Albert-Ludwigs-Universität Freiburg

Lineare Algebra I

Inoffizieller Mitschrieb

Stand: 18. Dezember 2017

Vorlesung gehalten von:

Prof. Dr. Patrick Dondl
Abteilung für Angewandte Mathematik

Einführung

- Das Wort Algebra stammt aus dem arabischen „al-jabr“.
- Allgemein ist Algebra die Lehre der mathematischen Symbole und deren Manipulation.
- Lineare Algebra: Insbesondere lineare Gleichungen

Aufbau der Vorlesung

1. Lineare Gleichungssysteme und der n-dimensionale reellen Raum
2. Grundlegende Objekte
3. Gruppen, Ringe, Körper
4. Vektorräume und lineare Abbildungen
5. Determinanten
6. Eigenwerte und Normalformen

Beispiel: Der Google-Pagerank

Gegeben seien vier Seiten mit Verlinkungen zwischen diesen Seiten. Von einer nicht verlinkten Seite wechselt man zufällig auf eine andere Seite. Der User startet an einer zufälligen Stelle und folgt von dort einem zufälligen Link auf eine andere Seite. Zusätzlich wird immer mit Wahrscheinlichkeit $(1-d),\ d \in [0,1]$ auf eine beliebige Website gewechselt.
Die wichtigste Seite ist nun die, auf welcher ein Benutzer sich mit der höchsten Wahrscheinlichkeit aufhält.

$$p(\delta_1) = \frac{1-d}{N} + d\left(\frac{p(\delta_2)}{1}, \frac{p(\delta_5)}{4}\right)$$
$$p(\delta_2) = \frac{1-d}{N} + d\left(\frac{p(\delta_1)}{3}, \frac{p(\delta_5)}{4}\right)$$
$$\vdots$$

Zur Berechnung von $p(\delta_j), j \in \{1..5\}$ gibt es Methoden aus der linearen Algebra.

Inhaltsverzeichnis

0 Lineare Gleichungssysteme und der n-dimensionale reelle Raum **3**
0.1 Der $\mathbb{R}^n$ . . . 3
0.2 Ein wenig euklidische Geometrie . . . 8
0.2.1 Geraden und Ebenen . . . 8
0.2.2 Das Skalarprodukt . . . 9

1 Grundlegende Objekte **11**
1.1 Elementare Aussagenlogik . . . 11
1.2 Mengen und Abbildungen . . . 12
1.3 Gruppen . . . 17
1.4 Ringe und Körper . . . 20

2 Vektorräume **25**
2.1 Definitionen und elementare Eigenschaften . . . 25
2.2 Basis und Dimension . . . 28

3 Lineare Abbildungen **35**
3.1 Definition und grundlegende Eigenschaften . . . 35

Stichwortverzeichnis **39**

0. Lineare Gleichungssysteme und der n-dimensionale reelle Raum

- Descartes führte "Koordinaten" ein in der Geometrie ein, also Zahlensysteme. Das führte dazu, das man nun leichter rechnen kann.
- Wir benutzen hier die reellen Zahlen (mit den üblichen Rechenregeln für die Addition):
  - $(x + y) + z = x + (y + z)$
  - $0 + x = x + 0 = x$
  - Es gibt für jedes x ein y mit $x + y = 0$, wir nennen dieses y das additiv inverse zu x ("-x").
  - $x + y = y + x$

  Und für Multiplikation:
  - $\lambda(x + y) = \lambda x + \lambda y$
  - $(\lambda + \mu)x = \lambda x + \mu x)$
  - $\lambda(\rho\mu) = (\lambda\rho)\mu$
  - $1x = x$
- Weiterhin brauchen wir die natürlichen Zahlen, die $1, 2, 3 \ldots$

0.1 Der $\mathbb{R}^n$

Für gegebenes $n \in \mathbb{N}$ definieren wir:

$$\mathbb{R}^n = \{x = (x_1, x_2, \ldots, x_n) : x_1, \ldots, x_n \in \mathbb{R}\}$$

Hierbei ist $(x_1, \ldots, x_n)$ ein geordnetes n-Tupel, die Reihenfolge beim Vergleich Elemente dieser Art ist wichtig.
Weiterhin gilt: $x, y, \in \mathbb{R} : x = y \Leftrightarrow x_1 = y_1, x_2 = y_2, \ \ldots \ x_n, = y_n$
Wir nennen diese n-Tupel auch Vektoren im $\mathbb{R}^n$.
Mit $\mathbb{R}^0$ bezeichnen wir die Menge $\{0\}$, welche nur das Nullelement enthält. Allgemein übertragen sich die Rechenregeln von $\mathbb{R}$. Wir schreiben:

$$x + y = (x_1 + y_1, \ldots, x_n + y_n) \text{ für } x, y \in \mathbb{R}^n \qquad \text{Vektoraddition}$$
$$\lambda x = (\lambda x_1, \ldots, \lambda x_n) \qquad \text{Skalarmultiplikation}$$

Definition – Lineare Gleichungssysteme

Eine lineare Gleichung über $\mathbb{R}$ ist ein Ausdruck der Form: $\alpha_1 x_1 + \alpha_2 x_2 + \ldots \alpha_n x_n = \beta$ für reelle Zahlen $\beta, \alpha_1, \ldots, \alpha_n \in \mathbb{R}$. Einen Vektor, $\xi = (\xi_1, \ldots, \xi_n) \in \mathbb{R}^n$ nennen wir Lösung, wenn die reellen Zahlen $\xi_1, \ \ldots \ , \xi_n$ eingesetzt in $x_1, \ldots, x_n$ die Gleichung erfüllen.
Ein lineares Gleichungssystem G ist ein System der Form

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \ \dots \ + a_{1n}x_n \ &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \ \dots \ + a_{2n}x_n \ &= b_2 \\ \vdots \qquad \vdots \qquad \ddots \qquad \vdots \qquad &\vdots \\ a_{m1}x_1 + a_{m2}x_2 + \ \dots \ + a_{mn}x_n &= b_m \end{aligned}$$

Die einzelnen Komponenten lassen sich auch zusammenfassen als

$$\sum_{j=1}^{n} a_{i,j}x_j = b_i \quad i \in \{1, \dots, m\}$$

oder, noch kürzer, in Matrixschreibweise:

$$Ax = b$$

Dabei bezeichnet A eine sog. Matrix mit den Einträgen $a_{i,j},\ i \in [0,\ \dots\ , m],\ j \in [0,\ \dots\ , n]$, wir schreiben

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$$

Ax für $x \in \mathbb{R}^n$ ist dann eine Kurzform für $\sum_{i=1}^{n} a_{ij}x_j$ mit einem Vektor $x = (x_1, \dots, x_n) \in \mathbb{R}^n$. Das Ergebnis ist ein Vektor $b = (b_1, \dots, b_m) \in \mathbb{R}^m$ für eine Matrix A mit m Zeilen und n Spalten.
Der Vektor b heißt rechte Seite des linearen Gleichungssystems, A heißt Koeffizientenmatrix des linearen Gleichungssystems. Eine Spalte, bzw. Zeile von A kann mit einem Vektor im $\mathbb{R}^m$ bzw. im $\mathbb{R}^n$ identifiziert werden. Wir sprechen von Spalten-, bzw. Zeilenvektoren der Matrix A.
Eine Matrix mit m Zeilen und n Spalten nennen wir $m \times n$ - Matrix. Für $x \in \mathbb{R}^n$, A eine $m \times n$ - Matrix und B eine $l \times m$ - Matrix gilt die Rechenregel $BAx = B(Ax)$. Ein Gleichungssystem $Ax = b$ heißt homogen, falls b der Nullvektor $(0, \dots, 0)$ ist und quadratisch für $m = n$ (eine quadratische Matrix A).

Definition – Normalform

Ein Gleichungssystem $Ax = b$ ist in Normalform, falls A die Gestalt

$$\begin{pmatrix} & 1 & 0 & 0 & \cdots & 0 & a_{1,k+1} & \cdots & a_{1,n} \\ & 0 & 1 & 0 & \cdots & 0 & a_{2,k+1} & \cdots & a_{2,n} \\ & 0 & 0 & 1 & \cdots & 0 & a_{3,k+1} & \cdots & a_{3,n} \\ & \vdots & \vdots & \vdots & \ddots & \vdots & \cdots & \ddots & \vdots \\ k & 0 & 0 & 0 & \cdots & 1 & a_{k,k+1} & \cdots & a_{k,n} \\ & \underbrace{\qquad\qquad\qquad\qquad}_{k} & & & & & & & \\ & 0 & & \cdots & & 0 & 0 & \cdots & 0 \\ & \vdots & & \ddots & & \vdots & \vdots & \ddots & \vdots \\ & 0 & & \cdots & & 0 & 0 & \cdots & 0 \end{pmatrix} \qquad \text{für ein } k \in \mathbb{N}_0$$

annimmt. Beispiele:

$$\begin{pmatrix} 1 & 0 & 3 \\ 0 & 1 & 4 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \qquad \text{Ist in Normalform mit } k = 2.$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad \text{Ist in Normalform mit } k = 3.$$

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \qquad \text{Ist in Normalform mit } k = 0.$$

Wir nennen k den Rang der Matrix A (bzw. des Gleichungssystems). Es gilt $0 \leq k \leq \min(m, n)$. Ein Gleichungssystem ist genau dann lösbar, wenn gilt: $b_{k+1} = b_{k+2} = \ldots = b_m = 0$. In diesem Fall lässt sich eine Lösung $\xi \in \mathbb{R}^n$ bestimmen, indem man $\xi_{k+1}, \ldots, \xi_n$ beliebig wählt, und danach $\xi_i = b_i - \sum_{j=k+1}^{n} a_{i,j}\xi_j,\ i \in \{1, \ldots, n\}$ wählt. Wir sagen die Lösungsmenge ist

$$\mathbb{L} = \left\{ \left(b_1 - \sum_{j=k+1}^{n} a_{1j}\xi_j \right), \ldots, \left(b_k - \sum_{j=k+1}^{n} a_{kj}\xi_j \right), \xi_{k+1}, \ldots, \xi_n \middle| \xi_{k+1}, \ldots, \xi_n \in \mathbb{R} \right\}$$

Wir nennen eine solche Menge $(n-k)$-parametrig.

Beispiel:

$$\begin{pmatrix} 1 & 0 & 3 \\ 0 & 1 & 4 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} x = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

Wähle $x_3 = 1$. Dann folgt daraus $x_2 = -3$ und $x_1 = -2$.

Lemma 0.1

Sei A eine $m \times n$ -Matrix mit Rang k. Dann gilt $k = n$ genau dann, wenn alle Gleichungssysteme mit A höchstens eine Lösung haben, und $k = m$, genau dann, wenn alle Gleichungssysteme mit A lösbar sind.
Beweis: klar aus der Darstellung.

Definition – Zeilenoperationen

Eine Zeilenoperation macht aus einem Gleichungssystem ein neues Gleichungssystem durch Multiplikation der i-ten Zeile mit einer Zahl $\lambda \in \mathbb{R} \setminus 0$ oder durch Addieren des λ-fachen der i-ten Zeile zur j-ten Zeile $(i \neq j)$. Wir bezeichnen diese Operationen mit Z_i^λ bzw. $Z_{i,j}^\lambda$.
Die Umkehrung von $Z_i^\lambda = Z_i^{\frac{1}{\lambda}}$, die Umkehrung von $Z_{i,j}^\lambda = Z_{i,j}^{-\lambda}$
Bemerkung: Die Zeilenoperationen sind umkehrbar.

Lemma 0.2

Ein Gleichungssystem G', welches aus einem Gleichungssystem G durch Zeilenoperationen hervorgeht, besitzt die gleichen Lösungen wie G.
Beweis:
Für Z_I^λ : betrachten wir nur die i-te Zeile:

$$a_{i,1}x_1 + \cdots + a_{i,n}x_n = b_i$$

Nach Z_i^λ:

$$\lambda a_{i,1}x_1 + \cdots + \lambda a_{i,n}x_n = \lambda b_i$$

Diese besitzen eindeutig die selbe Lösungen $\xi_1, \ldots, \xi_n$, ebenso für $Z_{i,j}^\lambda$.

Satz 0.3 – Gauß-Jordan-Elimination

Jedes lineare Gleichungssystem lässt sich durch Zeilenoperationen und Vertauschungen von Variablen (d.h. Vertauschung von Spalten) in Normalform bringen.

Beweis: Wir beweisen dies mittels eines expliziten Algorithmus' (der Gauß-Jordan-Elimination). Aus praktischen Gründen schreiben wir unser Gleichungssystem als sogenannte erweiterte Koeffizientenmatrix.

$$\left(\begin{array}{cccc|c} a_1 1 & a_1 2 & \cdots & a_1 n & b_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_m 1 & a_m 2 & \cdots & a_m n & b_m \end{array}\right)$$

Zunächst vergewissern wir uns, dass wir durch vermehrte Anwendung von $Z^1_{i,j}, Z^{-1}_{j,i}, Z^1_{i,j}$und Z_i^{-1} die i-te und j-te Zeile vertauschen können.
Sei y die i-te Zeile, z die j-te Zeile.

$$\begin{pmatrix} y \\ z \end{pmatrix} \xrightarrow{Z^1_{i,j}} \begin{pmatrix} y \\ z+y \end{pmatrix} \xrightarrow{Z^{-1}_{j,i}} \begin{pmatrix} -z \\ z+y \end{pmatrix} \xrightarrow{Z^1_{i,j}} \begin{pmatrix} -z \\ y \end{pmatrix} \xrightarrow{Z_i^{-1}} \begin{pmatrix} z \\ y \end{pmatrix}$$

Schritt 1: Falls alle Koeffizienten $a_{i,j} = 0$ sind, so ist die Matrix bereits in Normalform, und es ist nichts mehr zu tun.
Falls es einen von 0 verschiedenen Koeffizienten gibt, so können wir diesen durch Spalten- und Zeilenvertauschungen in die linke obere Ecke bringen. Damit ist nun $a_{1,1} \neq 0$. Nach $Z_1^{\frac{1}{a_{1,1}}}$ gilt $a_{1,1} = 1$. Nun wenden wir $Z_{1,2}^{-a_{2,1}}, \ldots, Z_{1,m}^{-a_{m,1}}$ und erhalten $a_{2,1} = \cdots = a_{m,1} = 0$. Die Matrix hat nun die Form

$$\left(\begin{array}{cccc|c} 1 & a_{1,2} & \ldots & a_{1,n} & b_1 \\ 0 & \ddots & & & \\ 0 & & \ddots & & \vdots \\ \vdots & & & \ddots & \\ 0 & a_{m,2} & \ldots & a_{m,n} & b_m \end{array}\right)$$

Schritt 2: Falls $a_{i,j} = 0$ für $2 \leq i \leq m$ und $2 \leq j \leq n$, so ist die Matrix in Normalform für k=1 und wir sind fertig. Falls nicht, so existiert $i \geq 2, j \geq 2$ mit $a_{i,j} \neq 0$.
Wir vertauschen die i-te Zeile mit der zweiten Zeile, und die j-te Spalte mit der zweiten Spalte. Damit ist $a_{2,2} \neq 0$. Nun wenden wir $Z_2^{\frac{1}{a_{2,2}}}$ an. Damit ist $a_{2,2} = 1$. Jetzt wenden wir $Z_{2,1}^{-a_{1,2}}, \ldots, Z_{2,m}^{-a_{m,2}}$ an und erhalten die Form:

$$\left(\begin{array}{ccccc|c} 1 & 0 & a_{1,3} & \ldots & a_{1,n} & b_1 \\ 0 & 1 & a_{2,3} & \ldots & a_{1,n} & b_2 \\ 0 & 0 & \ddots & & & b_3 \\ \vdots & & & \ddots & & \vdots \\ 0 & 0 & a_{m,3} & \ldots & a_{m,n} & b_m \end{array}\right)$$

Wir verwandeln damit der Reihe nach die Spalten der Matrix in Spalten, in welchen nur der Diagonaleintrag von 0 verschieden ist (dieser Eintrag ist gleich 1). Das Verfahren terminiert, wenn die Matrix in Normalform ist, oder wenn $\min(n, m)$ Schritte vollzogen sind. Auch in diesem Fall ist die Matrix in Normalform. □

Korollar 0.4

Sei A eine Matrix mit m Zeilen und n Spalten. Weiter sei k der Rang einer Normalform von A (d.h. einer Matrix in Normalform, welche aus A durch Zeilenoperationen und Spaltenvertauschungen hervorgeht). Ein Gleichungssystem mit Matrix A besitzt dann entweder keine Lösung, oder ein $(n-k)$-parametriges Lösungssystem. Es gilt $k = n$ genau dann, wenn jedes Gleichungssystem $Ax = b$ höchstens eine Lösung besitzt und $k = m$ genau dann, wenn jedes Gleichungssystem $Ax = b$ mindestens eine Lösung besitzt.

