Lineare Algebra

Lucas Westermann

5. Juni 2011

Inhaltsverzeichnis

Literatur

Mathematik für Informatiker: Teschl, Hackenberger
Lineare Algebra: Beutelspacher, Fischer, Lang (auf Englisch), Stammbach.

1 Grundlegendes

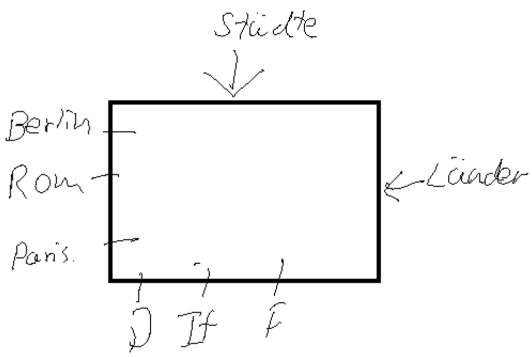
1.1 Mengen

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: $R_1^{-1} = \{(y, x) \in Y \in X : (x, y) \in R\}$ heißt Umkehrrelation.

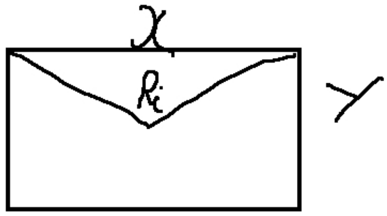
1.1.2 Beispiel

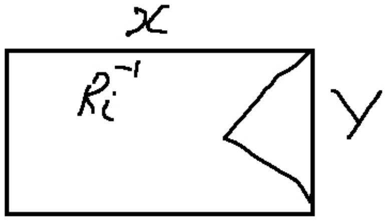
Die Menge $R_0 = \{(x, y) \in X \in Y : y$ ist Hauptstadt von x ist eine Relation zwischen der Menge X aller Länder und Y aller Städte.



1.1.3 Beispiel

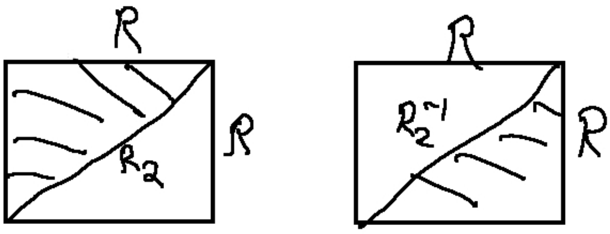
Mit den Mengen $X = \mathbb{R}$ $Y = [0, \infty)$ ist $R_1 = \{(x, |x|) \in X \times Y, X \in X\}$ ist eine Relation mit der Umkehrrelation $R^{-1} = \{(|x|, x) : x \in X\}$.





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 $R_2^{-1} = (y, x) : x \leq y$

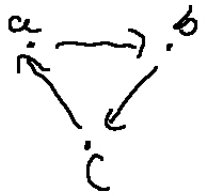


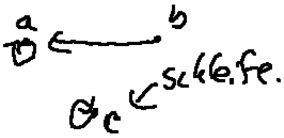
1.1.5 Beispiel

Die Menge $R_3 = \{(x, y) \in C \times C : x$ und y 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. $X = \{a, b, c\}$ $R = \{(a, b), (b, c), (c, d)\}$.





$X = \{a, b, c\}$ $R = \{(b, a), (a, a), (c, c)\}$.
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 $[x]$.

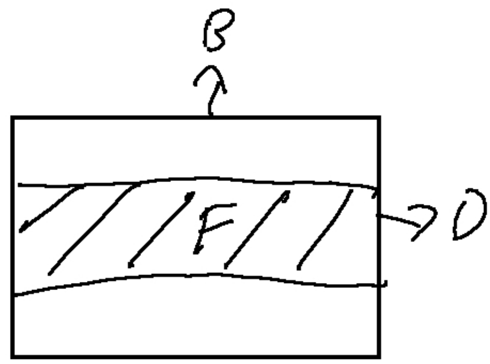
1.1.10 Beispiel

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

$F \subseteq D \times B$.

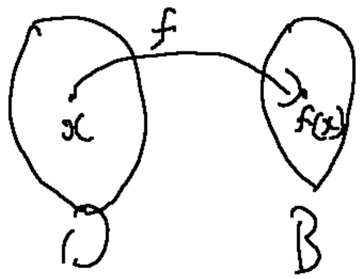


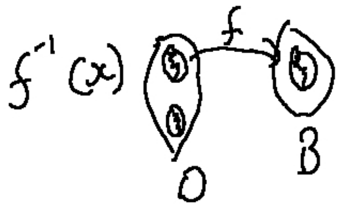
1.2.1 Definition (Abbildungen, Funktion)

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 $f : D \to B, x \mapsto f(x)$ oder $y := f(x)$ Mit einer weiteren nichtleeren Menge C und einer Abbildung $g : B \to C$ ist die Verknüpfung (Komposition) von g und f definiert als $g \circ f : D \to C, (g \circ f)(x) := g(f(x))$. 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: $f(X) := \{y \in B :$ es gibt ein $x \in X$ 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 $f : D \to B$ 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 $f : D \to B$ 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 $id_D : D \to D, id_D(x) := x$. Sie ist bijektiv.

