

Lineare Algebra

Lucas Westermann

May 29, 2011

Contents

Literatur	4
1 Grundlegendes	4
1.1 Mengen	4
1.1.1 Definition (Relation)	4
1.1.2 Beispiel	4
1.1.3 Beispiel	4
1.1.4 Beispiel	5
1.1.5 Beispiel	5
1.1.6 Beschreibung (Gerichtete Graphen)	5
1.1.7 Beispiel	6
1.1.8 Definition (Äquivalenzrelation)	6
1.1.9 Beispiel	6
1.1.10 Beispiel	6
1.2 Abbildungen	7
1.2.1 Definition (Abbildungen, Funktion)	7
1.2.2 Bemerkung	7
1.2.3 Beispiel (identische Abbildung)	8
1.2.4 Beispiel	8
1.2.5 Beispiel (ASCII-Code)	8
1.2.6 Definition (Umkehrabbildung)	9
1.2.7 Bemerkung	9
1.2.8 Korollar	9
1.3 Matrizen	9
1.3.1 Definition (Matrix)	10
1.3.2 Beispiel (n Tupeln, m -Spalten)	10
1.3.3 Kronecker-Symbol, Einheits- und Nullmatrixe)	10
1.3.4 Beispiel (Diagonal- und Dreieckmatrizen)	11
1.3.5 Bemerkung	11
1.3.6 Beispiel	12
1.3.7 Beispiel	12
1.3.8 Beispiel (RGB - Raum)	12
1.3.9 Beispiel (Inzidenzmatrix)	12
1.3.10 Satz (Rechenregeln für Matrizen)	13
1.4 Lineare Gleichungen	13
1.4.1 Definition (lineare Gleichung)	13
1.4.2 Bemerkung	14
1.4.3 Satz(Superpositionsprinzip)	14
1.4.4 Satz	14

1.4.5	Beispiel	14
1.4.6	Beispiel (Rückwärts-Substitution)	15
1.4.7	Beispiel	16
1.4.8	Satz	17
1.4.9	Satz	17
2	Lineare Räume	18
2.1	Algebraische Strukturen	18
2.1.1	Definition (Gruppe)	18
2.1.2	Bemerkung	18
2.1.3	Bemerkung (Potenzen)	18
2.1.4	Beispiel	18
2.1.6	Beispiel (modulo)	19
2.1.7	Beispiel (symmetrische Gruppe)	19
2.1.8	Korollar (Rechnen in Gruppen)	19
2.1.9	Definition (Körper)	19
2.1.10	Beispiel	20
2.1.11	Beispiel (Restklassenkörper modulo p)	20
2.1.12	Korollar	21
2.1.13	Bemerkung	21
2.1.14	Beweis	21
2.2	Vektorräume	22
2.2.1	Definition (linearer Raum, Vektorraum)	22
2.2.2	Beispiel	22
2.2.3	Beispiel	23
2.2.4	Beispiel (Lösungsmengen)	23
2.2.5	Beispiel (Funktionsräume)	23
2.2.6	Korollar	24

Literatur

Mathematik für Informatiker: Teschl, Hackenberger

Lineare Algebra: Beutelspacher, Fischer, Lang (auf Englisch), Stambach.

1 Grundlegendes

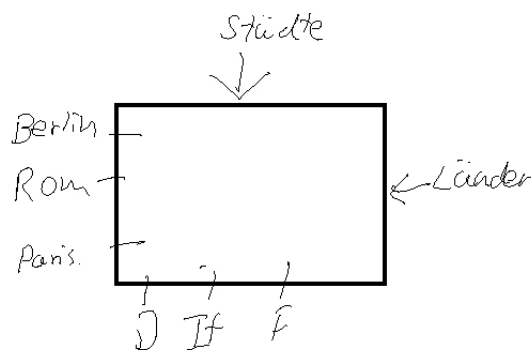
1.1 Mengen

1.1.1 Definition (Relation)

Gegeben sein Mengen X und Y . Eine Teilmenge des kartesisches Produkt $X \times Y = \{(x, y) : x \in X, y \in Y\}$ heißt Relation (R) zwischen X und Y ; im Fall $X = Y$ spricht man von einer Relation auf X . Ferner: $R_1^{-1} = \{(y, x) \in Y \times X : (x, y) \in R\}$ heißt Umkehrrelation.

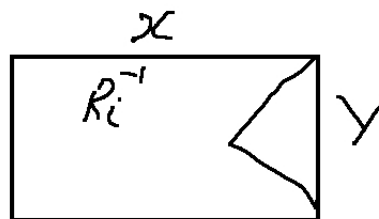
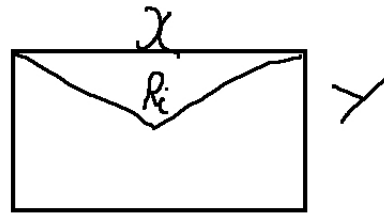
1.1.2 Beispiel

Die Menge $R_0 = \{(x, y) \in X \times Y : y \text{ ist Hauptstadt von } x\}$ ist eine Relation zwischen der Menge X aller Länder und Y aller Städte.



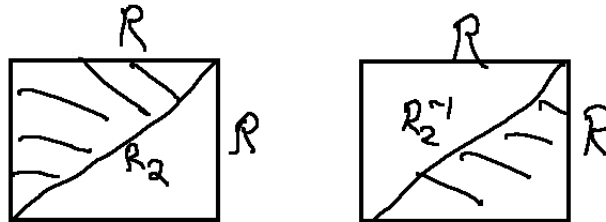
1.1.3 Beispiel

Mit den Mengen $X = \mathbb{R}$ $Y = [0, \infty)$ ist $R_1 = \{(x, |x|) \in X \times Y, x \in X\}$ ist eine Relation mit der Umkehrrelation $R^{-1} = \{(|x|, x) : x \in X\}$.



1.1.4 Beispiel

Mit den Mengen $X = Y = \mathbb{R}$ ist $R_2 = \{(x, y) \in X \times Y : x \leq y\}$ eine Relation $R_2^{-1} = \{(y, x) : x \leq y\}$

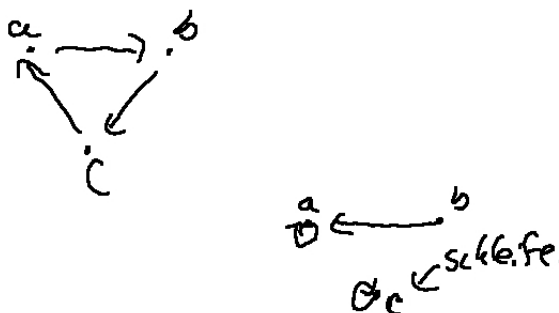


1.1.5 Beispiel

Die Menge $R_3 = \{(x, y) \in C \times C : x \text{ und } y \text{ haben gleichen Hersteller}\}$ ist eine Relation auf der Menge aller Computer C .

1.1.6 Beschreibung (Gerichtete Graphen)

Relation R auf endlichen Mengen X können alternative wie folgt dargestellt werden. Man repräsentiert die Elemente von X als Punkte in der Ebene (Knoten) und verbindet $x, y \in X$ genau dann durch einen Pfeil (gerichtete Kante), wenn $(x, y) \in R$. Das paar (X, R) heißt gerichteter Graph oder Digraph, z.B. $X = \{a, b, c\}$ $R = \{(a, b), (b, c), (c, d)\}$.



$$X = \{a, b, c\} \quad R = \{(b, a), (a, a), (c, c)\}.$$

Eine Relation R auf X heißt

reflexiv $\Leftrightarrow (x, x) \in R$ für alle $x \in X$

transitiv $\Leftrightarrow (x, y) \in R \Rightarrow (x, z) \in R$ für alle $x, y, z \in X$

symmetrisch $\Leftrightarrow (x, y) \in R$ für alle $x, y \in X$

1.1.7 Beispiel

Die Relation R_2 aus Beispiel 1.1.4 ist reflexiv, transitiv, aber nicht Symmetrisch. Die Relation R_3 aus Beispiel 1.1.5 ist reflexiv, transitiv und symmetrisch.

