarmultiplikation* $k \times V \to V$,

dabei müssen die folgenden Bedingungen erfüllt sein:

(V1) $(V, +)$ ist eine abelsche Gruppe. Das neutrale Element nennt man den *Nullvektor* $\underline{0}$.

(V2) Skalarmultiplikation assoziativ: $(\lambda\mu)v = \lambda(\mu v)$ für alle $\lambda, \mu \in k$ und alle $v \in V$.

(V3) Distributivität in v: $\lambda(v + w) = \lambda v + \lambda w$ für alle $\lambda \in k$ und alle $v, w \in V$.

(V4) Distributivität in λ: $(\lambda + \mu)v = \lambda v + \mu v$ für alle $\lambda, \mu \in k$ und alle $v \in V$.

(V5) Normierung: $1 \cdot v = v$ für jedes $v \in V$.

Beispiele Hier sind einige *reelle* Vektorräume, d.h. mit $k = \mathbb{R}$:

a) Geometrische Vektoren im dreidimensionalen Anschauungsraum.

b) $\mathbb{R}^n$

c) $C^0(\mathbb{R})$, die Menge aller stetigen Abbildungen $f\colon \mathbb{R} \to \mathbb{R}$. Mit Addition und Skalarmultiplikation punktweise: $(f + g)(x) := f(x) + g(x)$, $(\lambda f)(x) := \lambda \cdot f(x)$.

d) Alle Folgen in $\mathbb{R}$. Auch alle konvergente Folgen.

e) $\mathbb{C}$

f) Die Lösungsmenge eines homogenen linearen Gleichungssystems.

g) Alle Polynome, auch alle vom Grad höchstens n.

Bemerkung Hausaufgabe Nr. 28: Ist V ein k-Vektorraum, so gelten $\lambda \cdot \underline{0} = \underline{0} = 0 \cdot v$ und $(-\lambda)v = -(\lambda v) = \lambda(-v)$ für alle $\lambda \in k$ und alle $v \in V$.

Lemma 4.1. *Sei V ein k-Vektorraum. Erfüllen $\lambda \in k$ und $v \in V$ die Gleichung $\lambda v = \underline{0}$, so ist $\lambda = 0$ oder $v = \underline{0}$.*

Beweis. Wir zeigen: Ist $\lambda v = \underline{0}$ aber $\lambda \neq 0$, dann gilt $v = \underline{0}$. Da λ ein Element $\neq 0$ des Körpers k ist, gibt es ein $\mu \in k$ mit $\mu\lambda = 1$. Es ist dann

$$\underline{0} = \mu\underline{0} = \mu(\lambda v) = (\mu\lambda)v = 1v = v\,. \qquad \blacksquare$$

Beispiele Vektorräume über andere Körper $k \neq \mathbb{R}$:

a) k^n für beliebiges k.

b) $k^{m\times n}$ für beliebiges k.

c) Alle analytische Funktionen auf $\mathbb{C}$, für $k = \mathbb{C}$.

d) Alle Bytes (d.h. Folgen von 8 Bits) für $k = \mathbb{F}_2$; die Addition ist die Operation XOR, die Skalarmultiplikation ist durch $1v = v$, $0v = \underline{0}$ definiert.

e) Die Potenzmenge $\mathscr{P}(M)$ einer Menge M, für $k = \mathbb{F}_2$. Die Addition ist die symmetrische Differenz $\triangle$ von Mengen:

$$A \triangle B := \{x \mid x \text{ liegt in genau einer der Mengen } A, B\} = (A \cup B) \setminus (A \cap B)\,.$$

Diese Operation ist assoziativ, denn

$$(T_1 \triangle T_2) \triangle T_3 = T_1 \triangle (T_2 \triangle T_3) = \left\{ x \;\middle|\; \begin{array}{l} x \text{ liegt entweder in genau einer der Mengen} \\ T_1, T_2, T_3, \text{ oder in allen drei} \end{array} \right\}.$$

Der Nullvektor ist $\emptyset$, und $-T = T$. Die Skalarmultiplikation ist $1T = T$, $0T = \emptyset$.

f) $\mathbb{R}$ für $k = \mathbb{Q}$.

Bemerkung Die Vorstellung, dass die Elemente eines Vektorraums Vektoren sind, ist manchmal hilfreich – und manchmal nicht.