Beweis: Folgt aus Lemma 0.2 und daraus, dass Zeilen-, bzw. Spaltenoperationen die Lösungsmenge (modulo Variablentausch) nicht ändern. □

Korollar 0.5

Ein homogenes Gleichungssystem mit weniger Gleichungen als Variablen hat mindestens eine nicht triviale Lösung.

Beweis: Es gibt für homogene Gleichungssysteme immer die triviale Lösung. Der Rang der Matrix des Gleichungssystems in Normalform sei k. Damit existiert ein $(n-k)$-parametriges Lösungssystem, aber $k \leq min(n,m) \leq m \leq (n-1)$. Somit existiert mindestens eine weitere Lösung. □

Definition 0.6 – Lineare Unabhängigkeit

Eine Kollektion $a_1, \ldots, a_n$ von Vektoren in $\mathbb{R}^m$ heißt linear unabhängig, wenn sich keiner der Vektoren als Linearkombination der anderen Vektoren schreiben lässt.

Bemerkung: Als Linearkombination von $a_1, \ldots, a_n$ bezeichnen wir einen Ausdruck der Form $\alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_n a_n = \sum_{j=1}^{n} \alpha_j a_j$ für $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$

Lemma 0.7

Vektoren $a_1, \ldots, a_n$ sind genau dann linear unabhängig, wenn für alle $\xi_1, \ldots, \xi_n \in \mathbb{R}$ gilt: Falls $\xi_1 a_1 + \cdots + \xi_n a_n = 0$, dann gilt $\xi_1 = \cdots = \xi_n = 0$.

Beweis:

1. Falls $0 = \xi_1 a_1 + \cdots + \xi_n a_n$, und oBdA $\xi_1 \neq 0$ so folgt $a_1 = \sum_{j=2}^{n} -\frac{\xi_j}{\xi_1} a_j$. Somit wurde a_1 als Linearkombination von $a_2, \ldots, a_n$ geschrieben.
2. Falls aber oBdA $a_1 = \sum_{j=2}^{n} \lambda_j a_j$ so gilt: $0 = -a_1 = \sum j = 2^n$, damit ist ξ_1 (der erste Koeffizient) von 0 verschieden.

□

Lemma 0.8

Es seien $a_1, \ldots, a_n \in \mathbb{R}^m$ linear unabhängig und es gelte $b = \lambda_1 a_1 + \cdots + \lambda_n a_n$, mit $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$. Dann ist diese Linearkombination eindeutig.
Beweis: Es sei auch $b = \mu_1 a_1 + \cdots + \mu_n a_n$. Für Eindeutigkeit ist nun zu zeigen, dass $\mu_i = \lambda_i, 1 \leq i \leq n$. Wir ziehen die Gleichungen voneinander ab, und erhalten:

$$b - b = (\lambda_1 - \mu_1)a_1 + \ldots + (\lambda_n - \mu_n)a_n$$

$$\Leftrightarrow \; 0 = (\lambda_1 - \mu_1)a_1 + \ldots + (\lambda_n - \mu_n)a_n$$

Mit Lemma 0.7 folgt die Aussage.

Satz 0.9

Wenn man ein Gleichungssystem durch Zeilenoperationen und Spaltenvertauschungen auf Normalform bringt, so erhält man immer denselben Rang.
Bemerkung: Man kann damit vom Rang eines Gleichungssystems (bzw. einer Matrix) sprechen, auch wenn dieses nicht in Normalform ist.
Bemerkung: Ein einzelner Vektor a gilt als linear unabhängig, solange $a \neq 0$. Die leere Kollektion von Vektoren $(n = 0)$ bezeichnen wir ebenfalls als linear unabhängig.
Vor dem Beweis des Satzes 0.9 noch ein paar Feststellungen:

1. Die Tatsache, dass $(\xi_1, \ldots, \xi_n)$ Lösung eines linearen Gleichungssystems ist, lässt sich als lineare Abhängigkeit $\xi_1 a_1 + \cdots + \xi_n a_n = b$ ausdrücken, wobei a_i eine Spalte der Matrix des Gleichungssystems ist.

2. Ist das Gleichungssystem in Normalform, so sind die ersten k Spaltenvektoren linear unabhängig. Die folgenden $n-k$ Spaltenvektoren lassen sich aber als Linearkombination der ersten k darstellen, also
$$\lambda_{1,i} a_1 + \cdots + \lambda_{k,i} a_k = a_i \text{ für } k < i \leq n \text{ mit } \lambda_{1,i} = a_{1,i}, \ldots$$

3. Falls das Gleichungssystem lösbar ist, kann man dank $\xi_1 a_1 + \cdots + \xi_n a_n = b$ auch b als solche Linearkombination schreiben. Wegen Lemma 0.8 sind diese Linearkombinationen auch eindeutig.

Beweis: Wir bemerken zunächst, dass Zeilenoperationen und Spaltenvertauschung die Anzahl linear unabhängiger Spaltenvektoren nicht ändern. Wir überlegen uns nun, dass der Rang eines linearen Gleichungssystems nichts anderes als die maximale Anzahl linear unabhängiger Spaltenvektoren der Matrix ist.
Die ersten k Spalten sind linear unabhängig, da die Matrix in Normalform ist. Seien also $a_{i_1}, \ldots, a_{i_{k+1}}$ beliebige Spaltenvektoren der Matrix des Gleichungssystems. Nachdem in diesen Vektoren alle Einträge ab dem $k+1$-ten Eintrag 0 sind, hat das Gleichungssystem

$$x_1 a_{i_1} + \cdots + x_{k+1} a_{i_{k+1}} = 0$$

nur k mögliche Gleichungen. (Die Zeilen $k+1$ bis m in diesem Gleichungssystem sind $0 = 0$)
Nach Korollar 0.5 hat dieses homogene Gleichungssystem mit k Gleichungen und $k+1$ Unbekannten aber mindestens eine nicht triviale Lösung. Die Vektoren $a_{i_1}, \ldots a_{i_{k+1}}$ sind somit nicht linear unabhängig. □

Korollar 0.10

Wird ein Gleichungssystem *nur* durch Zeilenoperationen (also ohne Variablentausch) auf Normalform gebracht, so ist die Matrix, die man erhält, immer die gleiche. Falls das Gleichungssystem lösbar ist, so ist auch das erhaltene b immer das gleiche.

0.2 Ein wenig euklidische Geometrie

0.2.1 Geraden und Ebenen

Definition 0.11 – Geraden

1. Sei $v \neq 0$ ein Vektor in $\mathbb{R}^n$. Mit $\mathbb{R}v$ bezeichnen wir die Menge an Vektoren in $\mathbb{R}^n$ der Form $\mathbb{R}v = \{\lambda v : \lambda \in \mathbb{R}\}$
2. Sei $a \in \mathbb{R}^n$, $v \in \mathbb{R}^n$, $v \neq 0$. Als (affine) Gerade bezeichnen wir die Menge der Vektoren der Form $g = \{a + \lambda v : \lambda \in \mathbb{R}\} = a + \mathbb{R}v$

Bemerkung: Der Richtungsraum $\mathbb{R}v$ einer Geraden g ist durch diese eindeutig bestimmt als Menge der Differenzen $x - y$ aus Vektoren in g.

Lemma 0.12

Zwei Geraden $a + \mathbb{R}v, b + \mathbb{R}w$ sind genau dann gleich, wenn gilt $\mathbb{R}v = \mathbb{R}w$ und $a - b \in \mathbb{R}v$.

Beweis: Sei also $x = a + \mathbb{R}v$, d.h. $x = a + \lambda v$ für ein $\lambda \in \mathbb{R}$. Nach Annahme gilt $\mathbb{R}v = \mathbb{R}w$. Damit existiert ein $\mu \in \mathbb{R}$ mit $\lambda v = \mu w$ und somit $x = a + \mu w$. Weiterhin haben wir nach Annahme, dass $a - b \in \mathbb{R}v$, also existiert ein $\xi \in \mathbb{R}$ mit $a - b = \xi w$, also $x = a - (a - b) + \xi w + \mu w$ und somit $x = b + (\xi + \mu)w$. Es ist also $x \in b + \mathbb{R}w$.
Die Umkehrung, also die Behauptung, dass sich ein Punkt $y \in b + \mathbb{R}w$ auch als Punkt in $a + \mathbb{R}v$ schreiben lässt, folgt analog. □

Lemma 0.13

Durch zwei verschiedene Punkte in $\mathbb{R}^n$ geht genau eine Gerade.
Beweis: Übung

Definition 0.14 – Parallelität

Zwei Geraden heißen parallel, wenn sie die gleichen Richtungsräume haben.

Definition 0.15

Eine (affine) Ebene ist eine Menge der Form $a + \mathbb{R}v + \mathbb{R}w$ für linear unabhängige Vektoren v, w.
Bemerkung: Auch hier gilt, das der Raum $\mathbb{R}v + \mathbb{R}w$ eindeutig bestimmt ist als Menge aller Differenzen von Punkten in der Ebene.

Lemma 0.16

Zwei nicht-parallele Geraden, die in einer Ebene liegen, schneiden sich.

Beweis: Es sei $E = c + \mathbb{R}v_1 + \mathbb{R}v_2$ eine Ebene, $g_1 = a_1 + \mathbb{R}b_1$, $g_2 = a_2 + \mathbb{R}b_2$ zwei Geraden in E.
Wir suchen ξ_1, ξ_1, so dass $a_1 + \xi_1 w_1 = a_2 + \xi_2 w_2$. Nun schreiben wir $a_i = c + \beta_{1,i}v_1 + \beta_{2,i}v_2$ und $w_i = \alpha_{1,i}v_1 + \alpha_{2,i}v_2$ für $i = 1, 2$.
Das führt auf das Gleichungssystem

$$\alpha_{1,1}\xi_1 - \alpha_{1,2}\xi_2 = -\beta_{1,1} + \beta_{1,2}$$
$$\alpha_{2,1}\xi_1 - \alpha_{2,2}\xi_2 = -\beta_{2,1} + \beta_{2,2}$$

Nachdem g_1, g_2 nicht parallel sind, sind w_1, w_2 linear unabhängig. Damit sind aber die Spaltenvektoren der Matrix $\begin{pmatrix} \alpha_{1,1} & -\alpha_{1,2} \\ \alpha_{2,1} & -\alpha_{2,2} \end{pmatrix}$ ebenfalls linear unabhängig. Damit besitzt das Gleichungssystem eine Lösung (da $k = m$) nach Satz 0.9. □

0.2.2 Das Skalarprodukt

Im Folgenden seien $a = (a_1, \ldots, a_n), b = (b_1, \ldots, b_n)$ zwei Vektoren in $\mathbb{R}^n$.

Definition 0.17 – Skalarprodukt

Das Skalarprodukt von a und b ist definiert als $(a, b) = \sum_{j=1}^{n} a_j b_j$.

Lemma 0.18

Das Skalarprodukt zweier Vektoren a und b in $\mathbb{R}^n$ ist eine sogenannte symmetrische, positiv definite Bilinearform, das heißt:

1. $(a, b) = (b, a)$ (symmetrisch)
2. $(a + b, c) = (a, c) + (b, c)$ (linear)
3. $(\lambda a, b) = \lambda(a, b)$ (linear)
4. $(a, a) \geq 0$ (positiv definit)
5. $(a, a) = 0$ genau dann, wenn $a = 0$

für alle Vektoren $a, b, c \in \mathbb{R}^n$, alle $\lambda \in \mathbb{R}$.
Bemerkung: aus 1. und 2. folgt $(a, b + c = (a, b) + (a, c)$ und $(a, \lambda b) = \lambda(a, b)$ (Bilinearität).

Beweis: 1., 2., 3. sind klar aus der Definition. 4. und 5. folgen daraus, dass $(a, a) = a_1^2, \ldots, a_n^2$. □

Definition 0.19 – Norm

Die Norm (oder Länge) von a ist $\sqrt{(a, a)} = ||a||$.

Definition 0.20 – Winkel zwischen Vektoren

1. Der Winkel α zwischen zwei Vektoren $a, b \neq 0$ ist definiert durch $0 \leq \alpha \leq \pi$ und $cos(\alpha) = \frac{|(a,b)|}{||a|| \cdot ||b||}$.
2. Zwei Vektoren $a, b \in \mathbb{R}^n$ heißen orthogonal, falls gilt $(a, b) = 0$.

Lemma 0.21 – Cauchy-Schwarzsche Ungleichung

Es gilt $|(a, b)| \leq ||a|| \cdot ||b||$.

Beweis: Es gilt für jedes beliebiges $\lambda \in \mathbb{R}$: $0 \leq (a + \lambda b, a + \lambda b) = (a, a) + 2(\lambda a, b) + \lambda^2(b, b)$. Für $\lambda = -\frac{(a,b)}{(b,b)}$ ergibt sich $0 \leq (a, a) - 2\frac{(a,b)^2}{(b,b)} + \frac{(a,b)^2}{(b,b)}$. Für $b = 0$ ist die Aussage des Lemmas klar. Es folgt $(a, b)^2 \leq (a, a)(b, b)$. Falls a und b linear unabhängig sind so folgt $|(a, b)| < ||a||||b||$, denn dann ist $a + \lambda b \neq 0$ (für jedes $\lambda \in \mathbb{R}$) und die Ungleichung ist strikt (d.h. mit „<“). *Bemerkung:* □

Lemma 0.22 – Dreiecksungleichung

Es gilt $||a + b|| \leq ||a|| + ||b||$.

Beweis: $||a + b||^2 = (a + b, a + b) = ||a||^2 + 2(a, b) + ||b||^2 \leq ||a||^2 + 2||a||||b|| + ||b||^2 = (||a|| + ||b||)^2$ □

Korollar 0.23 – $||x - y||$ ist eine Metrik

Der $\mathbb{R}^n$ mit dem Abstand $d(x, y) = ||x-y||$ ist ein sogenannter metrischer Raum. Das bedeutet folgendes:

1. $d(x, y) \geq 0$
2. $d(x, y) = 0 \Leftrightarrow x = y$
3. $d(x, y) = d(y, x)$
4. $d(x, z) \leq d(x, y) + d(y, z)$

für alle $x, y, z \in \mathbb{R}^n$. Wir nennen d einen Abstand.

1. Grundlegende Objekte

1.1 Elementare Aussagenlogik

Aussagen (in der Mathematik) sind sprachliche Gebilde, welche entweder wahr (w) oder falsch (f) sind.
Darstellung mittels Wahrheitstabelle:
Beispiele:

Aussage	
A: es sind am 2.11.2017 mehr als fünf Personen im Hörsaal Rundbau	w
B: Der Dozent der LA in FR im WS 17/18 heißt Peter	f

Definition 1.1 – Logische Operatoren

A, B seien Aussagen.

1. „$\neg A$“, oder „nicht A“ ist die Negation von A

A	$\neg A$
w	f
f	w

2. Junktoren:
   $A \vee B$, „A oder B“ ist wahr, wenn mindestens eine der Aussagen A, B wahr ist.
   $A \wedge B$, „A und B“ ist wahr, wenn beide Aussagen A, B wahr sind.

A	b	$A \vee B$	$A \wedge B$
w	w	w	w
f	w	w	f
w	f	w	f
f	f	f	f

3. Implikationen:
   $A \Rightarrow B$ ist wahr, wenn A die Aussage B impliziert.
   $A \Leftrightarrow B$ ist wahr, wenn A genau dann wahr ist, wenn B wahr ist.

A	B	$A \Rightarrow B$	$A \Leftrightarrow B$
w	w	w	w
f	w	w	f
w	f	f	f
f	f	w	w

Beispiel: Sei G ein lineares Gleichungssystem mit m Zeilen, n Spalten und Grad k. Dann gilt

$$\begin{array}{lcl} k = n & \Rightarrow & \text{Lösung immer eindeutig.} \\ A & \Rightarrow & B \end{array}$$

Um die Aussage $A \Rightarrow B$ zu zeigen, können wir annehmen, das A wahr ist und müssen folgern, das B ebenfalls wahr ist.