Beispiel

Die Relation R_0 aus Beispiel 1.1.2 zwischen $X = \{Land\}$ und $Y = \{Stadt\}$ ist eine Funktion $r_o : X \to Y$ $r_0(Land)$:= 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 Haupstädte 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 $r_1 : \mathbb{R} \to [0, \infty)$, $r_1(x) := |x|$ Für sie gilt $r_1(\mathbb{R}) := [0, \infty)$ und $r_1^{-1}(\{y\}) = \{-y, y\}$ für alle $y \in [0, \infty)$. Also ist $r_1 : \mathbb{R} \to [0, \infty)$ 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 $f : \{0, 1, \cdots, 255 \text{ bzw. } 127\} \to \{\text{Zeichen}\}$.
Einfache Beispiele (etwa Beispiel 1.2.5) zeigen, dass die Umkehrrelation F^{-1} einer Abbildung $F \subseteq D \times B$ bzw. $f : D \to B$ nicht unbedingt eine Abbildung ist.

1.2.6 Definition (Umkehrabbildung)

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

1.2.7 Bemerkung

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

1.2.8 Korollar

Eine Abbildung $f : D \to B$ 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:

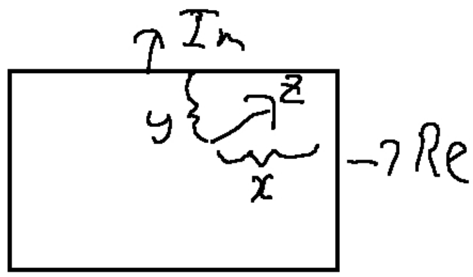
$$z_1 - z_2 = (x_1 - x_2, y_1 - y_2)$$

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

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 $m \times m$-Matrixe 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 $i \in \{1, \cdots, m\}$ nummeriert die m Zeilen, der zweite Index $j \in \{1, \cdots, m\}$ 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 $x = (x_1, \cdots, x_n)$ von Zahlen X, 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 $0 \in \mathbb{N}$.

1.3.4 Beispiel (Diagonal- und Dreieckmatrizen)

Man nennt eine quadratische Matrix $A = (a_{i,j})_{1 \leq i,j \leq n}$ diagonal falls $a_{i,j} = 0$ für $i \neq j$. Wir schreiben dann $A = \begin{pmatrix} a_{1,1} & 0 & \cdot & 0 \\ 0 & a_{2,2} & \cdot & 0 \\ 0 & \cdot & \cdot & a_{n,n} \end{pmatrix} = \mathrm{diag}(a_1, 1, \cdot, a_{n,n})$. 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: $A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ 0 & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & a_{n,n} \end{pmatrix}$ bzw. $A = \begin{pmatrix} a_{1,1} & 0 & \cdots & 0 \\ a_{2,1} & a_{2,2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{pmatrix}$.

Mathematische Operationen für Matrizen:

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

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

(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:

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

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 $I_m A = A = A I_m$

(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 <u>nullteilerfrei</u> 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: $(1, 0, 0) =$ rot, $(0, 0, 1)$ blau, $(1, 1, 0)$ 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 (Inzedenzmatrix)

Gerichtete Graphen ohne Schleifen (kein Knoten wird durch eine Kante mit sich selbst verbunden, siehe Bemerkung 1.1.6) mit den Knoten $\hat{1}, \cdots, \hat{m}$ mit den Knoten $1, \cdots, m$ lassen sich durch eine sogenannte Inzedenzmatrix $A \in \mathbb{K}^{m \times n}$ beschreiben mit

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

$$\begin{tikzcd} \hat{1} \arrow[r, "1"] & \hat{2} \arrow[d, "3"] \\ & \hat{3} \arrow[ul, "2"] \end{tikzcd}$$

. $A = \begin{pmatrix} 1 & -1 & 0 \\ -1 & 0 & 1 \\ 0 & 1 & -1 \end{pmatrix}$

$$\begin{tikzcd} \hat{1} \arrow[r, "1"] \arrow[dr, "2"] & \hat{2} \\ & \hat{3} \end{tikzcd}$$

$A = \begin{pmatrix} 1 & 1 \\ -1 & 0 \\ 0 & -1 \end{pmatrix}$

$$\begin{tikzcd} \hat{1} \arrow[r, "1"] \arrow[d, shift left, "2"] & \hat{2} \\ \hat{3} \arrow[u, shift left, "3"] \arrow[loop below, "4"] \end{tikzcd}$$