4.2 Linearkombinationen, lineare Abhängigkeit

Definition Sei V ein k-Vektorraum, und seien $v, v_1, v_2, \ldots, v_n$ Vektoren aus V. Gibt es Skalare $\lambda_1, \lambda_2, \ldots, \lambda_n \in k$ derart, dass

$$v = \sum_{i=1}^{n} \lambda_i v_i \text{ gilt,} \qquad \text{das heißt } v = \lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n\,,$$

so heißt v eine *Linearkombination* von $v_1, v_2 \ldots, v_n$.

Beispiele a) Jedes $v \in \mathbb{R}^3$ ist eine $\mathbb{R}$-lineare Kombination von $e_1 = (1, 0, 0)$, $e_2 = (0, 1, 0)$ und $e_3 = (0, 0, 1)$, denn $(x, y, z) = xe_1 + ye_2 + ze_3$.

b) In $V = \mathbb{R}^3$ sei $v_1 = (1, 3, 1)$ und $v_2 = (0, 2, 1)$. Der Vektor $u = (2, 0, -1)$ ist eine Linearkombination von v_1, v_2, denn $u = 2v_1 - 3v_2$. Dagegen ist $w = (1, 0, 1)$ keine Linearkombination von v_1, v_2: wäre nämlich $w = \lambda v_1 + \mu v_2$, dann $(\lambda, 3\lambda + 2\mu, \lambda + \mu) = (1, 0, 1)$. Ein Koeffizientenvergleich ergibt $\lambda = 1$, $\lambda + \mu = 1$ (weshalb $\mu = 0$) und $3\lambda + 2\mu = 0$, weshalb $3 = 0$, ein Widerspruch.

c) Der Nullvektor $\underline{0}$ ist eine Linearkombination jedes Systems $v_1, v_2, \ldots, v_n$ von Vektoren: man setzt $\lambda_i = 0$ für jedes i.

d) In $V = k^4$ sei $v_1 = (1, 0, 1, 0)$, $v_2 = (0, 1, 0, 1)$, $v_3 = (1, 1, 1, 0)$, $v_4 = (1, 1, 0, 0)$ und $v_5 = (0, 0, 1, 1)$. Der Vektor $v = (1, 1, 1, 1,)$ hat zwei verschiedene Darstellungen als eine Linearkombination von v_1, v_2, v_3, v_4, v_5: $v = v_1 + v_2$ und $v = v_4 + v_5$.

Somit ist $v_1 + v_2 - v_4 - v_5$ der Nullvektor. Das heißt, es gibt zwei verschiedene Darstellungen des Nullvektors als eine Linearkombination: die *triviale* Darstellung $\underline{0} = 0v_1 + 0v_2 + 0v_3 + 0v_4 + 0v_5$ sowie die nichttriviale Darstellung $\underline{0} = 1v_2 + 1v_2 + 0v_3 + (-1)v_4 + (-1)v_5$.

Definition Ein System $v_1, v_2, \ldots, v_n$ von Vektoren heißt *linear abhängig*, wenn der Nullvektor sich als eine nichttriviale Linearkombination des Systems darstellen lässt, d.h. wenn es Skalare $\lambda_1, \lambda_2, \ldots, \lambda_n \in k$ gibt, die nicht alle Null sind und trotzdem $\sum_{i=1}^n \lambda_i v_i = \underline{0}$ erfüllen.

Beispiele a) Im obigen Beispiel sind die Vektoren v_1, v_2, v_3, v_4, v_5 linear abhängig.

b) In $V = C^0(\mathbb{R})$ sind die Funktionen $f(x) = 2x$, $g(x) = 3x$ und $h(x) = x^2$ linear abhängig, denn $3f - 2g + 0h$ ist die konstante Funktion mit Wert 0.

Definition Ein System von Vektoren $v_1, v_2, \ldots, v_n$ heißt *linear unabhängig*, wenn es nicht linear abhängig ist. Das heißt: $v_1, v_2, \ldots, v_n$ sind linear unabhängig, wenn gilt: sind $\lambda_1, \lambda_2, \ldots, \lambda_n \in k$ Skalare mit der Eigenschaft, dass $\sum_{i=1}^n \lambda_i v_i = \underline{0}$ gilt, so muss $\lambda_i = 0$ gelten für jedes i.

Beispiele a) Das System $v_1 = (1, 3, 1)$, $v_2 = (0, 2, 1)$ ist linear unabhängig in $\mathbb{R}^3$, denn: ist $\lambda v_1 + \mu v_2 = \underline{0}$, dann $(\lambda, 3\lambda + 2\mu, \lambda + \mu) = (0, 0, 0)$. Komponentenvergleich: $\lambda = 0$; $\lambda + \mu = 0$, also $\mu = 0$.