1.1.8 Definition (Äquivalenzrelation)

Eine Relation A auf eine Menge X heißt eine Äquivalenzrelation, falls sie reflexiv, transitiv und symmetrisch ist. Für ein Paar $(x, y) \in A$ Schreiben wir $x \sim y$ und nennen x und y äquivalent.

1.1.9 Beispiel

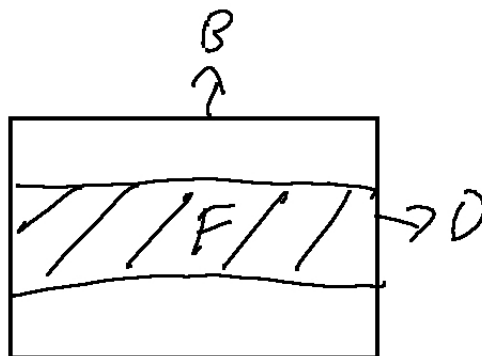
1. Sei X eine beliebige Menge. Dann ist $\{(x, y) \in X \times X : x = y\}$ eine Äquivalenzrelation (Identitätsrelation).
2. Ebenso ist das ganze Produkt $X \times X$ eine Äquivalenzrelation (Allrelation).
3. Die Relation R_3 aus Beispiel 1.1.5 ist eine Äquivalenzrelation. Mit ihr lassen sich Computer nach ihrem Hersteller klassifizieren. Für jedes $[x] := \{y \in X : x \sim y\}$ die von X erzeugte Äquivalenzklasse und ein Element $y \in [x]$ heißt Repräsentant von $[x]$.

1.1.10 Beispiel

1. Für die Identitätsrelation ist $[x] = \{x\}$ für alle $x \in X$. Die Allrelation besitzt genau eine Äquivalenzklasse $[x] = X$.
2. Im Beispiel 1.1.5 sind die Äquivalenzklassen die Menge aller Hersteller.

1.2 Abbildungen

$$F \subseteq D \times B.$$



1.2.1 Definition (Abbildungen, Funktion)

Eine Relation F zwischen zwei nichtleeren Mengen D und B heißt Abbildung oder Funktion von D nach B , falls für alle $x \in D$ gilt.

1) Es existiert ein $y \in B$ mit $(x, y) \in F$

2) Mit $y_1, y_2 \in B$ folgt aus $(x, y_1) \in F$ und $(x, y_2) \in F$, dass $y_1 = y_2$.

Die Menge D heißt Definitionsbereich und B Bildbereich von F . Im Fall $D = B$ spricht man von einer Abbildung auf D oder um einer Selbstabbildung auf D .

1.2.2 Bemerkung

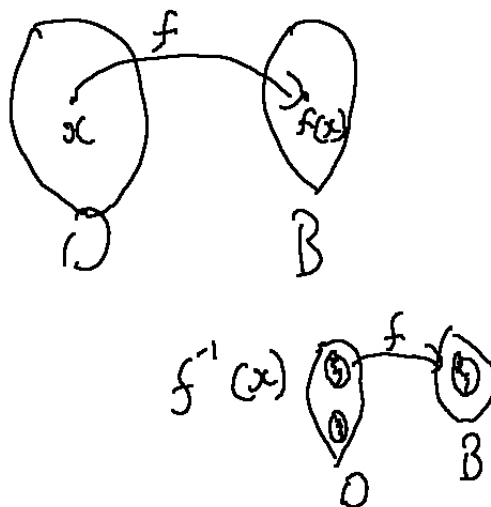
Veranschaulicht man Funktionen auf (endlichen) Mengen D als gerichtete Graphen (Beispiel 1.1.6), so geht von jedem Knoten genau eine Kante ab. Anstelle der Notation $F \subseteq D \times B$, $(x, y) \in F$ schreibt man auch $f : D \rightarrow B, x \mapsto f(x)$ oder $y := f(x)$. Mit einer weiteren nichtleeren Menge C und einer Abbildung $g : B \rightarrow C$ ist die Verknüpfung (Komposition) von g und f definiert als $g \circ f : D \rightarrow C$, $(g \circ f)(x) := g(f(x))$. Im Fall von Abbildungen f, g auf D gilt i.A. $f \circ g \neq g \circ f$. Statt einzelner Punkte $x \in D$ kann man auch Mengen $X \subseteq D$ abbilden: $f(X) := \{y \in B : \text{es gibt ein } x \in X \text{ mit } y = f(x)\}$. $f(X)$ heißt Bild von X unter f . Das Urbild einer Menge $Y \subseteq B$ ist definiert durch $f^{-1}(Y) := \{x \in D : f(x) \in Y\}$. Eine Abbildung $f : D \rightarrow B$ heißt

injektiv $\Leftrightarrow f^{-1}(\{y\})$ enthält für alle $y \in B$ höchstens ein Element

surjektiv $\Leftrightarrow f^{-1}(\{y\})$ enthält für alle $y \in B$ mindestens ein Element.

bijektiv $\Leftrightarrow f^{-1}(\{y\})$ enthält für alle $y \in B$ genau ein Element.

Eine Abbildung $f : D \rightarrow B$ ist genau dann bijektiv, wenn sie injektiv und surjektiv ist.



1.2.3 Beispiel (identische Abbildung)

Die identische Abbildung auf eine Menge $D \neq \emptyset$ ist $id_D : D \rightarrow D, id_D(x) := x$. Sie ist bijektiv.

Beispiel

Die Relation R_0 aus Beispiel 1.1.2 zwischen $X = \{Land\}$ und $Y = \{Stadt\}$ ist eine Funktion $r_0 : X \rightarrow Y$ $r_0(Land) := \text{Hauptstadt vom Land}$. Ihr Bild ist $r_0(X) = \{\text{Hauptstädte}\}$ und die Urbilder lauten:

$$r_0^{-1}(\{s\}) = \begin{cases} \emptyset & \text{falls } s \text{ keine Hauptstadt,} \\ \{l\} & \text{falls } s \text{ Hauptstadt von } l. \end{cases}$$

Folglich ist r_0 injektiv, aber nicht surjektiv. Betrachtet man die Menge aller Hauptstädte als Bildbereich von r_0 , so ist diese Abbildung auch surjektiv.

1.2.4 Beispiel

Die Relation R_1 zwischen \mathbb{R} und $[0, \infty)$ aus Beispiel 1.1.3 ist eine Abbildung und lässt sich schreiben als $r_1 : \mathbb{R} \rightarrow [0, \infty)$, $r_1(x) := |x|$. Für sie gilt $r_1(\mathbb{R}) := [0, \infty)$ und $r_1^{-1}(\{y\}) = \{-y, y\}$ für alle $y \in [0, \infty)$. Also ist $r_1 : \mathbb{R} \rightarrow [0, \infty)$ surjektiv, aber nicht injektiv. Betrachten wir r_1 mit ganz \mathbb{R} als Bildbereich, so gilt $r_1^{-1}(\{y\}) = \emptyset$ für $y < 0$ und dann ist r_1 nicht mehr surjektiv.