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 $\mathbb{K}^m$. 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): $a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n = b_1$
$a2, 1x_1 + a_{2,2}x_2 + \cdots + a_{2,n}x_n = b_2$
$\cdots$
$am, 1x_1 + a_{m,2}x_2 + \cdots + a_{m,n}x_n = b_m$. Oder noch unübersichtlicher $\sum_{j=1}^{n} a_{i,j}x_j = b_i$ für $1 \leq i \leq m$.
(2) (L_b) hat stehts die triviale Lösung $0 \in \mathbb{K}^m$. Inhomogene Gleichungen müssen nicht unbedingt lesbar 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 $X_1 = \dfrac{b_i}{a_{i,i}}$ für $1 \leq 1 \leq n$ ist dagegen $d_{i,i} = 0$ 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:

- $\begin{pmatrix} * & * & * \\ * & * & * \\ 0 & 0 & * \end{pmatrix}, \begin{pmatrix} 0 & * & * \\ 0 & * & * \\ 0 & * & * \end{pmatrix}, \begin{pmatrix} * & 0 & 0 \\ * & * & 0 \\ * & * & * \end{pmatrix}$ 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 $A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 2 \end{pmatrix}, b = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$
<u>Rückwärtssubstitution</u>: Aus der letzten Gleichung $x_3 + 2x_4 = 1$ sieht man, dass $x_4 = t$ frei gewählt wenden 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 (L_b) ändert sich nicht, wenn folgende Operationen auf (1.4b) angewandt werden:

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

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 $x_1, \cdots, x_n$ 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 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 $\dfrac{a_{i,1}}{a_{1,1}}$-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

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

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

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 #.

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 Umnummerieren 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:

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

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 $x_2, \cdots, x_m$. Durch Einsetzten 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_o). 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 $\circ : F(M) \times F(M) \to F(M)$ interpretiert werden - man spricht von einer Verknüpfung.

2.1.1 Definition (Gruppe)

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

2.1.2 Bemerkung

(1) Das neutrale Element $e \in \mathbb{G}$ ist eindeutig: In der Tat, bezeichnen $e_1, e_2 \in \mathbb{G}$ 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 $a \in \mathbb{G}$ ist auch das inverse Element $a^{-1} \in \mathbb{G}$ eindeutig. Für inverse Element a_1^{-1}, a_2^{-1} von a gilt nämlich

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

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

2.1.3 Bemerkung (Potenzen)

Die Potenzen $a^n \in \mathbb{G}$ eines $a \in \mathbb{G}$ (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 $(\mathbb{K}^{m\times n}\backslash\{0\}, \cdot)$ bilden keine Gruppe, da etwa $\mathrm{diag}(1, 0) \neq 0$ kein Inverses besitzt.

2.1.6 Beispiel (modulo)

Es sei $p \geq 2$ eine ganze Zahl und $\mathbb{Z}_p := \{0, \cdots, p-1\}$. 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 $k = a + b \mod p$ 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 $f : M \to M$. Dann ist die <u>symmetrischen Gruppe</u> $(S(M), \circ)$ eine i.A. nicht-kommutative Gruppe mit id_m als neutralem Element und $f^{-1} : M \to M$ als inversen Element zu f. Im Fall $M = \{1, \cdots, n\}$ schreiben wir $S_n := S(\{1, \cdots, n\})$. 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

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

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

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

Die verbleibende Implikation sei den Leser überlassen.

2.1.9 Definition (Körper)

Ein <u>Körper</u> $(\mathbb{K}, +, \cdot)$ ist eine Menge $\mathbb{K}$ mit mindestens zwei Elementen versehen.
Mit <u>den arithmetischen Operationen</u> $+ : \mathbb{K}\times\mathbb{K} \to \mathbb{K}$ (<u>Addition</u>) und $\cdot : \mathbb{K}\times\mathbb{K} \to \mathbb{K}$(<u>Multiplikation</u>).
$(\mathbb{K}_1)(\mathbb{K}, +)$ 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:

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

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

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

$(\mathbb{K}_3)$ 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 $\mathbb{Z}_p := \{0, \cdots, p\}$. 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

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

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

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

$$\text{Multiplikation: } \alpha \cdot_p \beta := l \text{ (2.1a)}$$

$(\mathbb{Z}_p, +_p, \cdot_p)$ 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	0
1	0	1

$\mathbb{Z}_3$:

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot_3$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

2.1.12 Korollar

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

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

Und ferner die Implikation $\alpha \cdot \beta = 0 \to \alpha = 0$ 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:

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

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 $0 \cdot \alpha \overset{(\mathbb{K}_1^2)}{=} (0 + 0) \cdot \alpha \overset{(\mathbb{K})}{=} 0\alpha + 0\alpha$ 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

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

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

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

2.1c ergibt sich mit Bemerkung 2.1.2(3) aus

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

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

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 $+ : \ X \times X \to X$ derart, dass $(X, +)$ eine kommutative Gruppe mit neutralem Element 0 oder Nullvektor.