Bemerkung: De Morgansche Gesetze

1. $(\neg A \vee \neg B) = \neg(A \wedge B)$
2. $(\neg A \wedge \neg B) = \neg(A \vee B)$

1.2 Mengen und Abbildungen

Problem: Der Begriff der Menge ist sehr schwer zu definieren (Vgl. Russelsche Antinomie). Endliche Mengen kann man durch Auflistung aller Elemente angeben, z.B. $X = \{x_1, x_2, x_3\}$. x_1, x_2, x_3 heißen dann Elemente von X und wir schreiben $x_1 \in X$.
Reihenfolge der Elemente und Mehrfachauflistung sind nicht relevant. Die Mächtigkeit einer Menge ist die Anzahl paarweise verschiedener Elemente. $\{1, 2, 2, 3\}$ beispielsweise hat Mächtigkeit 3. Die leere Menge $\{\}$ oder $\emptyset$ enthält kein Element.

Definition 1.2 – Teilmengen

1. Eine Menge Y heißt Teilmenge von X, wenn aus $x \in Y$ immer folgt $x \in X$. Wir schreiben $Y \subset X$.
2. Wir sagen $X = Y$ genau dann, wenn $X \subset Y$ und $X \supset Y$ d.h. zwei Mengen sind gleich, wenn sie die gleichen Elemente enthalten. („Extensionalitätsprinzip“)

Bemerkung:

1. $\emptyset \subset M$, für jede Menge M
2. $M \subset M$, für jede Menge M
3. Wenn gilt $M \subset N$, aber nicht $M = N$, dann heißt M „echte Teilmenge“ von N, wir schreiben dann $M \subsetneq N$. (Die ISO-Vorschrift sieht hier $\subset$ für „echte Teilmenge“ und $\subseteq$ für „Teilmenge“ vor, dies wird jedoch selten benutzt.)

Die Natürlichen Zahlen
Die einfachste unendliche Menge ist die der natürlichen Zahlen

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

deren Existenz wir annehmen, zusammen mit den üblichen Rechenregeln. Die natürlichen Zahlen genügen dem Prinzip der vollständigen Induktion. Sei $M \subset \mathbb{N}$ und es gelte:

1. $1 \in M$
2. falls $m \in M$, so ist auch $n + 1 \in M$

Dann gilt $M = \mathbb{N}$.
Durch Erweiterung von Zahlbereichen können wir aus $\mathbb{N}$ auch die ganzen Zahlen $\mathbb{Z}$, die rationalen Zahlen $\mathbb{Q}$ sowie die reellen Zahlen $\mathbb{R}$ konstruieren (ebenso die komplexen Zahlen $\mathbb{C}$).

Bemerkung: Es gilt $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

Teilmengen mit Eigenschaften
Aus einer Menge können wir Teilmengen auswählen, welche durch bestimme Eigenschaften charakterisiert werden. Wir schreiben

$$X' = \{x \in X : x \text{ hat Eigenschaft } E\}$$

oder auch

$$X' = \{x \in X \mid x \text{ hat Eigenschaft E}\}.$$

Definition 1.3 – Mengenoperationen

Sind X, Y Mengen, so können wir bilden:

1. Die Vereinigung $X \cup Y$, ist die Menge aller Elemente, welche in X oder in Y sind.
2. Der Schnitt $X \cap Y = \{x \in X : x \in Y\}$, ist die Menge aller Elemente, die sowohl in X als auch in Y sind.

3. Für $Y \subset X$ schreiben wir $X \setminus Y$ sprich „X ohne Y“ für die Menge $\{x \in X : x \notin Y\}$
4. Das „kartesische Produkt“ $X \times Y$ ist die Menge aller geordneten Tupel $\{(x, y) : x \in X, y \in Y\}$

Beispiele:

1. $\{1, 2, 4\} \cap \{2, 3\} = \{2\}$
2. $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$
3. Die Elemente der Menge $\{1, \{1\}, 2\}$ sind genau $1, \{1\}, 2$

Definition 1.4 – Abbildungen

Seien X, Y Mengen. Als Abbildung von X nach Y bezeichnen wir eine Vorschrift f, welche jedem Element $x \in X$ genau ein Element $y \in Y$ zuordnet. Wir schreiben

$$f : X \to Y, \quad x \mapsto f(x).$$

Definition 1.5 – Gleichheit von Abbildungen

Zwei Abbildungen $f : X \to Y,\ g : X \to Y$ heißen gleich, wenn für alle $x \in X$ gilt $f(x) = g(x)$.

Definition 1.6 – Bild und Urbild

Sei $f : X \to Y, M \subset X, N \subset Y$

1. Wir schreiben $f(M) = \{y \in Y : \text{es existiert } x \in M \text{ mit } f(x) = y\} \subset Y$ Bild von M
2. $f^{-1}(N) = \{x \in X : f(x) \in N\} \subset X$ Urbild von N

Beispiele:

$X = \{1, 2, 3\}$, $Y = \{3, 4, 5, 6\}$
$f(1) = 4, f(2) = 5, f(3) = 5$

- $M = \{1, 2\} \subset X$
- $f(M) = \{4, 5\} \subset Y$
- $f(\emptyset) = \emptyset \subset Y$
- $f(X) = \{4, 5\}$
- $N = \{3, 4, 5\}$
- $f^{-1}(N) = \{1, 2, 3\}$
- $f^{-1}(\emptyset) = \emptyset$
- $f^{-1}(\{6\}) = \emptyset$
- $f^{-1}(\{5\}) = \{2, 3\}$

$X = \mathbb{R}, Y = \mathbb{R}$

- $f : X \to Y, x \mapsto f(x) = x^2$
- $f([1, 2]) = [1, 4] \subset Y$
- $f^{-1}(\{0\}) = \{0\}$
- $f^{-1}(\{1\}) = \{-1, 1\}$
- $f^{-1}(\{-1\}) = \emptyset$

Achtung: $f^{-1}(N)$ ist nur definiert für Mengen $N \subset Y$. Insbesondere ist f^{-1} (zumindest jetzt) keine Abbildung von Y nach X.

Definition 1.7 – Einschränkung von Funktionen

Es sei $f : X \to Y$ eine Abbildung, $M \subset X$. Die Einschränkung von f auf M ist die Abbildung $f|_M = M \to Y, x \mapsto f(x)$.
Bemerkung: Der Unterschied zu f ist nur der eingeschränkte Definitionsbereich.

$$f : \mathbb{R} \to \mathbb{R},\ x \mapsto f(x) = x^2$$
$$M = R_0^+ = \{x \in \mathbb{R} : x \geq 0\}$$
$$(f|_M)^{-1}(\{1\}) = \{1\}$$

Definition 1.8 – Injektivität, Surjektivität, Bijektivität

Es sei $f : X \to Y$ eine Abbildung.

1. f heißt injektiv, falls gilt
$$(x,\ x' \in X, f(x) = f(x')) \Rightarrow x = x'$$
2. f heißt surjektiv, falls gilt
$$f(X) = Y$$
3. f heißt bijektiv, falls f injektiv und surjektiv ist.

Beispiel: $f : \mathbb{R} \to \mathbb{R}, x \mapsto f(x) = x^2$ ist nicht injektiv, da $f(-1) = f(1), 1 \neq -1$. f ist auch nicht surjektiv, da $f(x) \geq 0$. $f|_{\mathbb{R}_0^+} : \mathbb{R}_0^+ \to \mathbb{R}$ ist injektiv, aber nicht surjektiv. $f|_{\mathbb{R}_0^+} : \mathbb{R}_0^+ \to \mathbb{R}_0^+$ ist injektiv, und surjektiv, also bijektiv.

Definition 1.9 – Umkehrfunktionen

Es sei $f : X \to Y$ bijektiv. Wir schreiben dann $f^{-1} : Y \to X, f^{-1}(y) = x$ mit dem eindeutig definierten $x \in X$, sodass gilt $f(x) = y$.

Bemerkung: Die Sinnhaftigkeit der Definition 1.9 folgt sofort aus der Definition von Bijektivität.

Satz 1.10

Sei X eine endliche Menge, so sind für $f : X \to X$ folgende Aussagen äquivalent:

1. f ist injektiv
2. f ist surjektiv
3. f ist bijektiv

Bemerkung: Für nicht endliche Mengen haben wir einfache Gegenbeispiele:

$$f : \mathbb{N} \to \mathbb{N},\ x \mapsto f(x) = 2x$$

Beweis: X ist eine endliche Menge, wir schreiben $X = \{x_1, \ldots, x_n\}$ mit paarweise verschiedenen x_j.

i) Wir zeigen zunächst 1. $\Rightarrow$ 2.. Zu zeigen ist also: Falls f injektiv ist, so ist f auch surjektiv. Dies wird impliziert durch die Aussage „Ist f *nicht* surjektiv, so ist f auch *nicht* injektiv“, welche wir zeigen:
Sei f also nicht surjektiv – also $f(X) \neq X$. Damit besteht $f(X)$ aus $m < n$ Elementen. Verteilt man aber n Elemente in $m < n$ Schubladen, so muss eine Schublade existieren, in der mehr als ein Element ist. Damit kann f nicht injektiv sein (es existiert $x \neq x'$ mit $f(x') = f(x)$).

ii) 2. $\Rightarrow$ 1.: Sei f also nicht injektiv, dann existieren nach Definition $x, x' \in X, x' \neq x$ aber $f(x) = f(x')$. Damit kann aber $f(X)$ höchstens $n - 1$ Elemente enthalten und f ist auch nicht surjektiv.

iii) 3. $\Rightarrow$ 1.: trivial nach der Definition der Bijektivität

iv) 3. $\Rightarrow$ 2.: ebenso

v) 1. $\Rightarrow$ 3.: Aus Injektivität folgt bereits Surjektivität und damit auch Bijektivität.

vi) 2. $\Rightarrow$ 3.: Aus Surjektivität folgt bereits Injektivität und damit auch Bijektivität.

□

Definition 1.11 – Komposition von Abbildungen

Es seien X, Y, Z Mengen, $f : X \to Y,\ g : Y \to Z$ Abbildungen. Dann definiert $g \circ f : X \to Z, x \mapsto g(f(x)) = (g \circ f)(x)$ die Komposition von Abbildungen.

Bemerkung: Es gilt Assoziativität: $(h \circ g) \circ f = h \circ (g \circ f)$ für $f : X \to Y, g : Y \to Z, h : Z \to A$
aber *nicht* Kommutativität, d.h. im Allgemeinen gilt nicht $f \circ g = g \circ f$ für $f : X \to X, g : X \to X$, denn

$$f : \mathbb{R} \to R, f(x) = x + 1$$
$$g : \mathbb{R} \to \mathbb{R}, f(x) = x^2$$

ist ein Gegenbeispiel, denn im Allgemeinen gilt *nicht*, dass $(x + 1)^2 = x^2 + 1$.

Definition 1.12 – Identische Abbildung

Mit $Id_X : X \to X$ bezeichnen wir die identische Abbildung $x \mapsto x$.

Lemma 1.13 – Identität und Surjektivität bzw. Injektivität

Es sei $f : X \to Y$ eine Abbildung, $X,\ Y \neq \emptyset$. Dann gilt:

1. f ist genau dann injektiv, wenn eine Abbildung $g : Y \to X$ existiert, mit $g \circ f = Id_X$
2. f ist genau dann surjektiv, wenn $g : Y \to X$ existiert, mit $f \circ g = Id_Y$
3. f ist genau dann bijektiv, falls $g : Y \to X$ existiert, so dass sowohl $g \circ f = Id_X$ und $f \circ g = Id_Y$. Es gilt dann $g = f^{-1}$

Beweis:

1. Sei f injektiv. Dann existiert zu jedem $y \in f(X)$ genau ein $x \in X$ mit $f(x) = y$. Wir setzen $g(y) = x$ für ebensolche $y = f(x)$. Nun wählen wir $x_0 \in X$ beliebig und setzen $g(y') = x_0$ für alle $y' \in \backslash f(X)$. Dieses g erfüllt die Bedingung.
   Sei nun $g : Y \to X$ mit $g \circ f = Id_X$. Seien $x, x' \in X$ mit $f(x) = f(x')$. Es gilt $x = Id_X(x) = (g \circ f)(x) = g(f(x)) = g(f(x')) = (g \circ f)(x') = Id_X(x') = x'$. Also ist f injektiv.

2. Sei f surjektiv. Zu jedem $y \in Y$ wählen wir ein $x \in X$ mit $f(x) = y$ und setzen $g(y) = x$. Damit gilt $f \circ g = Id_Y$.
   Umgekehrt, sei $g : Y \to X$, so dass $f \circ g = Id_Y$. Sei $y \in Y$, dann gilt $y = f(g(y))$. Sei $x' = g(y)$. Damit ist $y = f(x'), x' \in X$ und $y \in f(X)$. Damit ist f surjektiv.

3. Sei f bijektiv. Die nun definierte Abbildung $f^{-1} : Y \to X$ erfüllt die Voraussetzung an g.
   Falls aber g existiert mit $g \circ f = Id_x$ und $f \circ g = Id_Y$, dann erfüllt g die Voraussetzungen von 1. und 2. und f ist sowohl injektiv als auch surjektiv. Es gilt dann auch $g = f^{-1}$.

□

Definition 1.14 – Menge aller Abbildungen

Seien X, Y Mengen. Mit $\mathrm{Abb}(X, Y)$ bezeichnen wir die Menge aller Abbildungen von X nach Y.
Bemerkung: $\{f \in \mathrm{Abb}(X, Y) :\ f \text{ surjektiv}\}$ ist nun ebenfalls definiert.

Definition 1.15 – Mächtigkeit von Mengen

Es seien X, Y Mengen. Wir sagen X ist gleichmächtig wie Y, falls eine bijektive Abbildung von X nach Y existiert.

Bemerkung: Für endliche Mengen M gilt $\#M = m$ genau dann, wenn M gleichmächtig wie $\{1, 2, \ldots, m\}$ ist.

Definition 1.16 – Potenzmenge

Sei M eine Menge. Die Menge aller Teilmengen von M heißt Potenzmenge von M, kurz 2^M.
Bemerkung: Für eine (beliebige nicht notwendigerweise bijektive) Abbildung $f : X \to Y$ ist f^{-1} eine Abbildung von 2^Y nach 2^X.

Satz 1.17 – Mächtigkeit von 2^M

Sei M eine endliche Menge mit $\#M = m$, $m \in \mathbb{N} \cup \{0\}$. Dann gilt $\#2^M = 2^m$.

Beweis: Für $m = 0$ gilt $M = \emptyset$ und die Aussage ist klar, denn $2^\emptyset = \{\emptyset\}$, und diese Menge besitzt ein Element.
Rest des Beweises mittel Induktion:
Wir nennen $K \subset \mathbb{N}$ die Menge der natürlichen Zahlen m, für welche die Aussage gilt, und zeigen:

1. $1 \in K$
2. falls $m \in K$ so ist auch $m + 1 \in K$.

Damit folgt (nach dem Induktionsprinzip), dass K = $\mathbb{N}$ und der Satz ist gezeigt.

Zu 1.: Die einelementige Menge M schreiben wir als $\{x\}$, die Teilmengen sind $\emptyset, \{x\}$. Somit ist $2^M = \{\emptyset, \{x\}\}$ mit $\#2^M = 2 = 2^1$.

Zu 2.: Es sei also $\#M = m+1$ und M_m eine Menge mit $\#M_m = m$. Wir dürfen annehmen, dass gilt $\#2^{M_m} = 2^m$. Wir schreiben M als $M_m \cup \{x\}, x \notin M_m$. Wir schreiben
$2^M = \{$Menge aller Teilmengen von M, welche x nicht enthalten$\} \cup \{$Menge aller Teilmengen von M, welche x enthalten$\} = A \cup B$ und es gilt $\#2^M = \#A + \#B$.
$\#A = \#2^{M_m} = m$, da $A = 2^{M_m}$.
Jede Menge in B ist aber eine Menge in 2^{M_m} vereinigt mit $\{x\}$ und $\#B = 2^m$. Somit gilt $\#2^M = 2^m + 2^m = 2^{m+1}$.
Damit gilt die Aussage für $m + 1$.

□

Wir kennen bereits das direkte (bzw. kartesische) Produkt zweier Mengen $X \times Y = \{(x, y) : x \in X, y \in Y\}$.

Definition 1.18 – Graph einer Funktion

Es sei $f : X \to Y$ eine Abbildung. Die Menge $\Gamma_f = \{(x, f(x)) \in X \times Y\}$ nennen wir Graph von f.