1.2.5 Beispiel (ASCII-Code)

Der ASCII-Code zur Codierung alpha-numerischer Zeichen ist gegeben durch eine bijektive Abbildung $f : \{0, 1, \dots, 255 \text{ bzw. } 127\} \rightarrow \{\text{Zeichen}\}$.

Einfache Beispiele (etwa Beispiel 1.2.5) zeigen, dass die Umkehrrelation F^{-1} einer Abbildung $F \subseteq D \times B$ bzw. $f : D \rightarrow B$ nicht unbedingt eine Abbildung ist.

1.2.6 Definition (Umkehrabbildung)

Eine Abbildung $f : D \rightarrow B$ heißt umkehrbar, falls ihre Umkehrrelation F^{-1} wieder eine Abbildung ist. Für letztere schreibt man $f^{-1} : B \rightarrow D$ und nennt sie Umkehrabbildung von f .

1.2.7 Bemerkung

Mit einer umkehrbaren Abbildung $f : D \rightarrow B$ ist auch ihre Umkehrfunktion $f^{-1} : B \rightarrow D$ umkehrbar mit $f^{-1} \circ f = id_D$ und $f \circ f^{-1} = id_B$

1.2.8 Korollar

Eine Abbildung $f : D \rightarrow B$ ist genau dann umkehrbar, wenn f bijektiv ist. Für umgekehrtes f existiert die Umkehrfunktion nur auf $f(D)$

Beweis: Hausaufgabe

1.3 Matrizen

Wir führen kurz die komplexen Zahlen \mathbb{C} ein. Darunter versteht man alle Paare $z = (x, y)$ reeller Zahlen $x, y \in \mathbb{R}$ mit der Addition:

$$z_1 + z_2 = (x_1 + x_2, y_1 + y_2)$$

und der Multiplikation:

$$z_1 \cdot z_2 := z_1 z_2 = (x_1 x_2 - y_1 y_2, x_1 y_2 + x_2 y_1)$$

wobei $z_1 = (x_1, y_1)$, $z_2 = (x_2, y_2)$

Differenz und Quotient ergeben sich zu:

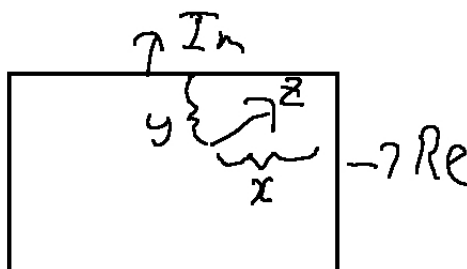
$$z_1 - z_2 = (x_1 - x_2, y_1 - y_2)$$

$$\frac{z_1}{z_2} = \left(\frac{x_1 x_2 + y_1 y_2}{x_2^2 + y_2^2}, \frac{x_2 y_1 - x_1 y_2}{x_2^2 + y_2^2} \right) \text{ falls } x_2^2 + y_2^2 \neq 0$$

Alternative Darstellung:

$$z = (x, y) = x + iy \text{ mit der Konvention } i^2 = -1$$

Wo x das Realteil ($Rez = x$) ist, und y das Imaginärteil ($Imz = y$).



Im Folgenden stehe \mathbb{K} für eine der drei Mengen \mathbb{Q} (rationalen Zahlen), \mathbb{R} (reelle Zahlen) oder \mathbb{C} .

1.3.1 Definition (Matrix)

Eine $m \times m$ -Matrix ist ein rechteckiges Schema von Zahlen $a_{ij} \in \mathbb{K}$ der Form

$$A = (a_{i,j})_{1 \leq i \leq m, 1 \leq j \leq m} = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,m} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,m} \end{pmatrix}$$

Der erste Index $i \in \{1, \dots, m\}$ nummeriert die m Zeilen, der zweite Index $j \in \{1, \dots, m\}$ die m Spalten der Matrix A , das Element $a_{ij} \in \mathbb{K}$ steht daher in der i -ten Zeile und der j -ten Spalte. Für die Menge aller solchen Matrizen schreiben wir $\mathbb{K}^{m \times m}$. Für eine quadratische Matrix A gilt $m = n$ und die $a_{i,i}$ heißen Diagonalelement.

$$A' = \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{m,1} & \cdots & a_{m,n} \end{pmatrix}$$

1.3.2 Beispiel (n Tupeln, m -Spalten)

Ein n -Tupel $x = (x_1, \dots, x_n)$ von Zahlen x_i , aus \mathbb{K} und als $1 \times m$ -Matrix interpretiert. Eine m -Spalte $x = \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}$ wird als $m \times 1$ -Matrixe verstanden, identifizieren $\mathbb{K}^m = k^{m \times 1}$.

1.3.3 Kronecker-Symbol, Einheits- und Nullmatrixe)

Wir definieren das Kronecker-Symbol $S_{i,j} := \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$ und $I_m := (S_{i,j})_{1 \leq i,j \leq m}$ ist die Einheitsmatrixe.

Bei der Nullmatrixe $0 = (0)_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$ sind alle Elemente gleich $0 \in \mathbb{K}$.

1.3.4 Beispiel (Diagonal- und Dreiecksmatrizen)

Man nennt eine quadratische Matrix $A = (a_{i,j})_{1 \leq i,j \leq m}$ diagonal falls $a_{i,j} = 0$ für $i \neq j$. Wir

schreiben dann $A = \begin{pmatrix} a_{1,1} & 0 & \cdot & 0 \\ 0 & a_{2,2} & \cdot & 0 \\ 0 & \cdot & \cdot & a_{n,m} \end{pmatrix} = \text{diag}(a_1, 1, \cdot, a_{m,n})$. Eine obere Dreiecksmatrix ist

quadratisch und erfüllt $a_{i,j} = 0$ für $i > j$, wogegen eine untere Dreiecksmatrix $a_{i,j} = 0$ für $i < j$

erfüllt. Sie sind von der Form: $A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ 0 & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & a_{m,n} \end{pmatrix}$ bzw. $A = \begin{pmatrix} a_{1,1} & 0 & \cdots & 0 \\ a_{2,1} & a_{2,2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{m,n} \end{pmatrix}$.

Mathematische Operationen für Matrizen:

- Skalare Multiplikation: $\mathbb{K} \times \mathbb{K}^{m \times n} \rightarrow \mathbb{K}^{m \times n}, \alpha \cdot A = \alpha A = (\alpha a_{i,j})_{\substack{1 \leq i \leq m \\ i \leq j \leq n}}$. Wir schreiben $-A := (-1) \cdot A$
- Addition: $+: \mathbb{K}^{m \times n} \times \mathbb{K}^{m \times n} \rightarrow \mathbb{K}^{m \times n}, A + B = (a_{i,j} + b_{i,j})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$. Die Subtraktion lautet $A - B = A + (-B)$.
- Genau für $m \times n$ -Matrizen A und $m \times p$ -Matrizen B lässt sich eine Multiplikation erklären. $\cdot: \mathbb{K}^{m \times n} \times \mathbb{K}^{m \times p} \rightarrow \mathbb{K}^{m \times n}$. $A \cdot B = AB := (\sum_{k=1}^m a_{i,k} b_{k,j})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq p}}$. das Produkt ist also eine $m \times n$ -Matrix.

Merke: Das Produkt macht nur Sinn, falls die Spaltenzahl der ersten mit der Zeilenzahl der zweiten Matrix übereinstimmt.