(2) Skalare Multiplikation $\cdot : \mathbb{K} \times X \to X$ derart, dass für alle $\alpha, \beta \in \mathbb{K}$ und $x, y \in X$ gilt:

$$\begin{aligned}
&(V_1)\ \alpha(x+y) = \alpha x + \alpha y \text{ Distributiv Gesetz}\\
&(V_2)\ (\alpha+\beta)\cdot x = \alpha x + \beta x \text{ Distributiv Gesetz}\\
&(V_3)\ (\alpha\beta)\cdot x = \alpha\cdot(\beta\cdot x) \text{ Assoziativ Gesetz}\\
&(V_4)\ 1\cdot x = x
\end{aligned}$$

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) $\alpha A := \alpha A = (\alpha a_{i,j})_{\substack{1\le i\le m\\1\le j\le n}}$
(1.3c) $A + B := (\alpha_{i,j} + \beta_{i,j})_{\substack{1\le i\le m\\1\le j\le n}}$
Ein n-Tupel $(x_1, \cdots, x_n) \in \mathbb{K}^{1\times n}$ 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 $\mathbb{Z}_2^2$

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

$\cdot_2$	$\begin{pmatrix}0\\0\end{pmatrix}$	$\begin{pmatrix}1\\0\end{pmatrix}$	$\begin{pmatrix}0\\1\end{pmatrix}$	$\begin{pmatrix}1\\1\end{pmatrix}$
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 $F(\omega, X) := \{u : \omega \to X\}$ 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 $x, y \in X$:

$$(a) 0_{\mathbb{K}} \cdot x = \alpha \cdot 0_x = 0_x$$
$$(b) \text{Falls } \alpha x = 0_x, \text{ so folgt } \alpha = 0 \in \mathbb{K} \text{ oder } x \in 0 \in X$$
$$(c) (-\alpha)x = \alpha(-\alpha) = -(\alpha x)$$
$$(d) \alpha(x - y) = \alpha x - \alpha y \text{ und } (\alpha - \beta)x = \alpha x - \beta x$$

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.

(b) (b) Es gelte $\alpha x = 0$ mit $\alpha \neq 0$ und wir zeigen $x = 0_x$ $\alpha \neq 0$ existiert $\frac{1}{\alpha}$. Nach (a) folgt $\frac{1}{\alpha}(\alpha \cdot x) = \frac{1}{\alpha} \cdot 0 = 0$ und andererseits $\frac{1}{\alpha}(\alpha x) = (\frac{1}{\alpha} \cdot \alpha) \cdot x = 1 \cdot x = x$

(c) , (d)

2.2.7 Definition (Unterraum)

Eine nicht leere Teilmenge $Y \subseteq X$ eines linearen Raumes $(X, +, \cdot)$ über $\mathbb{K}$ heißt Unterraum von X, falls gilt $\alpha_1 y_1 + \alpha_2 y_2 \in Y$ für alle $\alpha_1, \alpha_2 \in \mathbb{K}$ und $y_1, y_2 \in Y$

2.2.8 Bemerkung

Jeder lineare Raum x hat die trivialen Unterräume $\{0\}$ und X.

2.2.9 Beispiel (Stetige und stetig-differenzierbare Funktion)

Es sei $I \subseteq \mathbb{R}$ ein Inervall. Die Menge der stetigen Funktionen $C(I, \mathbb{R}^n)$ auf I mit Bildern in $\mathbb{R}^n$ ist ein Unterraum von $F(I, \mathbb{R})$. Ebenso sind stetig differenzierbare Funktionen $C^1(I, \mathbb{R})$ ein Unterraum von $C(I, \mathbb{R})$ und $F(I, \mathbb{R}^n)$

2.2.10 Beispiel (Polynome)

Mit gegebenem Körper $\mathbb{K}$ definieren wir den Raum der Polynome (über $\mathbb{K}$) durch
$P(\mathbb{K}) := \{p \in F(\mathbb{K}, \mathbb{K}) \exists n \in \mathbb{N}_0 : \exists a_0, ..., a_n \in \mathbb{K} : p(t) = \sum_{l=0}^{n} a_l \cdot t^l\}$;
seine Elemente heißen Polynome und die a_k deren Koeffizienten. Dann ist $P(\mathbb{K})$ ein Unterraum von $F(\mathbb{K}, \mathbb{K})$.
Der Grad $deg\ p$ eines Polynoms $p \in P(\mathbb{K})$ ist der maximale Inde $k \in \mathbb{N}_0$ für den $a_k = 0$ ist. Für $m \in \mathbb{N}_0$ sind die Mengen $P_m(\mathbb{K}) := \{p \in P(\mathbb{K}) : deg\ p \leq m\}$

Unterräume von $P(\mathbb{K})$, wogegen $\{p \in P(\mathbb{K}) : deg\ p = m\}$ für $m \neq 0$ kein Unterraum ist. Ferner ist jedes $P_n(\mathbb{K})$ Unterraum von $P_m(\mathbb{K})$ für $0 \leq n \leq m$.