Definition 1.19 – Relationen

Noch nützlicher ist das direkte Produkt, um eine sogenannte Relation zu definieren. Eine Relation R auf einer Menge X ist eine Teilmenge von $X \times X$. Wir sagen für $x, y \in X$, dass $x \sim y$ genau dann, wenn $(x, y) \in R$.
Beispiel:

$$x \sim y \Leftrightarrow x \leq y$$
$$\sim := \text{„Steht in Relation zu“}$$

Für das Beispiel gilt dann $R = \{(x, y) \in X \times X : x \leq y\}$.

Definition 1.20 – Äquivalenzrelationen

Eine Relation $\sim$ auf X heißt Äquivalenzrelation, falls gilt:

1. $x \sim x$ (Reflexivität)
2. $x \sim y \Rightarrow y \sim x$ (Symmetrie)
3. $x \sim y \wedge y \sim z \Rightarrow x \sim z$ (Transitivität)

für alle $x, y, z \in X$.
Beispiele:

- „=“ auf Zahlensystemen
- Sei $X = 2^N$. Für $x, y \in X$ gelte $x \sim y$ falls endliche Teilmengen A, B von x und y mit $x \setminus A = y \setminus B$

Definition 1.21 – Äquivalenzklassen

Sei X eine Menge mit Äquivalenzrelation $\sim$. Eine Menge $A \subset X$ heißt Äquivalenzklasse bezüglich $\sim$, falls gilt:

1. $A \neq \emptyset$
2. $x, y \in A \Rightarrow x \sim y$
3. $x \in A,\ y \in X,\ x \sim y \Rightarrow y \in A$

Proposition 1.22 – Partitionierung in Äquivalenzklassen

Sei X eine Menge mit Äquivalenzrelation $\sim$. Dann gehört jedes $a \in X$ zu genau einer Äquivalenzklasse A bezüglich $\sim$. Für zwei Äquivalenzklassen A, A' gilt entweder $A = A'$ oder $A \cap A' = \emptyset$.

Beweis: Für $a \in X$ definieren wir die Menge $A = \{x \in X : a \sim x\}$. Weil $a \sim a$, gilt $a \in A$, somit ist $A \neq \emptyset$. Sind nun $x, y \in A$, so gilt $a \sim x \wedge a \sim y$. Damit folgt $x \sim a$ und $a \sim y$ und somit $x \sim y$. Für $x \in A, y \in X$ mit $x \sim y$. gilt $a \sim x, x \sim y$ also $a \sim y$ und somit $y \in A$. Damit ist A eine Äquivalenzklasse und a ist in *mindestens* einer Äquivalenzklasse enthalten.

Es ist noch zu zeigen, dass zwei Äquivalenzklassen entweder gleich oder disjunkt sind.
Seien also A, A' Äquivalenzklassen mit $A \cap A' \neq \emptyset$. Also existiert $b \in A \cap A'$. Falls nun $x \in A$, so gilt $x \sim b$. Nachdem b auch in A' liegt, folgt aber $x \in A'$. Damit folgt $a \subset A'$. Die Umkehrung, also $A' \subset A$, folgt ebenso. □

Definition 1.23 – Quotientenmenge

Es sei X eine Menge mit Äquivalenzrelation $\sim$. Die Menge der Äquivalenzklassen in X bezeichnen wir als Quotientenmenge und schreiben für diese Menge $X/\sim$.

Bemerkung: Wir können eine Abbildung definieren, welche jedem $a \in X$ dessen Äquivalenzklasse zuordnet: $X \to x/\sim, a \mapsto A_a$ (nach Proposition 1.22 eindeutig zugeordnete Äquivalenzklasse). Ein solches a heißt dann Repräsentant der Äquivalenzklasse A_a.

Beispiel: Sei $X = \mathbb{N}$. Wir schreiben $X \sim y$, falls sowohl x als auch y gerade bzw. ungerade Zahlen sind. Sei $a \in X$. Die zugehörige Äquivalenzklasse ist gegeben durch:

1. Die Menge aller geraden Zahlen, falls a gerade ist.
2. Die Menge aller ungeraden Zahlen, falls a ungerade ist.

1.3 Gruppen

Definition 1.24 – Verknüpfungen

Es sei G eine Menge. Eine Verknüpfung $*$ auf G ist eine Abbildung:

$$\begin{aligned} * : G \times G &\to G \\ (a, b) &\mapsto *(a, b) \end{aligned}$$

Bemerkung: Oft schreiben wir einfach $a * b$ für $*(a, b)$.

Beispiele:

1. $G = \mathbb{N}$, $*(a,b) = a \cdot b$
2. $G = \mathbb{N}$, $*(a,b) = a + b$
3. Sei X eine Menge und $G = \text{Abb}(X,X)$, dann ist $*(f,g) = f \circ g$

Definition 1.25 – Gruppen

Eine Menge G mit Verknüpfung $*$ heißt Gruppe, falls gilt:

1. $(a * b) * c = a * (b * c)$ (Assoziativität)
2. Es existiert ein Element $e \in G$, sodass gilt:
   (a) $a * e = a$ für alle $a \in G$ (neutrales Element)
   (b) Für alle $a \in G$ existiert $a' \in G$ mit $a' * a = e$ (inverses Element)

Die Gruppe heißt abelsch, falls zusätzlich gilt

$$a * b = b * a \text{ für alle } a, b \in G$$

Bemerkung: Wir schreiben oft einfach $a \cdot b$ bzw. ab für $a * b$.

Beispiele

1. $G = \mathbb{Z}$, $*(a,b) = a + b$. Dabei ist $e = 0$ und $a' = -a$
2. $G = \mathbb{Q} \setminus \{0\}$, $*(a,b) = a \cdot b$. Dabei ist $e = 1$ und $a' = \frac{1}{a}$
3. $G = \{f \in \text{Abb}(X,X), f \text{ bijektiv}\}, *(f,g) = f \circ g$. Dabei ist $e = Id_X$ und das Inverse f^{-1}

Achtung: 1 und 2 sind abelsch, 3 nicht notwendigerweise.

Proposition 1.26 – Eindeutigkeit neutrales Element

Es sei G eine Gruppe. Dann gilt

1. Das neutrale Element ist eindeutig bestimmt, und es gilt auch $a * e = a$
2. Das inverse Element a' ist zu jedem $a \in G$ eindeutig bestimmt und es gilt auch $a * a' = e$

Beweis: Wir betrachten ein $e \in G$ und ein $a \in G$, wobei e ein neutrales Element ist. Es sei a' ein Inverses zu a. Es folgt $aa' = e(aa') = (a''a')(aa') = a''(a'(aa')) = a''((a'a)a') = a''(ea') = a''a' = e$.
Somit gilt $ae = a(a'a) = (aa')a = a$.
Sei $\hat{e}$ ein anderes neutrales Element. Dann gilt $e\hat{e} = e$ und $e\hat{e} = \hat{e}$. Damit folgt $e = \hat{e}$.
Sei nun $\hat{a}'$ ein weiteres inverses Element, dann folgt $\hat{a}' = \hat{a}'e = \hat{a}'(aa') = (\hat{a}'a)a' = ea' = a'$

□

Bemerkung:

1. Wir schreiben a^{-1} für das (nun) eindeutig bestimmte inverse Element zu a. Es gilt also $a^{-1}a = aa^{-1} = e$ sowie $(a^{-1})^{-1} = a$ und $(ab)^{-1} = b^{-1}a^{-1}$, denn $(b^{-1}a^{-1})(ab) = b^{-1}((a^{-1}a)b) = b^{-1}(eb) = b^{-1}b = e$
2. Es folgen auch die Kürzungsregeln:
   (a) $a\hat{x} = ax \Rightarrow x = \hat{x}$
   (b) $\hat{y}a = ya \Rightarrow y = \hat{y}$

Definition 1.27 – Rechts- und Linkstranslation

Für $a \in G$, G eine Gruppe, schreiben wir

1. $\tau_a : G \to G$, $x \mapsto xa$ (Rechtstranslation)

2. ${}_a\tau : G \to G,\ x \mapsto ax$ (Linkstranslation)

Lemma 1.28

1. Falls G eine Gruppe ist, so sind τ_a und ${}_a\tau$ bijektiv.
2. Sei G eine Menge mit assoziativer Verknüpfung. Dann folgt Definition 1.25.2 aus Surjektivität von τ_a und ${}_a\tau$

Beweis:

1. Bijektivität folgt aus $(\tau_a)^{-1}$ gegeben durch $(\tau_a)^{-1}(x) = xa^{-1}$, denn $(\tau_a)^{-1}(\tau_a(y)) = \tau_a(y)a^{-1} = (ya)a^{-1} = y$ für jedes $y \in G$.
2. Seien also τ_a und ${}_a\tau$ surjektiv. Dann existiert für jedes $b \in G$ eine Lösung für $xa = b$ sowie $ay = b$. Damit existiert aber zu $a \in G$ ein e mit $ea = a$. Für beliebiges $b \in G$ folgt dann $eb = e(ay) = (ea)y = ay = b$. Durch Lösen von $xa = e$ bekommen wir analog das Inverse Element zu a. □

Bemerkung:

1. Falls die Gefahr der Verwechslung besteht, schreiben wir gerne $(G, *)$ für eine Gruppe G mit Verknüpfung $*$, beispielsweise $(\mathbb{Q}, +)$ für $\mathbb{Q}$ mit Addition, oder $(\mathbb{Q}\setminus\{0\}, \cdot)$ für $\mathbb{Q}\setminus\{0\}$ mit Multiplikation.
2. Bei der Verknüpfung $+$ gehen wir immer von Kommutativität aus.
3. Endliche Gruppen kann man mit einer (Gruppen-) Tafel darstellen:

$*$	e	$\cdots$	a_i
e	e	$\cdots$	a_i
$\vdots$	$\vdots$	$\ddots$	$\vdots$
a_j	a_j	$\cdots$	$a_i * a_j$

4. Es gibt nur eine zweielementige Gruppe:

$*$	e	a
e	e	a
a	a	e

Definition 1.29 – Untergruppen

Es sei $(G, \cdot)$ eine Gruppe, $G' \subset G$. G' heißt Untergruppe von G, falls für $a, b \in G'$ auch gilt:

1. $ab \in G'$
2. $a^{-1} \in G'$

Definition 1.30 – Homo- und Isomorphismen auf Gruppen

Seien $(G, \cdot), (H, *)$ Gruppen, und $\varphi : G \to H$ eine Abbildung.

1. Die Abbildung φ heißt Homomorphismus, falls gilt:

$$\varphi(a \cdot b) = \varphi(a) * \varphi(b) \text{ für alle } a, b \in G$$

2. φ heißt Isomorphismus, falls φ zusätzlich bijektiv ist.

Proposition 1.31 – Untergruppen sind Gruppen

Es sei $(G, \cdot)$ eine Gruppe, G' eine Untergruppe von G. Dann ist $(G', \cdot)$ selbst eine Gruppe.

Beweis: Assoziativität folgt sofort. Es existiert ein a^{-1} in G', somit auch $e = aa^{-1} \in G'$.

□

Proposition 1.32 – Eigenschaften von Homomorphismen

Sei $\varphi : G \to H$ ein Homomorphismus von Gruppen $(G, \cdot)$, $(H, *)$. Dann gilt

1. $\varphi(e) = \hat{e}$ mit neutralen Elementen $e \in G, \hat{e} \in H$
2. $\varphi(a^{-1}) = (\varphi(a))^{-1}$ für alle $a \in G$
3. Für einen Isomorphismus φ ist auch φ^{-1} ein Homomorphismus

Beweis:

1. $\hat{e} * \varphi(e) = \varphi(e) = \varphi(e \cdot e) = \varphi(e) * \varphi(e)$. Nach der Kürzungsregel folgt $\hat{e} = \varphi(e)$
2. Nach 1. gilt $\hat{e} = \varphi(e) = \varphi(a^{-1}a) = \varphi(a^{-1}) * \varphi(a)$ also ist $\varphi(a^{-1}) = (\varphi(a))^{-1}$
3. Wir betrachten $c, d \in H$ mit $c = \varphi(a)$, $d = \varphi(b)$. Dann gilt $\varphi(ab) = \varphi(a) * \varphi(b) = c * d$, also $\varphi^{-1}(c * d) = \varphi^{-1}(\varphi(ab)) = ab = \varphi^{-1}(c)\varphi^{-1}(d)$

□

Beispiele:

1. $G = (\mathbb{R}, +), H = (\{x \in \mathbb{R} : x > 0\}, \cdot)$

$$\exp : \mathbb{R} \to \mathbb{R}_*^+, x \mapsto e^x$$

ist ein Isomorphismus, denn $e^{x+y} = e^x e^y$.

2. Wir betrachten $(\mathbb{Z}, +)$. Sei $m \in \mathbb{Z}$. Dann ist $\varphi_m : \mathbb{Z} \to \mathbb{Z}, a \mapsto ma$ ein Homomorphismus, denn $m(a + b) = ma + mb$. Das Bild $\phi_m(\mathbb{Z}) = m\mathbb{Z} = \{ma : a \in \mathbb{Z}\} \subset \mathbb{Z}$ ist eine Untergruppe von $(\mathbb{Z}, +)$, denn $ma + mb = m(a + b) \in m\mathbb{Z}$ und $-(ma) = m(-a) \in m\mathbb{Z}$.
Dazu betrachten wir die Menge $r + m\mathbb{Z}$ (für $r \in \{0, 1, \ldots, m-1\}$) mit $r + m\mathbb{Z} = \{r + ma : a \in \mathbb{Z}\}$.
Dann gilt $\mathbb{Z} = (0 + m\mathbb{Z}) \cup (1 + m\mathbb{Z}) \cup \cdots \cup (m - 1 \cup m\mathbb{Z})$ und die Vereinigung ist disjunkt.
Für $a \in \mathbb{Z}$ gilt $\frac{a}{m} = k + \frac{r}{m}$ für $k \in \mathbb{Z}, r \in \{0, \ldots, m-1\}$ (Division mit Rest). Dann gilt $a \in r + m\mathbb{Z}$. (denn $a = km + r$).
Wir bezeichnen die Mengen $r + m\mathbb{Z}$ auch als sogenannte „*Restklassen modulo m*“.
Falls a, a' in derselben Klasse $r + m\mathbb{Z}$ sind, gilt $\frac{a-a'}{r} \in \mathbb{Z}$, und wir schreiben $a \equiv a' \mod m$ (ist kongruent zu). Zu $a \in \mathbb{Z}$ schreiben wir $\bar{a} = a + m\mathbb{Z}$, die zu a gehörige Restklasse und wir definieren eine Addition $\bar{a} + \bar{b} = \overline{a + b}$. Wir müssen sicherstellen, dass die Definition nicht von der Auswahl des Repräsentanten abhängt, das ist aber leicht zu sehen.
$\bar{a} = \bar{a'}, \bar{b} = \bar{b'}$, dann folgt auch schon, dass gilt $\overline{a + b} = \overline{a' + b'}$.

Satz – Zyklische Gruppen

Für $m \in \mathbb{N}$ sei $\mathbb{Z}/m\mathbb{Z} = \{\bar{0}, \ldots, \overline{m-1}\}$.
Dann gilt, dass $\mathbb{Z}/m\mathbb{Z}, +$ (+ definiert wie oben) eine abelsche Gruppe ist. Die Abbildung $\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}, a \mapsto \bar{a} = a + m\mathbb{Z}$ ist ein surjektiver Homomorphismus.
Beweis: Übung.
Wir nennen diese Gruppen die zyklischen Gruppen der Ordnung m.

1.4 Ringe und Körper

Definition 1.33 – Ringe

Es sei R eine Menge, $+ : R \times R \to R$ und $\cdot : R \times R \to R$ Verknüpfungen. $(R, +, \cdot)$ heißt Ring, falls gilt:

1. $(R, +)$ ist eine abelsche Gruppe
2. Die Multiplikation ist $\cdot$ assoziativ.

3. Das Distributivgesetz gilt:

$$a \cdot (b + c) = ab + ac$$
$$(b + c) \cdot a = ba + ca$$

Ein Ring heißt kommutativ, falls gilt $a \cdot b = b \cdot a$ für alle $a, b \in R$.
Falls ein Element $1 \in R$ existiert mit $1 \cdot a = a \cdot 1 = a$ für alle $a \in R$, dann nennen wir dieses Element Einselement. Das neutrale Element der Addition + heißt Nullelement (oder 0).

Proposition 1.34 – Absorption durch Nullelement

Es gilt $0 \cdot a = a \cdot 0 = 0$.