1.3.5 Bemerkung

(1) Um Produkte von Matrizen $A \in \mathbb{K}^{m \times n}$ und $B \in \mathbb{K}^{m \times p}$ zum berechnen ergibt sich das Schema

$$\begin{array}{c|c} B & \\ \hline A & C \end{array} C = (\sum_{k=1}^m a_{i,k} b_{k,j})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq p}}$$

(2) Spezialfall: $A \in \mathbb{K}^{m \times m}, x \in \mathbb{K}^m$ $Ax = \sum_{k=1}^m \begin{pmatrix} a_{1,k} & x_1 \\ \vdots & \vdots \\ a_{m,k} & x_k \end{pmatrix}$.

1.3.6 Beispiel

Das Produkt von $A = \begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix}$ und $B = \begin{pmatrix} 4 & 5 \\ 6 & 7 \end{pmatrix}$ lautet:

$$\begin{array}{c|cc} & 4 & 5 \\ \hline & 6 & 7 \\ \hline 0 & 1 & 0 \cdot 4 + 1 \cdot 6 & 5 \cdot 0 + 1 \cdot 7 \\ 2 & 3 & 2 \cdot 4 + 6 \cdot 3 & 2 \cdot 5 + 7 \cdot 3 \end{array}$$

also $C = AB = \begin{pmatrix} 6 & 7 \\ 26 & 31 \end{pmatrix}$.

Im Umgekehrter Reihenfolge gilt $BA = \begin{pmatrix} 10 & 19 \\ 14 & 27 \end{pmatrix}$. Daher ist das Produkt von Matrizen ist nicht kommutativ $AB \neq BA$.

1.3.7 Beispiel

(1) Für $A \in \mathbb{K}^{m \times n}$ gilt $I_m A = A = A I_n$

(2) Für $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ und $B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ gilt $AB = 0$, womit das Produkt von Matrizen nicht nullteilerfrei ist, d.h. $AB = 0$ kann gelten, ohne dass ein Faktor Null ist.

(3) Das Produkt von $\begin{pmatrix} 0 & 1 & 2 \\ 3 & 4 & 5 \end{pmatrix}$ und $\begin{pmatrix} 6 & 7 \\ 8 & 9 \end{pmatrix}$ ist nicht definiert, $\begin{pmatrix} 6 & 7 \\ 8 & 9 \end{pmatrix} \begin{pmatrix} 0 & 1 & 2 \\ 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 21 & 34 & 47 \\ 27 & 44 & 61 \end{pmatrix}$ dagegen schon.

1.3.8 Beispiel (RGB - Raum)

Im RGB-Farbmodell werden Farben durch Tupel (r, g, b) reeller Zahlen $r, g, b \in \mathbb{R}$ beschreiben: $(1, 0, 0) = \text{rot}$, $(0, 0, 1) = \text{blau}$, $(1, 1, 0) = \text{gelb}$. Alternativ: *YIQ*-Modell (y, i, q) .

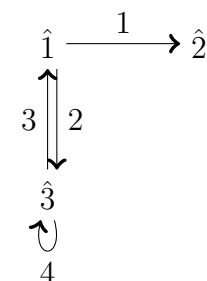
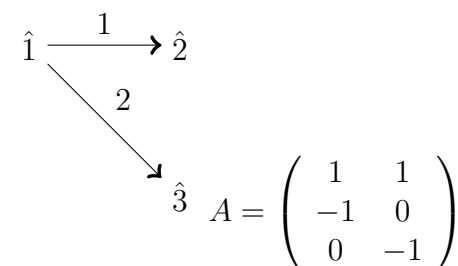
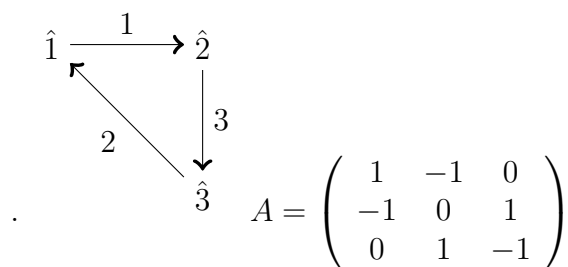
Umrechnung $\begin{pmatrix} y \\ i \\ q \end{pmatrix} = \begin{pmatrix} 0.3 & 0.6 & 0.1 \\ 0.6 & -0.3 & -0.3 \\ 0.2 & -0.5 & 0.3 \end{pmatrix} \begin{pmatrix} r \\ g \\ b \end{pmatrix}$.

1.3.9 Beispiel (Inzidenzmatrix)

Gerichtete Graphen ohne Schleifen (kein Knoten wird durch eine Kante mit sich selbst verbunden, siehe Bemerkung 1.1.6) mit den Knoten $\hat{1}, \dots, \hat{n}$ mit den Knoten $1, \dots, m$ lassen sich durch eine

sogenannte Inzidenzmatrix $A \in \mathbb{K}^{m \times n}$ beschreiben mit

$$a_{i,j} = \begin{cases} 1, & \text{Von Knoten } \hat{1} \text{ geht die Kante } j \text{ aus.} \\ -1, & \text{ein Knoten } \hat{1} \text{ mündet die Kante } j \\ 0, & \text{Knoten } \hat{1} \text{ und Kante } j \text{ berühren sich nicht.} \end{cases}$$



Nicht schleifen frei!

1.3.10 Satz (Rechenregeln für Matrizen)

Für Zahlen $\alpha \in \mathbb{K}$ und Matrizen $A \in \mathbb{K}^{m \times n}$, $B \in \mathbb{K}^{m \times p}$ gelten das Distributiv-Gesetz. $A(B+C) = AB + AC$ für alle $C \in \mathbb{K}^{m \times p}$ und die Assoziativ-Gesetze $(\alpha A)B = A(\alpha B)$, $A(BC) = (AB)C$ für alle $C \in \mathbb{K}^{p \times q}$. Beweis: Übung.

1.4 Lineare Gleichungen

1.4.1 Definition (lineare Gleichung)

Es seien $A \in \mathbb{K}^{m \times n}$ und $b \in \mathbb{K}^m$. Dann bezeichnet man (L_b) $Ax = b$ als lineare Gleichungssystem mit m Gleichungen für die n Unbekannte $x_m \in \mathbb{K}$ oder kurz also lineare Gleichung in \mathbb{K}^n . A heißt Koeffizientenmatrix und b Inhomogenität von (L_b) . Im Fall $b \neq 0$ nennt man (L_b) inhomogen und

erhält andernfalls die homogene Gleichung: $(L_0) Ax = 0$. Eine Lösung von (L_b) ist ein Element $x \in \mathbb{K}^m$ mit $Ax = b$ und $L_b := \{x \in \mathbb{K}^m : Ax = b\}$ steht für die Lösungsmenge von (L_b) .

1.4.2 Bemerkung

(1) Ausgeschrieben lautet (L_b) : $a_{1,1}x_1 + a_{1,2}x_2 + \dots + a_{1,n}x_n = b_1$

$a_{2,1}x_1 + a_{2,2}x_2 + \dots + a_{2,n}x_n = b_2$

...

$a_{m,1}x_1 + a_{m,2}x_2 + \dots + a_{m,n}x_n = b_m$. Oder noch unübersichtlicher $\sum_{j=1}^n a_{i,j}x_j = b_i$ für $1 \leq i \leq m$.

(2) (L_b) hat stets die triviale Lösung $0 \in \mathbb{K}^m$. Inhomogene Gleichungen müssen nicht unbedingt lösbar sein: $0x = 1$.

1.4.3 Satz(Superpositionsprinzip)

Es seien $x, y \in \mathbb{K}^n$ Lösungen von (L_0) . Dann ist auch $\alpha x + \beta y$ eine Lösung von (L_0) , d.h. $\alpha x + \beta y \in L_0$ für alle $\alpha, \beta \in \mathbb{K}$.

Beweis: Übung.