2.2.11 Satz (Schnitte und Summen von Unterräumen)

Ist I eine nichtleere Indexmenge und und $(Y_i)_{i \in I}$ eine Familie von Unterräumen von X.

(a) Der Durchschnitt $\bigcap\limits_{i \in I} Y_i$ ist ein Unterraum von X.

(b) Für endliche I ist die Summe $\sum\limits_{i \in I} Y_i := \{\sum\limits_{i \in I} y_i \in X : y_i \in Y_i$ mit $i \in I\}$ der kleinste Unterraum von X, der jedes y_i enthält.

Für $I = \{1, ..., n\}$ schreibt man auch $Y_1 + ... + Y_m = \sum\limits_{i \in J} Y_i$.

Beweis:

(a) Es seien $\alpha, p \in \mathbb{R}$ und $x, y \in \cap_{i \in I} Y_i$. Dann gilt $x, y \in Y_i$ für alle $i \in I$ und da jedes Y_i ein Unterraum von X ist, folgt $\alpha \cdot x + \beta \cdot y \in Y_i$ für jedes $i \in I$. Dies impliziert, dass $\alpha \cdot x + \beta \cdot y \in \cap_{i \in I} Y_i$

(b) Wir zeigen $Y := \sum\limits_{i \in I} Y_i$ ist ein Unterraum von X. Dazu sei $x = \sum\limits_{i \in I} x_i$ und $y = \sum\limits_{i \in I} y_i$ mit $x_i, y_i \in Y_i$ und wir erhalten für alle $\alpha, \beta \in \mathbb{R}$:
$\alpha \cdot x + \beta \cdot y = \alpha \sum\limits_{i \in I} x_i + \beta \sum\limits_{i \in I} y_i = \sum\limits_{i \in I} (\underbrace{\alpha x_i + \beta y_i}_{\in Y_i})$

Zu zeigen y ist kleinster Unterraum der alle Y_i enthält.
Dazu sei $z \subseteq X$ ein weiterer Unterraum von X der alle Y_i enthält. Für $x_i \in Y_i$ ist dann auch $x_i \in Z$ für alle $i \in I$, da Y_i in Z enthalten sind.
Aus der Unterraumeigenschaft von Z resultiert $\sum\limits_{i \in I} x_i \in Z$ und folglich ist $Y \subseteq Z$

2.3 Lineare Abhängigkeiten

Gegeben sei eine nichtleere Menge S von Vektoren aus einem linearen Raum X über dem Körper $\mathbb{K}$. Existieren zu einem gegebenem $x \in X$ dann endlich viele Koeffizienten $a_i \in \mathbb{R}$ und $x_i \in \mathcal{S}$, $1 \leq i \leq n$, mit $x = \sum\limits_{i=1}^{n} a_i \cdot x_i$ so bezeichnen wir x als Linearkombination der Vektoren aus S.

2.3.1 Definition (Spann)

Es sei $\mathcal{S} \leq X$. Der Spann oder die lineare Hülle *span* $\mathcal{S}$ von $\mathcal{S}$ ist die Menge aller Linearkombinationen. Ferner setzt man *span* $\{0\} = \{0\}$.

2.3.2 Beispiel

Für endliche $\mathcal{S} = \{x_0, ..., x_n\}$ ist der *span* $\mathcal{S} = \{\sum_{i=1}^{n} \alpha_i \cdot x_i \in X : \alpha_i \in \mathbb{K}\}$ $\mathbb{K} = \mathbb{R}$: $e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ gilt *span* $\{e_i, e_2\} = \mathbb{R}^2$
span $\{x_1, x_2\}$ wenn $x_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ und $x_2 = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$ aber $y_1 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ und $y_2 = \begin{pmatrix} 2 \\ 2 \end{pmatrix}$ dann *span* $\{y_1, y_2\} = \mathbb{R} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \in \mathbb{R}^2$

2.3.3 Beispiel (Monome)

Polynome $m_n(l) := t^n$, $n \in \mathbb{N}_0$ heißen Monome. Dann lassen sich die Polynome als lineare Hülle der Monome darstellen, d.h. *span* $\{m_n\}_{n \in \mathbb{N}_0} = P(\mathbb{K})$ insbesondere ist *span* $\{m_0, ..., m_n\} = P_n(\mathbb{K}^n)$
span $\{m_{2n}\}_{n \in \mathbb{N}_0} = \{p \in P(\mathbb{K}) : p(t) = p(-t)$ auf $\mathbb{K}\}$
span $\{m_{2n-1}\}_{n \in \mathbb{N}_0} = \{p \in P(\mathbb{K}) : p(t) = -p(-t)$ auf $\mathbb{K}\}$

2.3.4 Beispiel

Es sei $\mathcal{S} \in X$ nicht leer. Dann ist die lineare Hülle der kleinste $\mathcal{S}$ umfassende Unterraum von X