Beweis: Wir erinnern uns an die Kürzungsregel: $\alpha + \xi = \beta + \xi \Rightarrow \alpha = \beta$. Wir schreiben also $0 + 0a = 0a = (0 + 0)a = 0a + 0a \Rightarrow 0 = 0a$. Ebenso folgt $0 = a0$. □

Beispiele:

1. $(\mathbb{Z}, +\cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +\cdot)$
2. $\mathbb{Z}.m\mathbb{Z}$ mit der Addition wie bisher und $\bar{a} \cdot \bar{b} = \overline{ab}$ (Nach Überprüfung der Unabhängigkeit von der Wahl des Repräsentanten)
3. Die 2×2-Matrizen $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ bilden einen Ring mit

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ac+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}$$

Die gewünschten Eigenschaften folgen sofort. Es gilt aber:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Definition 1.35 – Unterring und Ringhomomorphismus

Es sei $(R, +, \cdot)$ ein Ring, $R' \subset R$. $(R', +, \cdot)$ heißt Unterring, falls $(R', +)$ eine Untergruppe von $(R, +)$ ist und gilt $a, b \in R' \Rightarrow ab \in R'$.

Es seien $(R, +, \cdot)$, $(S, \hat{+}, \hat{\cdot})$ Ringe, $\varphi : R \to S$ eine Abbildung. φ heißt Ringhomomorphismus, falls gilt $\varphi(a + b) = \varphi(a) \hat{+} \varphi(b)$ und $\varphi(ab) = \varphi(a) \hat{\cdot} \varphi(b)$ für alle $a, b \in R$.

Definition 1.36 – Körper

Es sei K eine Menge, $+ : K \times K \to K, \cdot : K \times K \to K$ Verknüpfungen. $(K, +, \cdot)$ heißt Körper, falls gilt:

1. $(K, +)$ ist eine abelsche Gruppe
2. K^* sei gegeben durch $K \setminus \{0\}$. Dann ist $(K^*, \cdot)$ eine abelsche Gruppe.
3. Für $a, b, c \in K$ gilt $a(b + c) = ab + bc$ und $(b + c)a = ba + ca$

Bemerkung: Das neutrale Element der Multiplikation bezeichnen wir mit Eins (= 1), das Inverse zu a bezüglich der Multiplikation mit a^{-1} oder $\frac{1}{a}$, bezüglich der Addition mit $-a$.

Proposition 1.37 – Rechenregeln für Körper

Sei $(K, +, \cdot)$ ein Körper. Dann gilt:

1. $1 \neq 0$
2. $0a = a0 = 0$
3. $ab = 0 \Rightarrow a = 0 \vee b = 0$ (Nullteilerfreiheit)
4. $a(-b) - (ab)$ und $(-a)(-b) = ab$
5. $xa = \hat{x}a$ und $a \neq 0 \Rightarrow x = \hat{x}$

Beweis:

1. Folgt sofort, denn $(K^*, \cdot)$ ist eine Gruppe.
2. Folgt analog zu Ringen.
3. Folgt aus Gruppeneigenschaft von $(K^*, \cdot)$, da $(K^*, \cdot)$ unter der Multiplikation abgeschlossen ist, und somit a oder b nicht in K^* sein kann (also 0 ist)
4. Wir rechnen
$$ab + a(-b) = a(b - b) = a0 = 0$$
und
$$(-a)(-b) = -((-a)b) = -(-(ab)) = ab$$
5. Die Regel gilt für $x, \hat{x}$ beide in K^*. Ist aber $\hat{x} = 0$, so gilt $\hat{x}a = 0$ nach 2. und mit 3. folgt die Aussage.

□

Beispiele:

1. $(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot)$.
2. Die komplexen Zahlen $\mathbb{C}$, wie folgt definiert. Für $(a, b), (c, d) \in \mathbb{R} \times \mathbb{R}$ definieren wir
$$(a, b) + (c, d) = (a + c, b + d)$$
und
$$(a, b) \cdot (c, d) = (ac - bd, ad + bc)$$
mit $(0, 0)$ als Nullelement und $(1, 0)$ als Einselement. Das additive Inverse zu (a, b) ist dann $(-a, -b)$, das multiplikative Inverse ist $\left(\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2}\right)$. Wir bezeichnen den so konstruierten Körper mit $\mathbb{C}$.

   Wir betrachten nun die Abbildung $\mathbb{R} \to \mathbb{C}, a \mapsto (a, 0)$, welche injektiv ist. Wir sehen, dass zwischen $\mathbb{R} \times \{0\}$ und $\{(a, b) \in \mathbb{C} : b = 0\}$ nicht unterschieden werden muss, denn
$$(a, 0) \cdot (b, 0) = (ab, 0)$$
$$(a, 0) + (b, 0) = (a + b, 0)$$
   Wir schreiben $\mathrm{i} = (0, 1) \in \mathbb{C}$ und $(a, b) = (a, 0) + (0, b) = a + \mathrm{i}b$. Es gilt $\mathrm{i}^2 = \mathrm{ii} = -1$. Weiterhin schreiben wir für $z = (a, b) \in \mathbb{C}, \bar{z} = (a, -b)$. (bzw. $z = a + \mathrm{i}b, \bar{z} = a - \mathrm{i}b$). $\bar{z}$ (manchmal auch z^*) nennen wir komplex Konjugiertes (oder komplexe Konjugation) von z.

   Für komplexe Zahlen λ, μ gilt dann
$$\overline{\lambda + \mu} = \bar{\lambda} + \bar{\mu} \text{ sowie } \overline{\lambda\mu} = \bar{\lambda}\bar{\mu} \text{ und } \lambda \in \mathbb{R} \Leftrightarrow \lambda = \bar{\lambda}$$
   Für $\lambda = a + b\mathrm{i} \in \mathbb{C}$ sehen wir $\lambda\bar{\lambda} = (a + b\mathrm{i})(a - b\mathrm{i}) = a^2 + b^2 \in \mathbb{R}$ und wir definieren den Absolutbetrag
$$|\lambda| = \sqrt{\lambda\bar{\lambda}}$$

Damit gilt, dass $d(\lambda, \mu) = |\lambda - \mu|$ eine Metrik darstellt, denn

$$\begin{aligned} d(\mu, \lambda) &= d(\lambda, \mu) \\ d(\mu, \lambda) &= 0 \Leftrightarrow \lambda = \mu \\ d(\mu, \lambda) + d(\lambda, \kappa) &\geq d(\mu, \kappa) \end{aligned}$$

Das ist die selbe Metrik, die bereits im $\mathbb{R}^2$ eingeführt wurde:

$$d(x, y) = \sqrt{(x - y, x - y)} = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2} \quad \text{mit} \quad (\xi, \eta) = \xi_1\eta_1 + \xi_2\eta_2$$

Neu ist die Identität $|\lambda \cdot \mu| = |\lambda||\mu|$.

Wir betrachten noch eine geometrische Anschauung der komplexen Zahlen. Es sei $\lambda \in \mathbb{C}$ mit $|\lambda| = 1$. Dann gilt, dass $\lambda^{-1} = |\frac{1}{\lambda}| = 1$ (folgt aus der Definition des Inversen in $\mathbb{C}$).

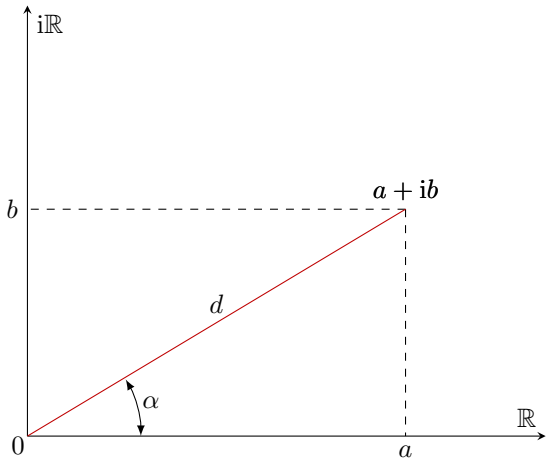
In der Analysis lernen wir, dass ein eindeutiges $\alpha \in [0, 2\pi)$ existiert, so dass

$$\lambda = cos(\alpha) + \mathrm{i}\sin(\alpha) = \mathrm{e}^{\mathrm{i}\alpha} \quad \text{für} \quad \lambda \in \mathbb{C}, |\lambda| = 1$$

Wir bezeichnen α als Argument von λ, also $\alpha = \arg\lambda$.

Sei nun $\lambda \in \mathbb{C} \setminus \{0\}$ beliebig (d.h. ohne die Einschränkung, dass $|\lambda| = 1$). Dann schreiben wir $\arg\lambda = \arg\frac{\lambda}{|\lambda|}$, denn $\left|\frac{\lambda}{|\lambda|}\right| = 1$.

Damit gilt $\lambda = |\lambda|\mathrm{e}^{\mathrm{i}\arg\lambda}$ für jedes $\lambda \in \mathbb{C}$. In der komplexen Ebene $\mathbb{C} = \mathbb{R}^2$ (auch Gaußsche Zahlenebene genannt) gilt dann mit $d = |\lambda|$, $\alpha = \arg\lambda$:



Wir sehen nun, dass gilt

$$\lambda\mu = |\lambda|\mathrm{e}^{\mathrm{i}\arg\lambda} \cdot |\mu|\mathrm{e}^{\mathrm{i}\arg\mu} = |\lambda||\mu|\mathrm{e}^{\mathrm{i}\arg\lambda}\mathrm{e}^{\mathrm{i}\arg\mu} = |\lambda||\mu|\mathrm{e}^{\mathrm{i}(\arg\lambda + \arg\mu)}.$$

Wir sehen: Beträge werden multipliziert, Argumente addiert bei der Multiplikation in $\mathbb{C}$.

Definition 1.38 – Nullteilerfreiheit von Ringen

Ein Ring $(R, +, \cdot)$ heißt nullteilerfrei, falls für $a, b \in R$ gilt

$$ab = 0 \Rightarrow a = 0 \vee b = 0.$$

Bemerkung: Wir sehen, dass jeder Körper bereits ein nullteilerfreier Ring ist.

Beispiel: Auf $\mathbb{Z}/m\mathbb{Z}$ ist bereits eine Addition definiert, mit der $\mathbb{Z}/m\mathbb{Z}$ eine Gruppe wird. Mit der Multiplikation

$$\bar{a} \cdot \bar{b} = \overline{ab}$$

für $\bar{a}, \bar{b} \in \mathbb{Z}/m\mathbb{Z}$ und Repräsentanten a und b wird $\mathbb{Z}/m\mathbb{Z}$ zu einem Ring. Wie für die Addition zeigen wir Unabhängigkeit von der Wahl der Repräsentanten, Assoziativität und Distributivgesetz sind leicht nachzurechnen. Der Ring ist kommutativ.

Satz 1.39 – Nullteilerfreiheit des Restklassenrings

Der Restklassenring $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ ist genau dann nullteilerfrei, wenn m eine Primzahl ist.

Beweis: Falls m nicht prim ist, gilt $m = k \cdot l$ mit $1 < k, l < m$. Damit gilt $\bar{k} \neq \bar{0}, \bar{l} \neq \bar{0}$, aber $\bar{k}\bar{l} = \overline{kl} = \bar{m} = \bar{0}$.
Umgekehrt: Sei m prim und $\bar{k}\bar{l} = 0$. Dann gilt $k \cdot l = r \cdot m$, für ein $r \in \mathbb{Z}$. Damit gilt aber, dass mindestens einer der Faktoren k, l einen Faktor m enthält. Also ist $\bar{k} = 0$ oder $\bar{l} = 0$. □

Satz 1.40

Ein nullteilerfreier, kommutativer Ring K mit endlich vielen Elementen und Eins ist ein Körper.

Beweis: Nach Lemma 1.28 reicht es zu zeigen, dass die Abbildung ${}_a\tau : K^* \to K^* : {}_a\tau(x) = ax$ für jedes $a \in K^*$ surjektiv ist. K^* ist eine endliche Menge, also folgt Surjektivität aus Injektivität. Sei also ${}_a\tau(x) = {}_a\tau(y)$, für x, y aus K^*. Es folgt $ax = ay$, also $a(x - y) = 0$. Damit gilt aber (wegen Nullteilerfreiheit und $a \in K^*$, also $a \neq 0$), dass $x - y = 0$, also $x = y$. □

Definition 1.41 – Charakteristik eines Ringes

Es sei R ein Ring mit Einselement 1. Die Charakteristik von R ist gegeben durch

$$\chi(R) = \begin{cases} 0 & \text{falls } n \cdot 1 \neq 0 \ \forall n \neq 0 \\ \min\left(n \in \mathbb{N} \setminus \{0\}\right) & \text{falls } n \cdot 1 = 0 \end{cases}$$

Statt $\chi(R)$ wird auch $\mathrm{char}(R)$ verwendet.
Achtung: Wir haben benutzt, dass $n \cdot a = a + a + \cdots + a$ (n-mal) mit $a \in R, n \in \mathbb{N}$

Lemma 1.42 – Charakteristik von Körpern

Ist K ein Körper, so gilt $\chi(K)$ ist entweder Null, oder eine Primzahl.

Beweis: Angenommen, $\chi(K) = m = k \cdot l \neq 0$ mit $1 < k, l < m$ (also m nicht prim). Es folgt $0 = m \cdot 1 = (k \cdot l)1 = (k \cdot 1)(l \cdot 1)$. Wegen Nullteilerfreiheit folgt $k \cdot 1 = 0$ oder $l \cdot 1 = 0$, und somit ein Widerspruch. □

Definition 1.43 – Schiefkörper

Ein Körper ohne Kommutativität bezüglich der Multiplikation nennen wir Schiefkörper (Beispiel: Quaternionen, siehe Übungsblatt).

2. Vektorräume

Wir kennen bereits $\mathbb{R}^n = \mathbb{R} \times \mathbb{R} \times \cdots \times \mathbb{R}$ mit Operationen $a + b$ für $a, b \in \mathbb{R}^n$ und $\lambda \cdot a$ für $a \in \mathbb{R}^n, \lambda \in \mathbb{R}$.

2.1 Definitionen und elementare Eigenschaften

Definition 2.1 – Vektorraum

Es sei K ein Körper, $(V, +)$ eine abelsche Gruppe mit einer Abbildung $K \times V \to V$, $(\lambda, b) \mapsto \lambda v$, sodass für alle $x, y \in V$, $\lambda, \mu \in K$ gilt:

1. $\lambda(x + y) = \lambda x + \lambda y$ — Erstes Distributivgesetz
2. $(\lambda + \mu)x = \lambda x + \mu x$ — Zweites Distributivgesetz
3. $\lambda(\mu x) = (\lambda\mu)x$ — Skalarmultiplikation
4. $1x = x$ — Einselement

Zu beachten ist hierbei, was Addition der Gruppe, was Multiplikation des Körpers und was die speziell definierte Abbildung ist. Dies ergibt sich jedoch eindeutig aus den Typen der verknüpften Elemente.
Wir nennen die Abbildung $(\lambda, v) \mapsto \lambda v$ skalare Multiplikation. Die Gruppe $(V, +)$ mit der skalaren Multiplikation heißt dann K-Vektorraum.
Bemerkung:

1. Ist $(R, +, \cdot)$ ein Ring, $(V, +)$ eine abelsche Gruppe mit Abbildung $R \times V \to V, (\lambda, v) \mapsto \lambda v$, welche die Bedingungen aus Definition 2.1 erfüllt. Dann ist V ein R-Modul (bzw. Links-R-Modul). Rechts-R-Moduln analog.
2. (a) Elemente in V heißen Vektoren, Elemente in K heißen Skalare.
   (b) Das Inverse zu $a \in V$ heißt $-a$ (das Inverse für Gruppen mit Addition)
3. Wir schreiben $(\lambda x) + (\mu y) = \lambda x + \mu y$ (d.h. „Punkt vor Strich“) für skalare Multiplikation
4. $K = \mathbb{R}$: reelle Vektorräume
   $K = \mathbb{C}$: komplexe Vektorräume

Beispiele

1. $\mathbb{R}^n$, siehe Kapitel 0
2. $\mathbb{C}^n$, $K = \mathbb{C}$ analog
3. Sei K ein beliebiger Körper, dann ist K^n ein Vektorraum, der aus den n-Tupeln von Körperelementen besteht. Addition in K^n erfolgt eintragsweise, Multiplikation für $\lambda \in K$ erfolgt ebenfalls eintragsweise.

$$\begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} + \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} = \begin{pmatrix} v_1 + w_1 \\ \vdots \\ v_n + w_n \end{pmatrix}$$

$$\lambda \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} = \begin{pmatrix} \lambda w_1 \\ \vdots \\ \lambda w_n \end{pmatrix}$$

   $K^0 := \{0\}$ ist der triviale Vektorraum.