1.4.4 Satz

Ist $\hat{x} \in \mathbb{K}^n$ eine Lösung von (L_b) so gilt $L_b = \hat{x} + L_0$. Hierbei: Für gegebene $x \in \mathbb{K}^n, A \subseteq \mathbb{K}^n$ ist $x + A := \{y \in \mathbb{K}^n : \text{es gibt ein } a \in A \text{ mit } y = x + a\}$

Beweis: Übung. Nun: Explizite Lösung von (L_b) !

Besonders einfach, falls $A \in \mathbb{K}^{m \times n}$ diagonal ist gilt nämlich $a_{i,i} \neq 0, 1 \leq i \leq n$, so besitzt (L_b)

die eindeutige Lösung $x \in \mathbb{K}^n$ mit Elementen $x_i = \frac{b_i}{a_{i,i}}$ für $1 \leq i \leq n$ ist dagegen $a_{i,i} = 0$ für ein

$1 \leq i \leq n$, so besitzt (L_b) unendlich viele Lösungen für $b_i = 0$ und anderenfalls keine Lösung.

Allgemeinere Klasse: Ein $A \in \mathbb{K}^{m \times n}$ ist in Zeilen-Stufen-Form (ZSF) falls in jeder Zeile gilt:

(1) Beginnt sie mit k Nullen, so stehen unter diesen Nullen lediglich weitere Nullen.

(2) Unter dem ersten Element $\neq 0$ stehen nur Nullen.

Bei strenger ZSF muss zusätzlich gelten: (3) Über dem ersten Element $\neq 0$ stehen nur Nullen

1.4.5 Beispiel

(1) Obere Dreiecksmatrizen sind in ZSF, Diagonalmatrizen sogar in strenger ZSF.

(2) Bezeichnet $*$ ein Element $\neq 0$, so gilt:

$$\bullet \begin{pmatrix} * & * & * \\ * & * & * \\ 0 & 0 & * \end{pmatrix}, \begin{pmatrix} 0 & * & * \\ 0 & * & * \\ 0 & * & * \end{pmatrix}, \begin{pmatrix} * & 0 & 0 \\ * & * & 0 \\ * & * & * \end{pmatrix} \text{ sind nicht in ZSF.}$$

- $\begin{pmatrix} * & * & * & * \\ 0 & * & * & * \\ 0 & 0 & 0 & * \end{pmatrix}$ ist in ZSF (aber nicht strenger ZSF).
- $\begin{pmatrix} * & * & 0 & 0 \\ 0 & 0 & * & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$ ist in strenger ZSF

1.4.6 Beispiel (Rückwärts-Substitution)

Die inhomogene lineare Gleichung (1.4b) $\begin{cases} x_1 + 2x_2 + 3x_3 + 4x_4 = 1, \\ x_2 + 2x_3 + 3x_4 = 1, \\ x_3 + 2x_4 = 1 \end{cases}$ hat die Koeffizientenmatrix bzw. Inhomogenität $A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 2 \end{pmatrix}, b = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$

Rückwärtssubstitution: Aus der letzten Gleichung $x_3 + 2x_4 = 1$ sieht man, dass $x_4 = t$ frei gewählt werden kann, $t \in \mathbb{K}$. Dies liefert $x_3 = 1 - 2t$. Die bekannten Variablen x_3, x_4 können in die zweite Gleichung von (1.4b) eingesetzt werden, also $x_2 = 1 - 2x_3 - 3x_4 = t - 1$ und analog liefert die erste Gleichung $x_1 = 1 - 2x_2 - 3x_3 - 4x_4 = 0$. Die Lösungsmenge von (1.4b) ist also:

$$L_b = \left\{ \begin{pmatrix} 0 \\ t-1 \\ 1-2t \\ t \end{pmatrix} \in \mathbb{K}^4 : t \in \mathbb{K} \right\} = \begin{pmatrix} 0 \\ -1 \\ 1 \\ 0 \end{pmatrix} + \mathbb{K} \begin{pmatrix} 0 \\ 1 \\ -2 \\ 1 \end{pmatrix}$$

Die Lösungsmenge L_b von (1.4b) ändert sich nicht, wenn folgende Operationen auf (1.4b) angewandt werden:

- Vertauschen von Gleichungen
- Multiplikation von Gleichungen mit $\alpha \in \mathbb{K} \setminus \{0\}$
- Addition des α -fachen der k -ten Gleichung zur j -ten.
Diese sind elementare Zeilentransformationen.

ZIEL: Transformiere A bzw. (L_b) auf ZSF mittels elementare Zeilentransformationen. Systematisch: Gauß Algorithmus.

Zu seiner Beschreibung gehen wir davon aus, dass die erste Spalte von A von 0 verschieden ist (anderenfalls sind x_1, \dots, x_n umzunummerieren). Ohne Sonderfälle zu berücksichtigen gilt:

1. Ordne die Gleichungen in (1.4a) so an, dass $a_m \neq 0$. In der gängigen Notation schreibt man

$$\text{nun (1.4b) als } \begin{array}{cccc|c} a_{1,1} & a_{1,2} & \cdots & a_{1,n} & b_1 \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m,1} & a_{m,2} & \cdots & a_{m,n} & b_m \end{array}$$

2. Subtrahiere von der i -ten Gleichung, $2 \leq i \leq m$ in (1.4a) das $\frac{a_{i,1}}{a_{1,1}}$ -fache der ersten Gleichung:

$$\begin{array}{cccc|c} a_{1,1} & a_{1,2} & \cdots & a_{1,n} & b_1 \\ 0 & a_{2,2}^{(1)} & \cdots & a_{2,n}^{(1)} & b_2^{(1)} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & a_{m,2}^{(2)} & \cdots & a_{m,n}^{(1)} & b_m^{(1)} \end{array} \quad \begin{cases} a_{1,1}x_1 + \cdots + a_{1,n}x_n = b_1 \\ A^{(1)}x^{(1)} = b^{(1)} \end{cases}$$

mit $A^{(1)} \in \mathbb{K}^{(m-1) \times (n-1)}$, $b \in \mathbb{K}^{m-1}$.

3. Transformiere $A^{(1)}x^{(1)} = b^{(1)}$ entsprechend und fahre sukzessive fort, bis (idealerweise) eine Dreiecks- oder ZSF entstanden ist.
4. Löse das resultierende System durch Rückwärts-Substitution.

1.4.7 Beispiel

Als Kurzschreibweise für

$$(1.4d) \quad \begin{cases} x_1 + 2x_2 + 3x_3 = 0 \\ 4x_1 + 5x_2 + 6x_3 = 0 \\ 7x_1 + 8x_2 + 9x_3 = 0 \end{cases}$$

$$\begin{array}{ccc|c} 1 & 2 & 3 & 0 \\ 4 & 5 & 6 & 0 \\ 7 & 8 & 9 & 0 \end{array} \begin{array}{l} \\ II - 4I \\ II - 7I \end{array} \Leftrightarrow \begin{array}{ccc|c} 1 & 2 & 3 & 0 \\ 0 & -3 & -6 & 0 \\ 0 & -6 & -12 & 0 \end{array} \begin{array}{l} \\ (-\frac{1}{3}) \\ III - 2II \end{array} \Leftrightarrow \begin{array}{ccc|c} 1 & 2 & 3 & 0 \\ 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 \end{array}$$

Damit ist (1.4d) äquivalent zu $\begin{cases} x_1 + 2x_2 + 3x_3 = 0 \\ x_2 + 2x_3 = 0 \end{cases}$

Rückwärts-Substitution: Wähle $x_3 = t$ mit $t \in \mathbb{K}$ und es folgt $x_2 = -2x_3 = -2t$, $x_1 = -2x_2 + 3x_3 = t$. Die Lösungsmenge von (1.4d) ergibt sich zu:

$$L_0 = \left\{ \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix} \in \mathbb{K}^3 : t \in \mathbb{K} \right\} = \mathbb{K} \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix}$$

1.4.8 Satz

Hat (L_0) weniger Gleichungen als Unbekannte, dass heißt $m < n$, so besitzt sie unendlich viele Lösungen. Beweis:

- I. Man zeigt (*) (L_0) hat eine nichttriviale Lösung.
- II. Da (L_0) nach Schritt (I) eine Lösung $x \neq 0$ besitzt ist nach dem Superpositionsprinzip aus Satz 1.4.3 auch jeder $tx, t \in \mathbb{K}$, eine Lösung \neq .