Beweis: $x, y \in \mathcal{S}$ ist $\alpha x + \beta y$, $\alpha, \beta \in \mathbb{K}$ in *span* $\mathcal{S}$. Also ist *span* $\mathcal{S}$ Unterraum von X. *span* $\mathcal{S}$ enthält die Vektoren aus $\mathcal{S}$ und damit ist $\mathcal{S} \subseteq$ *span* $\mathcal{S}$, $Y \subseteq X$ ein Unterraum von X mit $x \in Y$ für sämtliche $x \in \mathcal{S}$. Dann liegen sämtliche Linearkombinationen von Vektoren aus $\mathcal{S}$ in Y. Also ist *span* $\mathcal{S}$ in Y enthalten.

2.3.5 Korollar

Ist x eine Linearkombination von Vektoren aus $\mathcal{S} \subseteq X$, so gilt span$\mathcal{S}$=span$(\mathcal{S} \cup \{x\})$.
Beweis: Wir zeigen die Behauptung durch zwei Inklusionen:
($\subseteq$) Es ist klar dass span$\mathcal{S}$ $\subseteq$span$(\mathcal{S} \cup \{x\})$
($\supseteq$) Also Linearkombination von Vektoren aus $\mathcal{S}$ liegt x auch in span$\mathcal{S}$.
Demnach ist span$\mathcal{S}$ derjenige Unterraum welcher $\mathcal{S}$ und $\{x\}$ enthält.
Damit folgt aus Prop 2.3.4, dass span$(\mathcal{S} \cup \{x\})$=span$\mathcal{S}$.

2.3.6 Definition (lineare Unabhängigkeit)

Eine endliche Menge $\{x_1, \cdots, x_n\}$ von Vektoren aus X heißt linear unabhängig falls gilt:

$$\sum_{k=1}^{n} \xi_k x_k = 0 \Rightarrow \xi_k = 0 \forall n = 1, n$$

Griechische Buchstaben:

$$\eta \; - \; \text{eta}$$

$$\xi \; - \; \text{xi}$$

$$\zeta \; - \; \text{zeta}$$

Für beliebige Mengen $\mathcal{S} \subseteq X$ nennt man $\mathcal{S}$ linear unabhängig, wenn jede endliche Teilmenge von $\mathcal{S}$ linear unabhängig ist, die leere Menge $\emptyset$ wird als lineare unabhängig betrachtet. Eine Teilmenge von X heißt linear abhängig, falls sie nicht linear unabhängig ist.
Man nennt Vektoren $x_1, x_2, \cdots$ linear unabhängig, wenn $\{x_1, x_2, \cdots\}$ diese Eigenschaft hat.

2.3.7 Bemerkung

(1) lineare Abhängigkeit einer endlichen Menge $\{x_1, \cdots x_n\}$ bedeutet, dass eine nichttriviale Darstellung der Null aus Vektoren x_u existiert:
Man Kann also

$$(2.3a) \sum_{k=1}^{n} \xi_k x_k = 0$$

schreiben, ohne dass alle ξ_k verschwinden.

(2) Jede Obermenge einer linear abhängigen Menge ist linear abhängig. Jede Teilmenge einer linear unabhängigen Menge ist linear unabhängig.

2.3.8 Beispiel

Die Menge $\{0\}$ ist linear abhängig, dagegen ist $\{x\}, x \neq 0$, linear unabhängig.

2.3.9 Proposition

Es sei $\mathcal{S} \subseteq X$ nichtleer und $x, x_1, \cdots, x_n \in X$

(a) Ist $\mathcal{S} = \{x_1, \cdots, x_n\}$ linear abhängig, so lässt sich mindestens ein Vektor aus $\mathcal{S}$ als Linearkombination der weiteren Elementen von $\mathcal{S}$ darstellen.

(b) Für jede Linearkombination x aus $\mathcal{S}$ ist $\mathcal{S} \cup \{x\}$ linear abhängig.

Beweis:

(a) Weil $\{x_1, \cdots, x_n\}$ linear abhängig ist, besitzt 0 die Darstellung (2.3a) in welcher nicht alle ξ_k verschwinden. Also existiert ein Index $1 \leq k^* \leq n$ mit $\xi_{k^*} \neq 0$ und damit

$$X_{k^*} = -\xi_k^{-1} \sum_{\substack{k=1 \\ k \neq k^*}}^{n} \xi_k x_k = \sum_{\substack{k=1 \\ k \neq k^*}}^{n} (-\xi_k^{-1} \xi_k) x_k$$

(b) Mit $x = \sum_{k=1}^n \xi_k x_k$ ist $x - \sum_{k=1}^n \xi_k x_k$ eine nichttriviale Darstellung der 0

In $X = \mathbb{K}^m$ gilt: Es sei $\mathcal{S} = \{a_1, \cdots, a_n\} \subseteq \mathbb{K}^m$. Mit der $m \times n$-Matrize $A := (a_1, \cdots, a_n)$ ist die Beziehung $\sum_{k=1}^n \xi_k a_k = 0$ (vgl. (2.3a)) äquivalent zu:

$$(2.3b) Ax = 0, x \begin{pmatrix} \xi_1 \\ \vdots \\ \xi_n \end{pmatrix}$$

Demzufolge ist $\mathcal{S}$ genau dann linear unabhängig, wenn $Ax = 0$ nur die triviale Lösung hat. Aus Satz 1.4.8 (in Verbindung mit Blatt 5, Aufg. 1) erhalten wir daher, dass mehr als m Vektoren stets linear abhängig sind.