4. Es sei K ein Körper, X eine Menge, $V = \text{Abb}(X, K)$ mit

$$(f+g)(x) = f(x) + g(x) \text{ für alle } x \in X, f, g \in V.$$

Damit wird V zu einer abelschen Gruppe, denn oben ist eine Addition $+(f, g)$ definiert. Wir definieren nun $(\lambda f)(x) = \lambda(f(x))$ für alle $\lambda \in K, f \in V, x \in X$ als Skalarmultiplikation. Damit wird V zu einem Vektorraum.

Proposition 2.2 – Eigenschaften von Vektorräumen

Es sei V ein K-Vektorraum. Dann gilt:

1. $0x = 0 \in V$ für alle $x \in V$
2. $\lambda 0 = 0$ für alle $\lambda \in K$
3. Falls $\lambda \in K, x \in V, \lambda x = 0 \in V$, dann gilt $\lambda = 0$ oder $x = 0$
4. $(-1)x = -x$ für alle $x \in V$

Beweis:

1. $0x = (0+0)x = 0x + 0x \Rightarrow 0x = 0$
2. $\lambda 0 = \lambda(0+0) = \lambda 0 + \lambda 0 \Rightarrow \lambda 0 = 0$
3. Zu zeigen ist $\lambda \in K^*, x \in V, \lambda x = 0$. Dann folgt $x = 0$. Es gilt aber $x = 1x \overset{\lambda \neq 0}{=} (\lambda^{-1}\lambda)x = \lambda^{-1}(\lambda x) = \lambda^{-1}0 = 0$
4. $x + (-1)x = 1x + (-1)x = (1-1)x = 0x = 0$

□

Bemerkung: Es sei $(G.+)$ eine Gruppe, $y \in G$. Falls gilt $y = y+y$, so folgt $y = 0$, denn die Kürzungsregel besagt $a + \hat{x} = a + x \Rightarrow x = \hat{x}$. Mit $x = 0, \hat{x} = y, a = y$. Also $y + y = y + 0 = y \Rightarrow y = 0$.

Definition 2.3 – Untervektorräume

Es sei K ein Körper, V ein K-Vektorraum. Weiteres sei $W \subset V$. Dann heißt W Untervektorraum von V, falls gilt:

1. $W \neq \emptyset$
2. $v, w \in W \Rightarrow v + w \in W$
3. $v \in W, \lambda \in K \Rightarrow \lambda v \in W$

Beispiel: $V = R^2, W = \{v = (v_1, v_2) \in V : v_1 = 0\}$
Gegenbeispiel: $V = R^2$, $W = \{v = (v_1, v_2) \in V : v_2 = 1\}$ ist kein Untervektorraum von V

Satz 2.4 – Untervektorräume sind Vektorräume

Ein Untervektorraum ist (mit der induzierten Addition und Skalarmultiplikation) ein Vektorraum.

Beweis: Sei V ein K-Vektorraum, W ein Untervektorraum von V.

1. W ist eine Untergruppe von $(V, +)$, denn W ist nicht leer und abgeschlossen bezüglich der Addition. Das neutrale Element $0 \in W$, denn für ein beliebiges $w \in W$ folgt mit (3.), dass $0 = 0w \in W$. Zu $v \in W$ gilt weiter $-v = (-1)v \in W$ nach (3.)
2. Kommutativität und Assoziativität der Untergruppe $(W, +)$ folgt sofort, Distributivgesetze ebenfalls.

Damit ist W ein Vektorraum.

□

Bemerkung: Es sei I eine Menge und für jedes $a \in I$ sei M_a wieder eine Menge. So ein I nennen wir Indexmenge. Nun verallgemeinern wir Schnittmenge und Vereinigung:

$$\bigcap_{a \in I} M_a = \{x : x \in M_a \text{ für jedes } a \in I\}$$
$$\bigcup_{a \in I} M_a = \{x : x \in M_a \text{ für ein } a \in I\}$$

Lemma 2.5

Es sei V ein K-Vektorraum, I eine Indexmenge und für jedes $a \in I$ sei $W_a \subset V$ ein Untervektorraum. Dann gilt

1. $W = \bigcap_{a \in I} W_a$ ist ein Untervektorraum von V
2. Seien $a, b \in I$, dann folgt $\hat{W} = W_a \cup W_b$ ist ein Untervektorraum von V genau dann, wenn $W_a \subset W_b$ oder $W_b \subset W_a$

Beispiele

1. $V = R^3$, $I = \{1, 2\}$
2. $W_1 = \{v = (v_1, v_2, v_3) \in V : v_1 = 0\}$
3. $W_2 = \{v = (v_1, v_2, v_3) \in V : v_2 = 0\}$
4. $W = W_1 \cap W_2 = \{v = (v_1, v_2, v_3) \in V : v_1 = v_2 = 0\}$ ist ein Untervektorraum.
5. $W_1 \cup W_2 = \{v = (v_1, v_2, v_3) \in V : v_1 = 0 \vee v_2 = 0\}$ ist kein Untervektorraum von V, denn $w_1 = (0, 1, 1) \in W_1, w_2 = (1, 0, 1) = W_2$, aber $w_1 + w_2 = (1, 1, 2)$ ist nicht in $W_1 \cup W_2$

Beweis:

1. Es gilt $0 \in W_a$ für jedes $a \in I$, also gilt $0 \in W$.

   Es seien $x, y \in W$, also gilt $x, y \in W_a$ für jedes $a \in I$. Nachdem W_a (für jedes a) ein Untervektorraum von V ist, gilt $x + y \in W_a$ für jedes $a \in I$, also $x + y \in W$. Ebenso folgt $\lambda x \in W$.

2. „$\Leftarrow$“ folgt sofort, denn wenn $W_a \subset W_b$, so gilt $W_a \cup W_b = W_b$ und somit ist $W = W_b$ ein Untervektorraum

   „$\Rightarrow$“ Sei $\hat{W} = W_a \cup W_b \subset V$ ein Untervektorraum und sei $W_a \not\subset W_b$.

   Zu zeigen ist nun, $W_b \subset W_a$. Es sei $x \in W_b$, wir zeigen, dass folgt $x \in W_a$. Sei $y \in W_a \setminus W_b$ (sodass ein y existiert, nachdem $W_a \not\subset W_b$). Es folgt $x + y \in \hat{W}$, also $x + y \in W_a$ oder $x + y \in W_b$. Es gilt aber, dass $y = (x + y) - x$, und somit $x + y \notin W_b$. Somit gilt $x + y \in W_a$, also $(x + y) - y = x \in W_a$.

   □

Definition 2.6 – Linearkombination und Erzeugendensysteme

Es sei V ein K-Vektorraum, $E \subset V$ eine Menge.

1. Für jedes $e \in E$ sei $\lambda_e \in K$, so dass nur endlich viele $\lambda_e \neq 0$ sind. Dann schreiben wir

   $$\sum_{e \in E} \lambda_e \cdot e = \sum_{e \in E, \lambda_e \neq 0} \lambda_e \cdot e \in V \quad \text{und} \quad \sum_{e \in V} \lambda_e \cdot e$$

   heißt Linearkombination der $e \in E$

2. Ein beliebiges $x \in V$ heißt darstellbar als Linearkombination der $e \in E$, falls $\lambda_e \in k$ existieren, mit $\lambda_e \neq 0$ für endlich viele $e \in E$ und es gilt $x = \sum_{e \in E} \lambda_e \cdot e$.

3. Spann oder Aufspann: $\text{span}(E) = \{x \in V : x \text{ als Linearkombination der } e \in E \text{ darstellbar}\}$ (manchmal auch als lineare Hülle bezeichnet)

4. Falls gilt $W = \text{span}(E)$, so heißt $E \subset V$ Erzeugendensystem von W.

5. $W \subset V$ heißt endlich erzeugt über K, falls ein Erzeugendensystem für W mit nur endlich vielen Elementen existiert.

Beispiel: $V = R^2, E = \{(1,0),(0,1),(1,1)\} \subset V$. Dann gilt $V = \text{span}(E)$, denn sei $v = (v_1, v_2) \in R^2, v_1, v_2 \in \mathbb{R}$ und es gilt $v = v_1 + \cdot(1,0) + v_2 \cdot (0,1)$. V ist also endlich erzeugt.

Lemma 2.7

Es sei V ein K-Vektorraum, $E \subset V$. Dann gilt

1. $\text{span}(E)$ ist ein Untervektorraum von V

2. Falls $W \subset V$ ein Untervektorraum ist mit $E \subset W$, so gilt $\text{span}(E) \subset W$. Es folgt, dass $\text{span}(E) \subset V$ der minimale Untervektorraum ist, der E enthält.

Beweis:

1. Folgt sofort aus der Definition, denn

   (a) $\text{span}(E) \neq \emptyset$, denn $0 \in \text{span}(E)$

   (b) Für $v_1, v_2 \in \text{span}(E)$ gilt $v_1 + v_2 \in span(E)$, denn wir können die Koeffizienten λ_e^{v1} und λ_e^{v2} addieren. Ebenso für μv_1.

2. Sei $W \subset V$ ein Untervektorraum, $E \subset W$. Es folgt aufgrund der Abgeschlossenheit von W bezüglich Addition und Skalarmultiplikation, dass jede Linearkombination der $e \in E$ wieder in W liegt. □

2.2 Basis und Dimension

Ziel: finde möglichst kleine Erzeugendensysteme für Vektorräume.

Beispiel: Wir betrachten $\mathbb{R}^2, e_1 = (1,0), e_2 = (0,1)$. Dann gilt

$$\text{span}(\{e_1, e_2\}) = \{x \in \mathbb{R}^2 : x = (x_1, x_2),\ x_1 = \lambda_1 e_1,\ x_2 = \lambda_2 e_2,\ \lambda_1,\ \lambda_2 \in \mathbb{R}\} = \mathbb{R}^2.$$

Allerdings nur $\{e_1\}$ oder nur $\{e_2\}$ ist kein Erzeugendensystem für $\mathbb{R}^2$. Mit $e_3 = \{1,1\}$ ist $\{e_1, e_2, e_3\}$ ein Erzeugendensystem für $\mathbb{R}^2$, aber kein kleinstmögliches im obigen Sinne.

Im Folgenden sei stets K ein Körper und V ein K-Vektorraum.

Definition 2.8 – Familien von Elementen

Seien X, I Mengen. Für jedes $j \in I$ sei $e_j \in X$. Dann bezeichnen wir die Abbildung $I \to X, j \mapsto e_j$ als „durch I induzierte Familie von Elementen von X“. Wir schreiben $(e_j)_{j \in I} \in X^I = \text{Abb}(I, X)$.

Bemerkung: Es sei $I = \{1, 2, 3, \ldots, n\}$. Dann gilt $\mathbb{R}^I = \mathbb{R}^{\{1,2,\ldots,n\}} = \mathbb{R}^n$. Die Abbildung ist hier $1 \mapsto x_1$, $2 \mapsto x_2$, …, $n \mapsto x_n$.
Für $I = \mathbb{N}$ is $\mathbb{R}^{\mathbb{N}}$ die Menge der reellen Folgen.

Definition 2.9 – Minimale und linear unabhängige Erzeugendensysteme

Es sei I eine Menge, und $(v_i)_{i \in I}$ eine Familie von Vektoren $v_i \in V$.

1. $(v_i)_{i \in I}$ heißt minimales Erzeugendensystem von V, falls $E = \{v_i, i \in I\}$ ein Erzeugendensystem von V ist und gilt $(J \subsetneq I) \Rightarrow \text{span}(v_j, j \in J) \neq V$

2. $(v_i)_{i \in I}$ heißt lineare unabhängig, falls gilt:
   Es sei $(\lambda_i)_{i \in I} \in K^I$ (eine durch I induzierte Menge von Skalaren) mit $\lambda_i \neq 0$ für endlich viele $i \in I$ und $\sum_{i \in I} \lambda_i v_i = 0$, dann folgt $\lambda_i = 0$ für alle $i \in I$. Nicht linear unabhängige Familien heißen linear abhängig.

Bemerkung: Für $I = \emptyset$ ist $(v_i)_{i \in I}$ stets linear unabhängig.

Beispiele: Siehe Kapitel 0.

Lemma 2.10

Es sei $(v_i)_{i \in I} \in V^I$. Dann gilt:

1. Falls $v_j = 0$ für ein $j \in I$, dann ist $(v_i)_{i \in I}$ linear abhängig
2. Falls $i, j \in I$ existieren, mit $v_i = v_j$ dann ist $(v_i)_{i \in I}$ linear abhängig
3. Falls $I = \{i\}$ ist, dann ist $(v_i)_{i \in I}$ linear unabhängig genau dann, wenn $v_i \neq 0$
4. Sind $(v_i)_{i \in I}$ linear unabhängig, dann gilt $(J \subset I) \Rightarrow (v_j)_{j \in J}$ ebenfalls als linear unabhängig
5. Sei $I \neq \emptyset$, dann gilt $(v_i)_{i \in I}$ ist linear abhängig genau dann, wenn $j_0 \in I$ existiert, sodass $J \subset I \setminus \{j_0\}$, J ist eine endliche Menge und es existiert $(\mu_j)_{j \in J} \in K^I$, sodass $\mu_{j_0} = \sum_{j \in J} \mu_j v_j$ (Ein Element lässt sich als Linearkombination der anderen schreiben)

Beweis:

1. $1 \cdot v_j = 0$ und $1 \neq 0 \Rightarrow$ linear abhängig
2. Klar aus 1. und Definition
3. Folgt direkt aus der Definition
4. Der Beweis erfolgt in zwei Richtungen:

   „$\Rightarrow$“ Sei also $(v_i)_{I \in I}$ linear abhängig. Also existieren $(\lambda_i)_{i \in I} \in K^I$ (nur endlich viele $\neq 0$) und ein $\lambda_{i_0} \neq 0$ mit $i_0 \in I$ und $\sum_{i \in I} \lambda_i v_i = 0$. Damit gilt $\lambda_{i_0} v_{i_0} = -\sum_{i \in I \setminus \{i_0\}} \lambda_i v_i \Rightarrow v_{i_0} = -\sum_{i \in I \setminus \{i_0\}} \frac{\lambda_i}{\lambda_{i_0}} v_i$

   „$\Leftarrow$“ Es sei $v_{j_0} = \sum_{i \in I \setminus \{j_0\}} \mu_i v_i$, dann setzen wir

   $$\lambda_i = \begin{cases} 1, & \text{falls } i = j_0 \\ -\mu_i, & \text{falls } i \in I \setminus \{j_0\} \end{cases}$$

   und es gilt $\sum_{i \in I} \lambda_i v_i = 0$.

□

Satz 2.11

Es sei $(v_i)_{i \in I} \in V^I$. Dann sind äquivalent:

1. $(v_i)_{i \in I}$ ist ein minimales Erzeugendensystem von V
2. $(v_i)_{i \in I}$ ist ein linear unabhängiges Erzeugendensystem von V
3. Jedes $v \in V$ besitzt eine eindeutige Darstellung als Linearkombination der v_i mit $i \in I$
4. $(v_i)_{i \in I}$ ist eine maximale lineare unabhängige Familie, d.h. für jedes $w \in V$ gilt: $(w, (v_i)_{i \in I})$ ist linear abhängig

Beweis: Zu zeigen ist 1. $\Rightarrow$ 2. $\Rightarrow$ 3. $\Rightarrow$ 4. $\Rightarrow$ 1. (Zirkelschluss).

1. $\Rightarrow$ 2. Wir zeigen $\neg 1. \Rightarrow \neg 2.$

   Sei $(v_i)_{i \in I}$ ein Erzeugendensystem, aber nicht linear unabhängig. Laut Lemma 2.10.5 existiert ein $j_0 \in I$, sodass $v_{j_0} = \sum_{i \in I \setminus \{j_0\}} \lambda_i v_i$ mit $\lambda_i \in K$, nur endlich viele $\lambda_i \neq 0$.

   Wir behaupten: $(v_j)_{j \in I \setminus \{j_0\}}$ ist ein Erzeugendensystem. Sei also $x \in V$, und $(v_i)_{i \in I}$ ein Erzeugendensystem. Es gilt: $x = \sum_{i \in I} \mu_i v_i = \sum_{i \in I \setminus \{j_0\}} + \mu_{j_0} v_{j_0} = \sum_{i \in I \setminus \{j_0\}} \mu_i v_i + \mu_{j_0} \sum_{i \in I \setminus \{j_0\}} \lambda_i v_i$ mit $\mu_i \in K$, nur endlich viele $\mu_i \neq 0$.