1.4.9 Satz

Besitzt (L_b) genauso viele Gleichungen wie Unbekannte, d.h. $m = n$, so gilt:

- (a) Ist $L_0 = \{0\}$, so besitzt (L_b) genau eine Lösung.
- (b) Besitzt (L_0) eine nichttriviale Lösung, so existieren entweder keine oder unendlich viele verschiedene Lösungen von (L_b)

Beweis:

- (a) Wie gehen mittels vollständiger Induktion vor.
Für $n = 1$ gilt die Behauptung offenbar. Im Induktionsschritt gelte (a) für $n - 1$. Da (L_0) nur die triviale Lösung hat gilt $A \neq 0$. Durch Umm nummerieren erreichen wir $a_{1,1} \neq 0$. Dann wird zur i -ten Gleichung, $2 \leq i$, in (1.4a) das $-\frac{a_{i,1}}{a_{1,1}}$ -fache der ersten Gleichung addiert:

$$(1.4f) \quad \begin{cases} a_{1,1}x_1 + \cdots + a_{1,n}x_n = b_1 \\ A^* = \begin{bmatrix} x_2 \\ \vdots \\ x_n \end{bmatrix} = b^* \end{cases} \quad \text{mit } A^* \in \mathbb{K}^{(n-1) \times (n-1)}, b^* \in \mathbb{K}^{n-1}$$

Beweis:

Wir wissen:

- (a) Die homogene Gleichung $A^*x^* = 0$ hat nur die triviale Lösung, denn sonst hätte (L_0) eine nicht triviale Lösung. Das Teilsystem $A^*x^* = b^*$ besitzt nach Induktionsannahme genau eine Lösung x^* mit Elementen x_2, \dots, x_n . Durch Einsetzen in die erste Gleichung in (1.4f) folgt ein eindeutiger Wert x_1 und die Lösung von (L_b) in eindeutiger Weise.
- (b) Es sei \hat{x} eine Lösung von (L_b) und x eine nichttriviale Lösung von (L_0) . Dann liefern die Sätze 1.4.3 und 1.4.4, dass $\hat{x} + \alpha x$ die Gleichung löst für jedes $\alpha \in \mathbb{K}$. In diesem Fall hat (L_b) unendlich viele Lösungen. Die einzige verbleibende Möglichkeit ist, dass (L_b) keine Lösung besitzt.

2 Lineare Räume

2.1 Algebraische Strukturen

Bezeichnet $M \neq \emptyset$ eine Menge und $F(M)$ die Menge aller Selbstabbildungen auf M , so kann die Komposition \circ als Abbildung $\circ : F(M) \times F(M) \rightarrow F(M)$ interpretiert werden - man spricht von einer Verknüpfung.

2.1.1 Definition (Gruppe)

Eine Gruppe (G, \cdot) ist eine nichtleere Menge G mit einer Verknüpfung $\cdot : G \times G \rightarrow G$ mit den Eigenschaften: (G_1) \cdot ist Assoziativ, d.h. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ für $a, b, c \in G$
 (G_2) es existiert ein neutrales Element $e \in G$ mit $a \cdot e = a = e \cdot a$ für $a \in G$
 (G_3) zu jedem $a \in G$ existiert ein inverses Element $a^{-1} \in G$ mit $a \cdot a^{-1} = a^{-1} \cdot a = e$ für $a \in G$
 Bei einer kommutativen oder Abel'scher Gruppe gilt ferner $(G_4) a \cdot b = b \cdot a$ für alle $a, b \in G$. Für eine Halbgruppe müssen nur (G_1) und (G_2) gelten.

2.1.2 Bemerkung

- (1) Das neutrale Element $e \in G$ ist eindeutig: In der Tat, bezeichnen $e_1, e_2 \in G$ zwei neutrale Elemente, so folgt nach (G_2) ist: $e_2 = e_1 \cdot e_2$ und $e_1 \cdot e_2 = e_1$, also $e_1 = e_2$
- (2) Zu gegebenem $a \in G$ ist auch das inverse Element $a^{-1} \in G$ eindeutig. Für inverse Element a_1^{-1}, a_2^{-1} von a gilt nämlich

$$a_1^{-1} \stackrel{(G_2)}{=} a_1^{-1} \cdot e \stackrel{(G_3)}{=} a_1^{-1} \cdot (a \cdot a_2^{-1}) \stackrel{(G_1)}{=} (a_1^{-1} \cdot a) \cdot a_2^{-1} \stackrel{(G_3)}{=} e \cdot a_2^{-1} \stackrel{(G_2)}{=} a_2^{-1}$$

- (3) Entsprechend $e = e^{-1}$, $a = (a^{-1})^{-1}$

2.1.3 Bemerkung (Potenzen)

Die Potenzen $a^n \in G$ eines $a \in G$ (G ist eine multiplikative Halbgruppe) sind rekursiv erklärt durch $a^0 := e$, $a^{n+1} := a \cdot a^n$ für alle $n \in \mathbb{N}_0$. In einer Gruppe setzen wir $a^n := (a^{-n})^{-1}$ für $n < 0$.

2.1.4 Beispiel

- (1) $(\mathbb{Z}, +)$ ist eine kommutative additive Gruppe mit neutralen Element 0 und dem zu $a \in \mathbb{Z}$ inverses Element $-a$. Dagegen ist (\mathbb{Z}, \cdot) keine Gruppe, denn das multiplikative Inverses lässt sich innerhalb von \mathbb{Z} nicht erklären. Ebenso ist $(\mathbb{N}, +)$ keine (additive) Gruppe.
- (2) Es sei $\mathbb{K} \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$. Dann ist $(\mathbb{K}, +)$ eine kommutative additive Gruppe mit neutralem Element 0 und $-a$ als zu a Inversen. Auch $(\mathbb{K} \setminus \{0\}, \cdot)$ ist eine kommutative multiplikative Gruppe mit neutralem Element 1 und dem zu a inversen Element $\frac{1}{a}$.

- (3) Mit $\mathbb{K} \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{C}\}$ bilden die Matrizen $(\mathbb{K}^{m \times n}, +)$ eine kommutative additive Gruppe mit neutralem Element 0 und den Inversen $-A$ zu A . Die quadratischen reellen rationalen oder komplexen Matrizen $(\mathbb{K}^{m \times n} \setminus \{0\}, \cdot)$ bilden keine Gruppe, da etwa $\text{diag}(1, 0) \neq 0$ kein Inverses besitzt.

2.1.6 Beispiel (modulo)

Es sei $p \geq 2$ eine ganze Zahl und $\mathbb{Z}_p := \{0, \dots, p-1\}$. Für beliebige $a, b \in \mathbb{Z}$ gibt es vermöge der Division mit Rest eindeutige $m \in \mathbb{Z}$ und $k \in \mathbb{Z}_p$ mit $a + b = mp + k$ wir schreiben dann $k = a + b \bmod p$ oder $k =: a +_p b$. Dann ist $(\mathbb{Z}_p, +_p)$ eine kommutative Gruppe mit dem neutralem Element 0.