2.3.10 Beispiel

(1) Für die kanonischen Einheitsvektoren in $\mathbb{K}^m$

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, e_2 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \cdots e_m = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

gilt in obiger Terminologie $A = I_m$. Also besitzt $Ax = 0$ nur die triviale Lösung und $\{e_1, \cdots, e_m\}$ ist linear unabhängig.

(2) Es sei $\lambda \in \mathbb{R}$ um die lineare Unabhängigkeit von

$$x_1 \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, x_2 = \begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix}, x_3 = \begin{pmatrix} 7 \\ 8 \\ \lambda \end{pmatrix}$$

in $\mathbb{R}^3$ zu untersuchen, betrachten wir die Gleichung (2.3b) mit

$$A = \begin{pmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & \lambda \end{pmatrix}$$

und lösen sie mit dem in Beispiel 1.4.6 beschriebenen Schema:

$$\begin{array}{ccc|cc} 1 & 4 & 7 & 0 & \\ 2 & 5 & 6 & 0 & 2I-II \\ 3 & 6 & \lambda & & 3I-II \end{array} \Rightarrow \begin{array}{ccc|cc} 1 & 4 & 7 & 0 & \\ 0 & 3 & 6 & 0 & :3 \\ 0 & 6 & 21-\lambda & & III-2II \end{array} \Leftrightarrow \begin{array}{ccc|cc} 1 & 4 & 7 & 0 & \\ 0 & 1 & 2 & 0 & :3 \\ 0 & 0 & 9-\lambda & & III-2II \end{array}$$

Also hat $Ax = 0$ für $\lambda \neq 9$ nur die triviale Lösung (lineare Unabhängigkeit von $\{x_1, x_2, x_3\}$ und für $\lambda = 9$ nichttriviale Lösungen (lineare Abhängigkeit).

2.3.11 Satz

Eine Menge $\mathcal{S} \subseteq X$ ist genau dann linear unabhängig, wenn jedes $x \in \mathcal{S}$ auf nur eine Art (bis auf Glieder mit Null-Koeffizienten) als Linearkombinationen von Vektoren aus $\mathcal{S}$ dargestellt werden kann.

2.4 Basis und Dimensionen

Es sei X ein linearer Raum über den Körper $\mathbb{K}$.

2.4.1 Definition (Basis)

Eine Menge $\mathcal{X} \subseteq X$ heißt <u>Basis</u> von X, falls $\mathcal{X}$ linear unabhängig mit $X = \text{span}\mathcal{X}$ ist:
Eine Menge $\mathcal{X}$ mit $X = \text{span}\mathcal{X}$ heißt Erzeugendessystem (EZS) von X genannt. Man nennt X endlich erzeugt, falls er ein endliches EZS hat.

2.4.2 Beispiel

Die Basis von $\{0\}$ ist die leere Menge.

2.4.3 Beispiel (Standardbasis)

Die mittels der kanonischen Einheitsvektoren aus Beispiel 2.3.10 (1) gebildete Menge $\mathcal{E}_m := \{e_1, \cdots, e_m\}$ ist eine Basis von $\mathbb{K}^m$, die sogenannte Standardbasis, damit ist $\mathbb{K}^m$ endlich erzeugt.

2.4.4 Beispiel (Polynome)

Für $\mathbb{K} = \mathbb{R}$ oder $\mathbb{K} = \mathbb{C}$ sind $\mathcal{M}_n := \{m_0, \cdots m_n\}$ aus Beispiel 2.3.3 eine Basis der Polynome $\mathcal{P}_n(\mathbb{K})$ von maximalem Grad n. Ebenso ist $\{m_n\}_{n\in\mathbb{N}_0}$ eine Basis von $\mathcal{P}(\mathbb{K})$. Somit ist jedes $\mathcal{P}_n(\mathbb{K})$ endlich erzeugt, $\mathcal{P}(\mathbb{K})$ dagegen nicht.