Sogar das System $v_1, v_2, v_3 = (1, 0, 1)$ ist linear unabhängig: ist $\lambda v_1 + \mu v_2 + \nu v_3 = \underline{0}$, dann $(\lambda + \nu, 3\lambda + 2\mu, \lambda + \mu + \nu) = (0, 0, 0)$. Komponentenvergleich:

$$\lambda + \nu = 0 \quad \text{(I)} \qquad 3\lambda + 2\mu = 0 \quad \text{(II)} \qquad \lambda + \mu + \nu = 0 \quad \text{(III)}\,.$$

(III) − (I): $\mu = 0$. Aus (II) folgt $\lambda = 0$, aus (I) folgt jetzt $\nu = 0$. Also $\lambda = \mu = \nu = 0$.

Das System $v_1, v_2, v_3, v_4 = (0, 1, 0)$ dagegen ist nicht linear unabhängig, denn $v_1 = v_3 + 3v_4$, also $1 \cdot v_1 + 0 \cdot v_2 + (-1) \cdot v_3 + (-3) \cdot v_4 = \underline{0}$.

b) In $C^0(\mathbb{R})$ sei $f(x) = 1$, $g(x) = x^2$ und $h(x) = e^x - 1$. Diese drei Funktionen sind linear unabhängig, denn: angenommen es ist $\lambda f(x)+\mu g(x)+\nu h(x) = 0$ für jedes $x \in \mathbb{R}$. Wir setzen $x = 0$ ein und erhalten $\lambda \cdot 1 + \mu \cdot 0 + \nu \cdot 0 = 0$, d.h. $\lambda = 0$. Jetzt setzen wir $x = 1$ und $x = -1$ ein:

$$\mu + \nu(e - 1) = 0 \quad \text{(I)} \qquad\qquad \mu + \nu(e^{-1} - 1) = 0 \quad \text{(II)}$$

(I) − (II): $\nu(e - e^{-1}) = 0$, also $\nu = 0$. Aus (I) folgt dann $\mu = 0$. Also $\lambda = \mu = \nu = 0$.

4.3 Untervektorräume, Erzeugendensysteme

Definition Sei V ein k-Vektorraum und $U \subseteq V$ eine Teilmenge. Ist U selbst ein Vektorraum, und zwar mit der gleichen Addition und Skalarmultiplikation wie V, dann nennt man U einen *Untervektorraum* von V.

Anders gesagt: $U \subseteq V$ ist ein Untervektorraum, falls $\underline{0}$ in U liegt, und außerdem $u + v$ und λu in U liegen $\forall u, v \in U$, $\forall \lambda \in k$. Die Gesetze (Assoziativität usw.) gelten dann in U, denn sie gelten sogar in V.

Lemma 4.2. *Eine Teilmenge U eines k-Vektorraums V ist genau dann ein Untervektorraum, wenn folgende Bedingungen gelten:*

$$\text{a) } U \neq \emptyset \qquad\qquad \text{b) } \lambda u + \mu v \in U \text{ für alle } \lambda, \mu \in k, \forall u, v \in U.$$

Beweis. Untervektorraum ⇒ Bedingungen: Wegen $\underline{0} \in U$ ist $U \neq \emptyset$. Da U bezüglich Skalarmultiplikation abgeschlossen ist, liegen λu, μv in U. Da U auch bezüglich Addition abgeschlossen ist, liegt $\lambda u + \mu v$ in U.

Bedingungen ⇒ Untervektorraum: Wegen $U \neq \emptyset$ gibt es ein $u_0 \in U$. Dann ist $\underline{0} = u_0 - u_0 = 1u_0 + (-1)u_0$ ein Element von U. Sind $u, v \in U$, dann liegen auch $u + v = 1u + 1v$, $-u = (-1)u + 1 \cdot \underline{0}$ und $\lambda u = \lambda u + 1 \cdot \underline{0}$ in U. ∎

Beispiele a) Aufgrund der Grenzwertsätze ist die Menge aller konvergenten Folgen in $\mathbb{R}$ ein Untervektorraum des $\mathbb{R}$-Vektorraums aller Folgen.

b) Die Menge P_5 aller Polynome vom Grad höchstens 5 ist ein Untervektorraum des Vektorraums aller Polynome. Die Menge aller Polynome vom Grad 5, die außerdem eine Nullstelle in $x = 2$ haben, ist widerum ein Untervektorraum von P_5.

c) Die Lösungsmenge des linearen Gleichungssystems $x_1 + x_2 - 3x_3 - x_4 = x_2 + 5x_4 = 0$ ist ein Untervektorraum des $\mathbb{R}^4$.