Damit ist aber $x = \sum_{j \in I \setminus \{j_0\}} \overbrace{(\mu_j + \mu_{j_0} v \lambda_j)}^{\vartheta_j} v_j = \sum_{j \in I \setminus \{j_0\}} \vartheta_j v_j$ mit $\vartheta_j \in K$, nur endlich viele $\vartheta_j \neq 0$.

2. $\Rightarrow$ 3. $v \in V \Rightarrow v = \sum_{i \in I} \lambda_i v_i$ (λ_i geeignet). Angenommen, die Darstellung sei nicht eindeutig, d.h. $v = \sum_{i \in I} \tilde{\lambda_i} v_i$, dann gilt $v - v = 0 = \sum_{i \in I} (\lambda_i - \tilde{\lambda_i}) v_i$, aus 2 folgt $\lambda_i - \tilde{\lambda_i} = 0 \Rightarrow \lambda_i = \tilde{\lambda_i}$, somit ist die Darstellung eindeutig

3. $\Rightarrow$ 4. Es sei eine eindeutige Darstellung für jedes $v \in V$. Zu zeigen ist:

   a) $(v_i)_{i \in I}$ ist linear unabhängig

   b) Für jedes $w \in V$ ist $(w, (v_i)_{i \in I})$ linear abhängig

   Zu a): Es sei $\sum_{i \in I} \lambda_i v_i = 0$ (λ_i geeignet). Es gilt $0 \in V$, die Darstellung $0 = \sum_{i \in I} \mu_i v_i$ mit $\mu_i = 0$ für jedes $i \in I$ ist eindeutig, also folgt $\lambda_i = \mu_i = 0 \; \forall i \in I$.

   Zu b): Sei $w \in V, w = \sum_{i \in I} \lambda_i v_i$ (λ_i geeignet). Dann gilt aber mit Lemma 2.10, dass $(w, (v_i)_{i \in I})$ linear abhängig ist.

4. $\Rightarrow$ 1. Sei $(v_i)_{i \in I}$ eine maximale lineare unabhängige Familie. Zu zeigen ist

   a) $\text{span}(\{v_i, i \in I\}) = V$

   b) $\text{span}(\{v_j, j \in J\}) \neq V$ für $J \subsetneq I$

   Zu a): Falls $w \in V \setminus \text{span}(\{v_i, i \in I\})$ existiert, ist $(w, (v_i)_{i \in I})$ linear unabhängig, denn $\mu_w + \sum_{i \in I} \lambda_i v_i = 0$ (mit $\lambda_i, \mu \in K$ geeignet) impliziert $\mu = 0$ und damit $\lambda_i = 0$ für alle $i \in I$. Das steht im Widerspruch zu der maximalen Unabhängigkeit der Familie.

   Zu b): Es sei $V = \text{span}(\{v_j : j \in J\}), J \subsetneq I$. Dann gilt v_{j_0} mit $j_0 \in I \setminus J$ lässt sich als Linearkombination $v_{j_0} = \sum_{j \in J} \lambda_j v_j$ schreiben, was ein Widerspruch zur linearen Unabhängigkeit der v_j darstellt.

□

Definition 2.12 – Basis eines Vektorraums

Eine Familie $(v_i)_{i \in I}$ mit $v_i \in V$ für alle $i \in I$ heißt Basis von V, falls $(v_i)_{i \in I}$ ein linear unabhängiges Erzeugendensystem von V ist.

Beispiel: $V = K^n$, Eine Basis ist gegeben durch $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$, wobei der i-te Eintrag 1 beträgt. Diese $(e_i)_{i \in \{1, \ldots, n\}}$ heißt kanonische (oder Standard-) Basis von K^n.
Bemerkung: Die kanonische Basis wurde hier aus Platzgründen zeilenweise statt vektoriell geschrieben.

Satz 2.13 – Basisauswahlsatz

Es sei $N \in \mathbb{N} \cup \{0\}$, $v_1, \ldots, v_N \in V$ und $v = span(\{v_1, \ldots, v_N\})$. Dann existieren $i_1, \ldots, i_n \in \{1, \ldots, N\}$, sodass $(v_{i_1}, \ldots, v_{i_n})$ eine Basis von V bilden.

Beweis: Wir verkleinern die Familie $(v_i)_{i \in \{1, \ldots, N\}}$ schrittweise:

1. Falls $(v_i)_{i \in \{1, \ldots, N\}}$ linear unabhängig ist, sind wir fertig.

2. Andernfalls existiert $j_0 \in \{1, \ldots, N\}$, so dass $v_{j_0} = \sum_{i \in \{1, \ldots, j_0 - 1, j_0 + 1, \ldots, N\}} \lambda_i v_i$. Damit ist aber $(v_1, \ldots, v_{j_0 - 1}, v_{j_0 + 1}, \ldots, v_n)$ immer noch ein Erzeugendensystem.

   Mit der Menge wiederholen wir den Schritt. Nach maximal N Schritten ist die Methode zum Ende gelangt.

□

Lemma 2.14

Sei $(v_1, \ldots, v_n)$ eine Basis von V, $w = \lambda_1 v_1 + \cdots + \lambda_n v_n$ mit $\lambda_a \neq 0$ für $a \in \{1, \ldots, n\}$. Dann gilt $(v_1, \ldots, v_{a-1}, w, v_{a+1}, \ldots, v_n)$ ist eine Basis.

Beweis: Durch Umnummerierung der Basisvektoren können wir annehmen, dass gilt $a = 1$. Sei also oBdA $a = 1$. Zu zeigen ist nun, dass $(w, v_2, \ldots, v_n)$ ein Erzeugendensystem (1.) und zusätzlich linear unabhängig (2.) ist.

1. Für $x \in V$ gilt $x = \mu_1 v_1 + \ldots + \mu_n v_n$, $\mu_i \in K$. Wir schreiben

$$v_1 = \lambda^{-1}(w - \lambda_2 v_2 - \ldots - \lambda_n v_n 0 + \ldots + \mu_n v_n)$$

   denn $\lambda_1 \neq 0$. Dann gilt

$$\begin{aligned} x = \quad & \mu_1 \lambda_1^{-1} w \\ & + (\mu_2 - \lambda_1^{-1}\lambda_2) v_2 \\ & + \quad \ldots \\ & + (\mu_n - \lambda_1^{-1}\lambda_n) v_n \end{aligned}$$

   und $(w, v_2, \ldots, v_n)$ ist ein Erzeugendensystem von V.

2. Sei $0 = \mu_1 w + \mu_2 v_2 + \ldots + \mu_n v_n$. Wir setzen w ein, und erhalten

$$0 = \mu_1 \lambda_1 v_1 + (\mu_2 + \mu_1 \lambda_2) v_2 + \ldots + (\mu_n + \mu_1 \lambda_n) v_n$$

   Nun ist aber nach Annahme $(v_1, \ldots, v_n)$ eine Basis von V. Also gilt $\mu_1 \lambda_1 = 0$, $\mu_2 + \mu_1 \lambda_2 = 0$, $\ldots$, $\mu_n + \mu_1 \lambda_n = 0$.

   Damit folgt $(\lambda_1 \neq 0) \Rightarrow \mu_1 = 0 \;\Rightarrow\; \mu_2 = 0,\ \mu_3 = 0,\ \ldots,\ \mu_n = 0$. Also sind $(w, v_2, \ldots, v_n)$ linear unabhängig und somit eine Basis von V.

□

Satz 2.15 – Basisaustauschsatz von Steinitz

Es sei $(v_1, \ldots, v_n)$ eine Basis von V und $(w_1, \ldots, w_m)$ sei eine linear unabhängige Familie von Vektoren in V. Dann gilt:

1. $m \leq n$
2. $(v_1, \ldots, v_n)$ kann so umnummeriert werden, dass $(w_1, \ldots, _m\,, v_{m+1}, \ldots, v_n)$ eine Basis ist.

Beweis: Erfolgt durch Induktion über m:

IA: Für $m = 0$ ist nichts zu zeigen.

IS: „$m \to m + 1$“

Sei $(w_1, \ldots, w_{m+1})$ also eine linear unabhängige Familie. Es gilt nach Lemma 2.10.4, dass $(w_1, \ldots, w_m)$ linear unabhängig sind. Nach der Induktionsannahme gilt also

i. $m \leq n$

ii. $(w_1, \ldots, w_m, v_{m+1}, \ldots, v_n)$ ist eine Basis von V (nach geeigneter Umnummerierung)

Zu zeigen ist nun:

a) $m + 1 \leq n$

b) $(w_1, \ldots, w_{m+1}, v_{m+2}, \ldots, v_n)$ ist eine Basis von V (nach geeigneter Umnummerierung)

Zu a): Wir zeigen die Aussage durch einen Widerspruch und nehmen also an, dass gilt: $m+1 > n$. Es folgt nach i.: $m \leq n$, dass $m = n$. Damit ist aber laut Induktionsannahme $(w_1, \ldots, w_m)$ eine Basis von V, also eine maximal linear unabhängige Familie, damit kann $(w_1, \ldots, w_{m+1})$ nicht mehr linear unabhängig sein ↯

Zu b): Es sei $w_{m+1} = \lambda_1 w_1 + \ldots + \lambda_m w_m + \lambda_{m+1} v_{m+1} + \ldots + \lambda_n v_n$. Es muss aber ein $a \geq m+1$ existieren mit $\lambda_a \neq 0$ (denn sonst wären $(w_1, \ldots, w_m)$ linear abhängig). Nach Lemma 2.14 kann v_a durch w_{m+1} ersetzt werden. Umnummerierung liefert das Ergebnis.

□

Korollar 2.16 – Alle Basen eines Vektorraumes haben gleich viele Elemente

V besitze eine Basis $(v_1, \ldots, v_n)$ mit $n \in \mathbb{N} \cup \{0\}$. Dann hat jede Basis von V genau n Elemente.

Beweis: Sei $(w_i)_{i \in I}$ eine weitere Basis. Es folgt sofort, dass die Anzahl der Elemente $\leq n$ ist. Insbesondere ist I endlich. Falls $m = \#I < n$ liefert das selbe Argument mit (v_I) und (w_i) vertauscht wieder einen Widerspruch ↯ □

Definition 2.17 – Dimension

Es sei V ein K-Vektorraum. Wir setzen

$$\dim_K(V) = \begin{cases} \infty, & \text{falls } V \text{ keine endliche Basis besitzt} \\ n, & \text{falls } V \text{ eine Basis mit } n \text{ Elementen besitzt} \end{cases}$$

$\dim_K(V)$ heißt Dimension von V.

Satz 2.18 – Basisergänzungssatz von Steinitz

Falls V endlich erzeugt ist, und $(w_i)_{i \in I}$ eine linear unabhängige Familie von Vektoren ist, dann existiert eine Basis von V, die alle w_i enthält. Insbesondere besitzt jeder endlich erzeugte Vektorraum eine Basis.

Beweis: Es seien $\{v_1, \ldots, v_n\} \subset V$ mit $n \in \mathbb{N} \setminus \{0\}$, mit $\operatorname{span}(\{v_1, \ldots, v_n\}) = V$. Aus dem Basisauswahlsatz folgt sofort Existenz einer Basis. Der Rest folgt mit Basisergänzungssatz. [Literaturangabe benötigt]

□

Lemma 2.19

Falls $\dim_k(v) = n$ mit $n \in \mathbb{N} \cup \{0\}$, dann gilt:

1. Falls $(v_1, \ldots, v_n)$ linear unabhängig ist, dann ist $(v_1, \ldots, v_n)$ bereits eine Basis
2. Falls $W \subset V$ ein Untervektorraum ist, so gilt

$$\dim_K(W) \leq \dim_K(V) \text{ und}$$
$$\dim_K(W) = \dim_K(V) \;\Rightarrow\; W = V$$

Beweis:

1. Folgt aus dem Basisaustauschsatz
2. Angenommen $(w_1, \ldots, w_m)$ sind linear unabhängig in W. Dann sind sie auch in V linear unabhängig. Damit folgt $m \leq n = \dim_K(V)$. Es folgt $\dim_K(W) \leq n$. Falls $\dim_K(W) = \dim_K(V)$ dann ist eine Basis von W nach 1. auch eine Basis von V. Also folgt sofort $V = W$.

□

Bemerkung: Es gibt nicht nur endlich erzeugte Vektorräume.

Beispiele:

1. $\mathbb{R}^{\mathbb{N}}$, also $(x_1, x_2, \ldots)$ mit eintragsweiser Addition (d.h. für $x = (x_1, \ldots), y = (y_1, y_2, \ldots)$ schreiben wir $x + y = (x_1 + y_2.x_2 + y_2, \ldots)$ und eintragsweiser Skalarmultiplikation (d.h. $\lambda x = (\lambda x_1, \lambda x_2, \ldots)$) ist ein $\mathbb{R}$ -Vektorraum. Es gilt $\dim_K(V) = \infty$, denn, angenommen $\dim_K(V) = n$, für $n \in \mathbb{N}_0$ kann man leicht $n + 1$ linear unabhängige Vektoren finden (z.B. $(1, 0, \ldots), (0, 1, 0, \ldots), \ldots, (0, \ldots, 0, 1, 0, \ldots)$) was einen Widerspruch darstellt ↯

   Die Vektoren $(1, 0, \ldots), (0, 1, 0, \ldots), \ldots)$ stellen auch keine Basis dar, insbesondere gibt es keine abzählbare Basis für V.

2. Die Menge konvergenter Folgen

3. $\mathrm{Abb}(\mathbb{R}, \mathbb{R})$

4. Die Menge der stetigen reellen Funktionen

5. $\{x \in \mathbb{R}^{\mathbb{N}}, x = (x_1, x_2, \ldots)$ mit endlich vielen $x_i \neq 0\} \subset \mathbb{R}^{\mathbb{N}}$. Hier ist $((1, 0, \ldots), (0, 1, 0, \ldots), \ldots)$ eine Basis.

Satz 2.20 – Existenz einer Basis

Jeder Vektorraum besitzt eine Basis.

Beweisidee: Es sei V ein K-Vektorraum. Es sei $\mathfrak{M} = \{A \subset V : A \text{ linear unabhängig}\} \subset 2^V$. Auf $\mathfrak{M}$ definiert „$\subset$“ eine Halbordnung, d.h. es gilt

1. $A \subset A$
2. $A \subset B \wedge B \subset A \Rightarrow A = B$
3. $A \subset B, B \subset C \Rightarrow A \subset C$

Wir betrachten nun Teilmengen $U \subset \mathfrak{M}$, welche total geordnet sind, d.h. für $A, B \in U$ gilt immer $A \subset B$ oder $B \subset A$.

Ein kurzes Beispiel aus $2^{\mathbb{R}}$ für U ist $U = \{(-j, j), j \in \mathbb{N}\}$. Solche Teilmengen von $\mathfrak{M}$ heißen auch Ketten. Nun sei $\mathcal{M}(U) = \bigcup_{A \in U} A$. Es gilt nun:

1. $\mathcal{M}(U) \subset V$
2. Für alle $A \in U : A \subset \mathcal{M}(U)$
3. Es seien $v_1, \ldots v_n$ Vektoren in $\mathcal{M}(U)$ und $\lambda_1, \ldots, \lambda_n \in K$, sodass gilt $\lambda_1 v_1 + \ldots + \lambda_n + v_n = 0$. Es existiert ein $\mathcal{A} \in U$, so dass $v_1, \ldots, v_n \in \mathcal{A}$, denn für $j = 1, \ldots, n$ existiert $A_j \in U$ mit $v_j \in A_j$. Nachdem U aber total geordnet ist, ist eines der A_j das größte davon, dieses nennen wir $\mathcal{A}$. Dieses $\mathcal{A}$ ist aber linear unabhängig, denn $\mathcal{A} \in \mathfrak{M}$. Damit folgt aber $\lambda_1 = \cdots = \lambda_n = 0$ und es gilt $\mathcal{M}(U)$ ist linear unabhängig und $\mathcal{M}(U) \in \mathfrak{M}$

Anders gesagt: jede Kette in $\mathfrak{M}$ besitzt eine obere Schranke in $\mathfrak{M}$.

Wir benutzen nun das Lemma von Zorn: Es sei $\mathfrak{M}$ eine Menge mit Halbordnung „$\subset$“, so dass jede Kette in $\mathfrak{M}$ eine obere Schranke in $\mathfrak{M}$ besitzt. Dann existiert ein maximales Element m in $\mathfrak{M}$, d.h. ein Element m, so dass gilt $B \in \mathfrak{M}, m \subset B \Rightarrow B = m$.