2.1.7 Beispiel (symmetrische Gruppe)

Es sei M eine nichtleere Menge und $S(M)$ bezeichnet alle bijektiven Selbstabbildungen $f : M \rightarrow M$. Dann ist die symmetrischen Gruppe $(S(M), \circ)$ eine i.A. nicht-kommutative Gruppe mit id_M als neutralem Element und $f^{-1} : M \rightarrow M$ als inversen Element zu f . Im Fall $M = \{1, \dots, n\}$ schreiben wir $S_n := S(\{1, \dots, n\})$. Die Menge aller nicht-notwendig bijektiven Selbstabbildungen $F(M)$ ist dagegen eine Halbgruppe bezüglich \circ .

2.1.8 Korollar (Rechnen in Gruppen)

Für alle $a, b, c \in \mathbb{G}$ gilt $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$, wie auch $a \cdot b = a \cdot c \Rightarrow b = c, a \cdot b = e \Rightarrow a = b^{-1}$.

Beweis:

Es seien $a, b, c \in \mathbb{G}$. Wir zeigen zunächst, dass $b^{-1} \cdot a^{-1}$ das inverse Element von $a \cdot b$ ist. Dazu

$$(b^{-1} \cdot a^{-1}) \cdot (a \cdot b) \stackrel{(G_1)}{=} b^{-1} \cdot (a^{-1} \cdot (a \cdot b)) \stackrel{(G_1)}{=} b^{-1} \cdot ((a^{-1} \cdot a) \cdot b) \stackrel{(G_3)}{=} b^{-1} \cdot (e \cdot b) \stackrel{(G_2)}{=} b^{-1} \cdot b \stackrel{(G_3)}{=} e$$

und entsprechend $(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = e$. Die erste Implikation ergibt sich nach Voraussetzung durch

$$b \stackrel{(G_2)}{=} e \cdot b \stackrel{(G_3)}{=} (a^{-1} \cdot a) \cdot b \stackrel{(G_1)}{=} a^{-1} \cdot (a \cdot b) = a^{-1} \cdot (a \cdot c) \stackrel{(G_1)}{=} (a^{-1} \cdot a) \cdot c \stackrel{(G_3)}{=} e \cdot c \stackrel{(G_2)}{=} c$$

Die verbleibende Implikation sei den Leser überlassen.

2.1.9 Definition (Körper)

Ein Körper $(\mathbb{K}, +, \cdot)$ ist eine Menge \mathbb{K} mit mindestens zwei Elementen versehen. Mit den arithmetischen Operationen $+$: $\mathbb{K} \times \mathbb{K} \rightarrow \mathbb{K}$ (Addition) und \cdot : $\mathbb{K} \times \mathbb{K} \rightarrow \mathbb{K}$ (Multiplikation).

$(\mathbb{K}_1)(\mathbb{K}, +)$ ist eine kommutative Gruppe mit neutralem Element 0 und den zu $\alpha \in \mathbb{K}$ inversen

Element $-\alpha$, d.h. für alle $\alpha, \beta, \gamma \in \mathbb{K}$ gilt:

$$\begin{aligned}(\mathbb{K}_1^1)\alpha + (\beta + \gamma) &= (\alpha + \beta) + \gamma \\(\mathbb{K}_1^2)\alpha + 0 &= 0 + \alpha = \alpha \\(\mathbb{K}_1^3)\alpha \cdot -\alpha &= -\alpha \cdot \alpha = 0 \\(\mathbb{K}_1^4)\alpha + \beta &= \beta + \alpha\end{aligned}$$

(\mathbb{K}_2) $(\mathbb{K}, \{0\}, \cdot)$ ist eine kommutative Gruppe mit neutralem Element 1 und zu $\alpha \in \mathbb{K}$ Inversem $\frac{1}{\alpha}$, d.h. es gilt für $\alpha, \beta, \gamma \in \mathbb{K}$ $\{0\}$.

$$\begin{aligned}(\mathbb{K}_2^1)\alpha \cdot (\beta \cdot \gamma) &= (\alpha \cdot \beta) \cdot \gamma \\(\mathbb{K}_2^2)\alpha \cdot 1 &= 1 \cdot \alpha = \alpha \\(\mathbb{K}_2^3)\alpha \cdot \frac{1}{\alpha} &= \frac{1}{\alpha} \cdot \alpha = 1 \\(\mathbb{K}_2^4)\alpha \cdot \beta &= \beta \cdot \alpha\end{aligned}$$

(\mathbb{K}_3) es gelten die Distributivgesetze $\alpha(\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$, $(\alpha + \beta) \cdot \gamma = \alpha \gamma + \beta \gamma$ für alle $\alpha, \beta, \gamma \in \mathbb{K}$. Üblich $\alpha\beta := \alpha \cdot \gamma$. Subtraktion als $\alpha - \beta := \alpha + (-\beta)$. Division $\frac{\alpha}{\beta} := \alpha \cdot \frac{1}{\beta}$.

2.1.10 Beispiel

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind Körper bzgl. $+, \cdot$

2.1.11 Beispiel (Restklassenkörper modulo p)

Mit einer gegebenen Primzahl $p \in \mathbb{N}$ definieren wir die Mengen $\mathbb{Z}_p := \{0, \dots, p\}$. Dann gibt für beliebige $\alpha, \beta \in \mathbb{Z}_p$ eindeutige Zahlen $m, n \in \mathbb{Z}$ und $k, l \in \mathbb{Z}_p$ derart, dass

$$\alpha + \beta = m \cdot p + k$$

$$\alpha \cdot \beta = np + l \text{ Division mit Rest.}$$

$$\text{Addition: } \alpha +_p \beta := k$$

$$\text{Multiplikation: } \alpha \cdot_p \beta := l$$

$(\mathbb{Z}_p, +_p, \cdot_p)$ ist Körper, der sogenannten Restklassenkörper modulo p .

$$\mathbb{Z}_2 : \begin{array}{c|cc} +_2 & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array}$$

	\cdot_2	0	1	
		0	0	
		1	0	
	$+_3$	0	1	2
$\mathbb{Z}_3 :$	0	0	1	2
	1	1	2	0
	2	2	0	1
	\cdot_3	0	1	2
		0	0	0
		1	0	1
		2	0	2

2.1.12 Korollar

Ist $(\mathbb{K}, +, \cdot)$ ein Körper, so gilt für alle $\alpha, \beta, \gamma \in \mathbb{K}$, dass

$$\begin{aligned} 0 \cdot \alpha &= \alpha \cdot 0 = 0, & \beta \cdot (-\alpha) &= -(\beta \cdot \alpha) = (-\beta) \cdot \alpha \quad (2.1b) \\ (-1) \cdot \alpha &= -\alpha, & (-\alpha) \cdot (-\beta) &= \alpha \cdot \beta \quad (2.1c) \end{aligned}$$

Und ferner die Implikation $\alpha \cdot \beta = 0 \rightarrow \alpha = 0$ oder $\beta = 0$.

2.1.13 Bemerkung

Es gilt $1 \neq 0$, da die Annahme $1 = 0$ folgenden Widerspruch impliziert: Da \mathbb{K} mindestens 2 Elemente enthält, gibt es ein $\alpha \in \mathbb{K}, \alpha \neq 0$ mit:

$$\alpha \stackrel{(\mathbb{K}_2^2)}{=} \alpha \cdot 1 = \alpha \cdot 0 \stackrel{(2.1b)}{=} 0$$

Daher ist der Restklassenkörper modulo 2 \mathbb{Z}_2 der kleinste Körper.