Definition Sei V ein k-Vektorraum und $v_1, v_2, \ldots, v_n$ ein System von Elementen aus V. Das *Erzeugnis* $\langle v_1, \ldots, v_n \rangle$ des Systems ist

$$\langle v_1, v_2, \ldots, v_n \rangle := \{v \in V \mid v \text{ ist eine Linearkombination von } v_1, \ldots, v_n\}.$$

Manche Autoren sagen *lineare Hülle* statt Erzeugnis.

Lemma 4.3. *$U := \langle v_1, \ldots, v_n \rangle$ ist ein Untervektorraum von V. Es ist der kleinste Untervektorraum, der $v_1, \ldots, v_n$ enthält.*

Beweis. Mit $\lambda_i = 0$ für jedes i sieht man, dass $\underline{0}$ im Erzeugnis liegt. Sind $\lambda, \mu \in k$ und $u, v \in \langle v_1, \ldots, v_n \rangle$, so gibt es Skalare $a_1, a_2, \ldots, a_n,\ b_1, b_2, \ldots, b_n \in k$ mit $u = \sum_{i=1}^n a_i v_i$, $v = \sum_{i=1}^n b_i v_i$. Es ist dann $\lambda u + \mu v = \sum_{i=1}^n c_i v_i$, wobei $c_i \in k$ für jedes $1 \leq i \leq n$ durch $c_i = \lambda a_i + \mu b_i$ gegeben wird. Folglich liegt auch $\lambda u + \mu v$ im Erzeugnis. Nach Lemma 4.2 ist U ein Untervektorraum.

U enthält jedes v_i: man setzt $\lambda_j = \begin{cases} 1 & j = i \\ 0 & \text{sonst} \end{cases}$, dann ist $\sum_{j=1}^n \lambda_j v_j = v_i$.

Ist $W \subseteq V$ ein Untervektorraum mit $v_1, \ldots, v_n \in W$, dann $U \subseteq W$, denn $\sum_{i=1}^n \lambda_i v_i \in W$. Dies zeigen wir per Induktion über n: Es ist $\lambda_1 v_1 \in W$, da $v_1 \in W$ und W ein Untervektorraum. Ist nun $w := \sum_{i=1}^{n-1} \lambda_i v_i \in W$, dann $\sum_{i=1}^n \lambda_i v_i = 1 \cdot w + \lambda_n v_n \in W$, da W Untervektorraum. Und wegen $U \subseteq W$ ist U tatsächlich der kleinster Untervektorraum, der $v_1, \ldots, v_n$ enthält. ∎

Definition Sei V ein k-Vektorraum, und $v_1, v_2, \ldots, v_n$ ein System von Elemente aus V. Gilt $V = \langle v_1, v_2, \ldots, v_n \rangle$, so heißt $v_1, v_2, \ldots, v_n$ ein *Erzeugendensystem* von V.

Ein Vektorraum mit einem (endlichen) Erzeugendensystem heißt *endlich-dimensional*.

In dieser Vorlesung beschäftigen wir uns vorwiegend mit endlich dimensionalen Vektorräumen.

Beispiele a) $(1,0)$, $(0,1)$ ist ein Erzeugendensystem von $\mathbb{R}^2$. $(1,0)$, $(1,1)$ ist ein weiteres Erzeugendensystem. $(1,2)$, $(3,1)$, $(4,4)$ ist noch eins.

b) $(1,2,1)$, $(1,1,1)$, $(1,0,1)$ ist kein Erzeugendensystem des $\mathbb{R}^3$, da $(2,0,1)$ keine Linearkombination dieser drei Vektoren ist.

Beispiel 4.4. Der reelle Vektorraum aller reellwertigen Polynome mit reellen ist nicht endlich dimensional.

Begründung: Angenommen doch, dann gibt es ein Erzeugendensystem der Form $p_1(X), \ldots, p_n(X)$. Setze

$$d := \max\{\operatorname{grad}(p_i) \mid 1 \leq i \leq n\}.$$

Da $p_1, \ldots, p_n$ ein Erzeugendensystem ist, gibt es (konstante) Skalare $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$ mit

$$X^{d+1} = \sum_{i=1}^n \lambda_i p_i(X).$$

Jetzt $(d+1)$-mal ableiten: Die rechte Seite wird zu Null, während die linke Seite zu $(d+1)!$ wird, Widerspruch.