Angewendet auf unseren Fall ergibt sich sofort ein maximales Element aus $\mathfrak{M} = \{A \in V : A \text{ linear unabhängig}\}$, also eine maximale lineare unabhängige Familie, d.h. eine Basis.

Das Lemma von Zorn ist (in der üblichen Mengenlehre nach Zermelo und Fraenkel, welche man in der Logik kennenlernt) äquivalent zum Auswahlaxiom (auch kennenzulernen in der Logik), welches besagt:

Sei $X = \{U_i, i \in I\}$ eine Menge von Mengen, dann existiert eine sogenannte Auswahlfunktion

$$F : X \to \bigcup_{i \in I} U_i \quad \text{mit} \quad F(U_i) = a_i \in U_i.$$

3. Lineare Abbildungen

Wir kennen schon lineare Abbildungen von $\mathbb{R}^n$ nach $\mathbb{R}^m$, nämlich diejenigen, welche durch Matrizen dargestellt werden.

3.1 Definition und grundlegende Eigenschaften

Im Folgenden sei K ein Körper und V ein K-Vektorraum.

Definition 3.1 – Lineare Abbildungen

Es seien V, W K-Vektorräume.

1. Eine Abbildung $F : V \to W$ heißt K-linear (oder Vektorraumhomomorphismus) falls gilt:

   $$\text{(a)} \quad F(x+y) = F(x) + F(y)$$
   $$\text{(b)} \quad F(\lambda x) = \lambda F(x)$$

   für alle $x, y \in V, \lambda in K$ und wir schreiben $F \in \mathrm{Hom}_K(V, W)$

2. Falls $V = W$, so heißt $F \in \mathrm{Hom}_K(V, W) = \mathrm{End}_K(V)$ Vektorraumendomorphismus

3. Ein Vektorraum-Komorphismus ist ein bijektiver Vektorraumhomomorphismus. Falls ein solcher Komorphismus von V nach W existiert, nennen wir W und V isomorph, und schreiben $V \cong W$

4. $\mathrm{Aut}_K(V) = \{F \in \mathrm{End}_K(V) : F \text{ bijektiv}\}$ sind die Vektorraum-Automorphismen von V

Bemerkung:

1. $\hat{V} \subset V$ ein Untervektorraum, dann ist die Inklusion $i : \hat{V} \to V, i(x) = x$ ein Vektorraumhomomorphismus

2. $\mathrm{Hom}_K(V, W) \subset \mathrm{Abb}(V, W)$ ist ein Untervektorraum

3. $\mathrm{End}_K(V)$ hat zusätzlich die Struktur eines Ringes mit Addition punktweise definiert, d.h.

   $$(F+G)(x) = F(x) + G(x)$$

   und Multiplikation als Hintereinanderausführung. Es gilt die Kompatibilitätseigenschaft

   $$(\lambda F) \circ G = \lambda(F \circ G) = F \circ (\lambda G) \quad \text{für alle} \quad F, G \in \mathrm{End}_K(V), \lambda \in K$$

   Eine solche Struktur (Ring, Vektorraum, Komposition) heißt K-Algebra.

4. $\mathrm{Aut}_K(V)$ ist eine Gruppe (mit Nacheinanderausführung als Verknüpfung). Aber: $\mathrm{Aut}_K(V)$ ist kein Vektorraum, außer $V = \{0\}$

Beweise : Siehe Übung.

Beispiele:

1. Matrizen induzieren lineare Abbildungen

2. $$V = \{f \in Abb(\mathbb{R}, \mathbb{R}) : f \text{ stetig differenzierbar}\}$$
   $$W = \{f \in Abb(\mathbb{R}, \mathbb{R}) : f \text{ stetig}\}$$

   Dann ist $D : V \to W, f \mapsto f'$ eine lineare Abbildung.

Bemerkung: Das Lösen von reellen linearen Gleichungssystemen $Ax = b$ entspricht also der Bestimmung der Menge $A^{-1}(\{b\})$, wobei A sowohl als (Koeffizienten-) Matrix als auch als lineare Abbildung aufgefasst werden kann.

Lemma 3.2 – Eigenschaften linearer Abbildungen

U, V, W seien K-Vektorräume, $F \in \mathrm{Hom}_K(V, W), G \in \mathrm{Hom}_K(U, V)$. Dann gilt

1. $F(0) = 0$
2. $F(x - y) = F(x) - F(y)$
3. $F \circ G \in Hom_K(U, W)$
4. Ist F ein Isomorphismus $\Rightarrow F^{-1} \in \mathrm{Hom}_K(W, V)$.
5. Sei I eine Indexmenge, $(v_i)_{i \in I} \in V^I$, dann gilt

$$(v_i)_{i \in I} \text{ linear abhängig } \Rightarrow (F(v_i))_{i \in I} \in W^I \text{ linear abhängig}$$

6. (a) Sei $\hat{V} \subset V$ ein Untervektorraum. Dann ist $F(\hat{V}) \subset W$ ebenfalls ein Untervektorraum. Insbesondere ist $\mathrm{Im}(F) = F(V)$ ein Untervektorraum.
   (b) Sei $\hat{W} \subset W$ ein Untervektorraum. Dann ist $F^{-1}(\hat{W}) \subset V$ ebenfalls ein Untervektorraum. Insbesondere ist $\ker(F) = F^{-1}(\{0\})$ ein Untervektorraum.
   (c) Sei F ein Isomorphismus. Dann gilt $F(\hat{V}) \cong \hat{V}$ für jeden Untervektorraum $\hat{V} \subset V$.
7. $\dim(Im(F)) \leq \dim(V)$

Beweis: Übungen.

Bemerkung: Es gilt natürlich auch $(F(v_i))_{i \in I}$ linear unabhängig $\Rightarrow (v_i)_{i \in I}$ linear unabhängig

Satz 3.3 – Definition linearer Abbildung durch Basis

Es seien V, W K-Vektorräume, I eine Indexmenge, $(v_i)_{i \in I}$ eine Basis von V. Weiterhin sei $(w_j)_{j \in I} \in W^I$ eine Familie von Vektoren in W. Dann existiert genau eine K-lineare Abbildung $F : V \to W$ mit $f(v_j) = w_j$ für alle $j \in I$.

Dieses F erfüllt weiterhin

1. $\mathrm{Im}(F) = \mathrm{span}(\{w_j : j \in I\})$
2. F injektiv $\Leftrightarrow (w_j)_{j \in I}$ linear unabhängig.

Beweis: Es sei $x \in V$. Damit existiert eine eindeutige Linearkombination $x = \sum_{j \in I} \lambda_j v_j$. Wir setzen

$$F(x) = \sum_{j \in I} \lambda_j w_j = \sum_{j \in I} \lambda_f F(v_j).$$

Nachdem F linear sein soll, ist dies die einzig mögliche Form von F, es existiert also höchstens eine solche lineare Abbildung. Es ist mittels Einsetzen leicht zu überprüfen, dass gilt

$$F(x + y) = F(x) + F(y) \text{ sowie}$$
$$F(\lambda x) = \lambda F(x)$$

Damit ist das oben definierte F linear und es existiert genau ein $F \in \mathrm{Hom}_K(V, W)$ mit den gewünschten Eigenschaften.

Zu 1.: Folgt direkt aus der Definition von F

Zu 2.: Es gilt F nicht injektiv

$$\begin{aligned} &\Leftrightarrow \exists x, y \in V, x \neq y : && F(x) = F(y) \\ &\Leftrightarrow \exists z \neq 0 : z = x - y : && F(z) = 0 \\ &\Leftrightarrow z = \sum_{j \in I} \lambda_j v_j \end{aligned}$$

und nicht alle $\lambda_j = 0$.
Somit ist $F\left(\sum_{j\in I} \lambda_j v_j\right) = \sum_{j\in I} \lambda_j F(v_j) = \sum_{j\in I} \lambda_j w_j = 0$ und $(w_j)_{j\in I}$ ist linear abhängig.

□

Bemerkung: Der Satz 3.3 besagt, dass man eine lineare Abbildung bereits kennt, wenn man ihre Wirkung auf alle Basisvektoren kennt.

Proposition 3.4

Es gilt $G \in \mathrm{Hom}_K(V, W)$ ist injektiv genau dann, wenn $\ker(G) = \{0\}$.

Beweis: Wurde bereits im Beweis von Satz 3.3 gezeigt. □

Korollar 3.5

Es sei V ein K-Vektorraum mit $\dim_K(V) = n < \infty$. Dann gilt $V \cong K^n$. Weiterhin sei W ein K-Vektorraum mit $\dim_K(W) = n$, dann gilt auch $V \cong W$.

Beweis: Nach dem Basisergänzungssatz existiert eine Basis $(v_1, \ldots, v_n)$ von V. Weiterhin sei $(e_1, \ldots, e_n)$ die Standardbasis von K^n. Dann gilt nach Satz 3.3, dass für genau eine K-lineare Abbildung ein F existiert mit $F(v_i) = e_i$ für $i = 1, \ldots, n$. F ist surjektiv, denn $\mathrm{Im}(F) = F(V) = \mathrm{span}(\{e_1, \ldots, e_n\}) = K^n$.
F ist injektiv, denn $(e_1, \ldots, e_n)$ ist linear unabhängig, der Schluss folgt mit Satz 3.3.2.

Ebenso für $V \cong W$.
Bemerkung: Der K^n ist also in einem gewissen Sinn der einzige n-dimensionale K-Vektorraum. Der Isomorphismus hängt von der Wahl der Basis in V ab, ist also nicht eindeutig bestimmt (man sagt, er ist nicht kanonisch). □

Bemerkung: Das Korollar hilft bei Fragen wie „Was ist die Lösungsmenge von $F(x) = 0$“ mit $F : V \to W$ linear, $\dim_K(V) = n < \infty$ endlich, $\dim_K(W) = m < \infty$, denn wir haben einen Isomorphismus $G : U \to K^n$, $H : W \to K^m$ und berechnen $F(x) = 0 \Leftrightarrow \tilde{F}(G(x)) = H(0)$ mit einer Abbildung $\tilde{F} : K^n \to K^m$, $\tilde{F}(v_i) = H(F(G^{-1}(e_i)))$ und es folgt mit Lemma 3.2: $\dim_K(\ker(F)) = \dim_K(\ker(\tilde{F}))$.

Definition 3.6

Seien V, W K-Vektorräume, $F \in \mathrm{Hom}_K(V, W)$. Dann heißt

$$\mathrm{rg}(F) = \dim_K(F(V)) = \dim_K(\mathrm{Im}(F))$$

der Rang von F.

Bemerkung: Falls G, $\tilde{G}$ Isomorphismen sind, so gilt $\mathrm{rg}(F) = \mathrm{rg}(F \cong G) = \mathrm{rg}(\tilde{G} \cong F)$ mit $F : V \to W$, $G : \tilde{V} \to V$, $\tilde{G} : W \to \tilde{W}$. Die Reihenfolge von Isomorphismenschaltungen ändert also den Rang nicht.

Satz 3.7 – Dimensionsformel

Es seien V, W K-Vektorräume, $F \in \mathrm{Hom}_K(V, W)$, $\dim_K(V)$ endlich. Dann gilt

$$\dim_K(V) = \dim_K(\ker(F)) + \mathrm{rg}(F).$$

Beweis: Nach Lemma 3.2 ist $\ker(F) \subset V$ ein Untervektorraum, also endlichdimensional [Literaturangabe benötigt]. Weiter ist $\mathrm{Im}(F) \subset W$ ein Untervektorraum, also mit $\dim_K(\mathrm{Im}(F))$ endlichdimensional [Literaturangabe benötigt]. Sei also $(v_1, \dots v_m)$ eine Basis von $\ker(F)$, $(w_1, \dots, w_r)$ eine Basis von $\mathrm{Im}(F)$ und es seien $u_1, \dots, u_r$ Vektoren in V mit $F(u_j) = w_j$ für $j = 1, \dots, r$.

Zu zeigen ist nun, dass $m + r = \dim_K(V)$ ist. Wir beweisen, dass $(v_1, \dots, v_m, u_1, \dots, u_r)$ eine Basis von V ist:

1. $(v_1, \dots, v_m, u_1, \dots, u_r)$ erzeugt V. Es sei also $x \in V$ beliebig. Es existieren $\lambda_1, \dots, \lambda_r \in K$ mit $F(x) = \sum_{j=1}^{r} \lambda_j w_j$, denn $(w_j)_{j=1,\dots,r}$ sind die Basis von $\mathrm{Im}(F)$. Nun sei $y = x - \sum_{j=1}^{r} \lambda_j v_j \in V$. dann gilt

$$F(y) = F(x) - F\left(\sum_{j=1}^{r} \lambda_j v_j\right) = F(x) - \sum_{j=1}^{r} \lambda_j F(v_j) = F(x) - \sum_{j=1}^{r} \lambda_j w_j = F(x) - F(x) = 0.$$

   Damit ist $y \in \ker(F)$ und es existieren $\mu_1, \dots, \mu_m$, sodass $y = \sum_{i=1}^{m} \mu_i v_i$. Damit gilt aber $x = \sum_{i=1}^{m} \mu_i v_i + \sum_{j=1}^{r} \lambda_j v_j$ und $x \in \mathrm{span}(\{v_1, \dots, v_m, u_1, \dots, u_r\})$.

   Somit erzeugt $(v_1, \dots, v_m, u_1, \dots, u_r)$ den Vektorraum V.

2. Nun ist zu zeigen, dass $(v_1, \dots, v_m, u_1, \dots, u_r)$ linear unabhängig ist.

   Es seien $\lambda_1, \dots, \lambda_m, \mu_1, \dots, \mu_r \in K$ mit $\sum_{i=1}^{m} \lambda_i v_i + \sum_{j=1}^{r} \mu_j u_j = 0$. Dann folgt

$$0 \overset{L3.2}{=} F(0) = \underbrace{\sum_{i=1}^{m} \lambda_i F(v_i)}_{=0} + \sum_{j=1}^{r} \mu_j F(v_j) = \sum_{j=1}^{r} \mu_j w_j \;\Rightarrow\; \mu_j = 0$$

   denn $(w_j)_{j=1,\dots,r}$ bilden eine Basis und sind somit linear unabhängig.

   Damit gilt $\sum_{i=1}^{m} \lambda_i v_i = 0$ also $\lambda_i = 0$ für $i = 1, \dots, m$, denn $(v_i)_{i=1,\dots,m}$ sind auch linear unabhängig.

□

Definition 3.8 – Direkte Summe

Es sei V ein K-Vektorraum, V_1, V_2 Untervektorräume.

1. Wir schreiben $V_1 + V_2 = \mathrm{span}(V_1 \cup V_2)$
2. $W = V_1 \oplus V_2$, falls $W = V_1 + v_2$ und $V_1 \cap V_2 = \{0\}$. W heißt dann direkte Summe von V_1 und V_2. V_1 und V_2 heißen dann komplementär.

Stichwortverzeichnis

Äquivalenz
- Klasse, 17
- Relation, 16

Abbildung, 13
- Bijektivität, 14
- Bild, 13
- Identische, 15
- Injektivität, 14
- Komposition, 14
- Menge, 15
- Surjektivität, 14
- Umkehr-, 14
- Urbild, 13

Abbildungen
- Homomorphismus, 19
- Isomorphismus, 19

Aussagen, 11

Ebene, 8
Erzeugendensystem, 28

Familie, 28

Gerade, 8
- Gleichheit, 8
- Parallelität, 8

Gruppe, 18
- abelsche, 18
- Translation, 18
- Unter-, 19
- zyklische, 20

Körper, 21
- Charakteristik, 24

Lineare
- Abbildungen, 35
- Gleichungssysteme, 3
  - Gauß-Jordan-Elimination, 5
  - Normalform, 4
  - Zeilenoperationen, 5
- Unabhängigkeit, 7

Logische Operatoren, 11

Menge, 12
- Aller Abbildungen, 15
- Operationen, 12
- Potenz-, 15
- Quotienten-, 17
- Teil-, 12

Metrik, 10

Relation, 16
Ring, 20
- -homomorphismus, 21
- Charakteristik, 24
- Unter-, 21

Skalar
- -produkt, 9

Ungleichung
- Cauchy-Schwarzsche, 9
- Dreicks, 10

Vektorraum, 25
- Basis, 30
  - -austauschsatz, 31
  - -auswahlsatz, 30
- Dimension, 32
- Unter-, 26

Zahlen
- Ganze, 12
- Komplexe, 22
- Natürliche, 12
- Rationale, 12
- Reelle, 3