2.1.14 Beweis

Wähle ein $\alpha, \beta, \gamma \in \mathbb{K}$. Es gilt $0 \cdot \alpha \stackrel{(\mathbb{K}_1^2)}{=} (0 + 0) \cdot \alpha \stackrel{(\mathbb{K})}{=} 0\alpha + 0\alpha$ mittels Korollar 2.1.8 ($+, a = b = 0$ und $c = 0$) folgt $0 \cdot \alpha = 0$, kommutativ liefert $\alpha 0 = 0$. Aus dieser Behauptung resultiert

$$(-\beta)\alpha + \beta\alpha \stackrel{(\mathbb{K}_3)}{=} (-\beta + \beta)\alpha = 0 \cdot \alpha = 0$$

mit Korollar 2.1.8 ($+, a = (-\beta)\alpha, b = \beta\alpha$). Dies liefert $-(\beta\alpha) = (-\beta)\alpha$ und $\beta(-\alpha) = -(\beta\alpha)$. Die Beziehung $(-1)\alpha = -\alpha$ resultiert aus dem eben gezeigten $\beta = 1$ und

$$(-1)\alpha = 1 \cdot (-\alpha) \stackrel{\mathbb{K}_2^2)}{=} -\alpha.$$

2.1c ergibt sich mit Bemerkung 2.1.2(3) aus

$$(-\alpha)(-\beta) \stackrel{2.1b)}{=} -(\alpha(-\beta)) \stackrel{2.1b)}{=} -(-(\alpha\beta)) = \alpha\beta = 0$$

Annahme: $\alpha \neq 0$ und $\beta \neq 0$ dann $1 \stackrel{\mathbb{K}_2^3)}{=} \frac{1}{\beta} \cdot \frac{1}{\alpha} \cdot \alpha \cdot \beta \stackrel{2.1b)}{=} 0$

2.2 Vektorräume

2.2.1 Definition (linearer Raum, Vektorraum)

Es sei \mathbb{K} ein Körper. Ein Vektorraum oder linearer Raum $(X, +, \cdot)$ (über \mathbb{K}) ist eine nichtleere Menge X mit arithmetische Operationen:

- (1) Addition $+: X \times X \rightarrow X$ derart, dass $(X, +)$ eine kommutative Gruppe mit neutralem Element 0 oder Nullvektor.
- (2) Skalare Multiplikation $\cdot: \mathbb{K} \times X \rightarrow X$ derart, dass für alle $\alpha, \beta \in \mathbb{K}$ und $x, y \in X$ gilt:

$$(V_1) \alpha(x + y) = \alpha x + \alpha y \text{ Distributiv Gesetz}$$

$$(V_2) (\alpha + \beta) \cdot x = \alpha x + \beta x \text{ Distributiv Gesetz}$$

$$(V_3) (\alpha\beta) \cdot x = \alpha \cdot (\beta \cdot x) \text{ Assoziativ Gesetz}$$

$$(V_4) 1 \cdot x = x$$

Die Elemente aus \mathbb{K} heißen Skalare und X heißen Vektoren.

Konventionen: $\alpha x := \alpha \cdot x$ $x - y := x + (-y)$

2.2.2 Beispiel

Es sei $(\mathbb{K}, +, \cdot)$ ein Körper.

(0) Der triviale Raum $\{0\}$ der nur die 0 enthält.

(1) Weiter ist \mathbb{K} ein Vektorraum über sich selbst.

(2) Die Menge aller $m \times n$ -Matrizen $\mathbb{K}^{m \times n}$ ist ein linearer Raum über \mathbb{K} bezüglich

$$(1.3b) \alpha A := \alpha A = (\alpha a_{i,j})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$$

$$(1.3c) A + B := (\alpha_{i,j} + \beta_{i,j})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$$

Ein n -Tupel $(x_1, \dots, x_n) \in \mathbb{K}^{1 \times n}$ bezeichnen wir als Zeilenvektor und eine m -Spalte (1.3a) als Spaltenvektor.

2.2.3 Beispiel

Es sei $p \in \mathbb{N}$ eine Primzahl und $n \in \mathbb{N}$. Dann sind die n -Spalten \mathbb{Z}_p^n in \mathbb{Z}_p mit den komponentenweisen Addition $+_p$ und skalaren Multiplikation \cdot_p ein linearer Raum über \mathbb{Z}_p . Insbesondere für \mathbb{Z}_2^2

$+_2$	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 1 \\ 1 \end{pmatrix}$
$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 1 \\ 1 \end{pmatrix}$
$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 1 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$
$\begin{pmatrix} 0 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 1 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$
$\begin{pmatrix} 1 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 1 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 1 \end{pmatrix}$
\cdot_2	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 1 \\ 1 \end{pmatrix}$
0	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$
1	$\begin{pmatrix} 0 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 0 \\ 1 \end{pmatrix}$	$\begin{pmatrix} 1 \\ 1 \end{pmatrix}$

2.2.4 Beispiel (Lösungsmengen)

Mit Satz 1.4.3 ist L_0 einer homogenen Gleichung ein Vektorraum über \mathbb{K} . Die Lösungsmenge L_b inhomogener Systeme ist kein linearer Raum über \mathbb{K} .

2.2.5 Beispiel (Funktionsräume)

Es sei $\omega \neq \emptyset$ und X ein linearer Raum über \mathbb{K} . Dann ist $F(\omega, X) := \{u : \omega \rightarrow X\}$ ein Vektorraum über \mathbb{K} mit punktweise definierten arithmetischen Operationen $(a+v)(t) := u(t)+v(t)$, $(\alpha u)(t) := \alpha u(t)$ für alle $t \in \omega, \alpha \in \mathbb{K}$.

Die Menge $F(\omega, X)$ wird als Funktionenraum bezeichnet. $\omega \in \mathbb{N}$, $\omega \in \mathbb{Z}$, dann bezeichnen wir $F(\omega, X)$ als Folgenraum.

2.2.6 Korollar

Ist $(X, +, \cdot)$ ein linearer Raum über \mathbb{K} so gilt für alle Skalare $\alpha, \beta \in \mathbb{K}$ und Vektoren $x, y \in X$:

$$(a) 0_{\mathbb{K}} \cdot x = \alpha \cdot 0_x = 0_x$$

$$(b) \text{ Falls } \alpha x = 0_x, \text{ so folgt } \alpha = 0 \in \mathbb{K} \text{ oder } x = 0 \in X$$

$$(c) (-\alpha)x = \alpha(-x) = -(\alpha x)$$

$$(d) \alpha(x - y) = \alpha x - \alpha y \text{ und } (\alpha - \beta)x = \alpha x - \beta x$$

Beweis: Es sei $\alpha \in \mathbb{K}$ und $x \in X$:

- (a) Es gilt $0_{\mathbb{K}}x = (0_{\mathbb{K}} + 0_{\mathbb{K}})x = 0_{\mathbb{K}}x + 0_{\mathbb{K}}x$ wegen V_2 . Nach Definition 2.2.1 (a) existiert zum Vektor $z := 0_{\mathbb{K}}x$ ein Vektor $-z$ mit $0 \cdot x + (-z) = 0_X$ und wir erhalten $0_X = 0 \cdot x + (-z) = (0 \cdot x + 0 \cdot x) + (-z) = 0 \cdot x + (0 \cdot x + (-z)) = 0 \cdot x + 0_x = 0 + x$ und die Beziehung $\alpha \cdot 0 = 0$ folge analog.