2.4.5 Lemma

Es sei $\mathcal{S} \subseteq X$ linear unabhängig. Gilt dann $x \notin \text{span}\mathcal{S}$, so ist auch $\mathcal{S} \cup \{x\}$ linear unabhängig.
Beweis: Es ist nachzuweisen, dass jede endliche Teilmenge von $\mathcal{S} \cup \{x\}$ linear unabhängig ist. Dazu sei $\{x_1, \cdots x_n, x\}$ eine solche Menge und $\sum_{k=1}^{n} \xi_k + x_k + \eta x = 0$ eine Darstellung der Null. Wäre $\eta \neq 0$, so könnte man x als Linearkombination der $x_1, \cdots, x_n$ darstellen, dies widerspricht $x \notin \text{span}\mathcal{S}$. Also gilt $\eta = 0$. Da aber $\{x_1, \cdots, x_n\}$ linear unabhängig ist, folgt $\xi_1 = \cdots = \xi_n = 0$. In trivialer Weise: ist X ein EZS von X. Unser Interesse besteht aber gerade in „kleinen“ EZSen.

2.4.6 Satz

Mit nicht leerem $\mathcal{X} \subseteq X$ sind äquivalent:

(a) $\mathcal{X}$ ist eine Basis von X

(b) Jeder Vektor $x \in X$ lässt sich eindeutig als Linearkombination von Vektoren aus $\mathcal{X}$ darstellen.

(c) $\mathcal{X}$ ist maximal linear unabhängig, d.h. $\mathcal{X}$ ist linear unabhängig und für jedes $x \in X \setminus \mathcal{X}$ ist $\mathcal{X} \cup \{x\}$ linear abhängig.

(d) $\mathcal{X}$ ist ein minimales EZS, d.h. keine echte Teilmenge von $\mathcal{X}$ ist ein EZS.

2.4.7 Bemerkung (Koordinaten)

Besitzt $x \in X$ bzgl. der Basis $\mathcal{X} := \{x_1, \cdots, x_n\}$ die nach Satz 2.4.6 (b) eindeutige Darstellung $x = \sum_{k=1}^{n} \xi_k x_k$ mit Koeffizienten $\xi_k \in \mathbb{K}$ so bezeichnet man das n-tupel $(\xi_1, \cdots, \xi_n)$ also Koordinaten von x (bzgl. $\mathcal{X}$). Von nun an sei X endlich erzeugt.

2.4.8 Satz

Jedes endliche EZS eines Vektorraumes enthält eine Basis. Insbesondere hat jeder endlich erzeugte lineare Raum eine Basis.
Beweis: Es sei $\mathcal{X}$ ein endliches EZS. Ist $\mathcal{X}$ keine Basis, so kann $\mathcal{X}$ nicht minimal sein und es existiert eine echte Teilmenge $\mathcal{X}^1 \overset{\subset}{\neq} \mathcal{X}$, die ebenfalls ein EZS ist. Ist wiederum $\mathcal{X}^1$ keine Basis, so existiert erneut eine echte Teilmenge $\mathcal{X}^2 \overset{\subset}{\neq} \mathcal{X}^1$, die X erzeugt. Durch Iteration erhält man eine echt absteigende Folge von Teilmengen $\cdots \subsetneqq \mathcal{X}^2 \subsetneqq \mathcal{X}^1 \subsetneqq \mathcal{X}$. Diese Folge bricht nach endlich vielen schritten ab, da $\mathcal{X}$ endlich ist, d.h. es gibt ein minimales $\mathcal{X}^k$. Dieses $\mathcal{X}^k$ ist nach Satz 2.4.6 eine Basis von X.

2.4.9 Proposition

Ist X endlich erzeugbar und $\mathcal{S} \subseteq X$ linear unabhängig, so existiert eine Basis von X, welche $\mathcal{S}$ als Teilmenge enthält.

2.4.10 Lemma (Austauschsatz von Steinitz)

Ist $\{x_1, \cdots x_p\}$ linear unabhängig und $\{y_1, \cdots, y_n\}$ ein EZS von X, so gilt $p \leq n$ und nach einer Umnummerierung der y_k ist $\{x_1, \cdots, x_p, y_{p+1}, \cdots, y_n\}$ ein EZS von X.

2.4.11 Satz (Dimension)

Falls X eine Basis von n Elementen besitzt, enthält jede Basis von X genau n Elemente. Wir bezeichnen n als Dimension von X und schreiben $n =\text{dim}X$.

2.4.12 Bemerkung

Ein linearer Raum X heißt unendlich-dimensional (symbolisch $\text{dim}X = \infty$) falls er kein endlichen EZS besitzt, anderenfalls heißt er endlich-dimensional.
Beweis: Es seien $\{x_1, \cdots, x_n\}$ und auch $\{y_1, \cdots, y_m\}$ Basen von X. Mit Lemma 2.4.10 folgt dann $n \leq m$, wie auch $m \leq n$, und somit $m = n$.

2.4.13 Beispiel

Für die bislang betrachteten Räume ist $\text{dim}\mathbb{K}^n = n$, $\text{dim}\mathbb{K}^{m\times n} = m \cdot n$, $\text{dim}\mathcal{P}_n(\mathbb{R}) = n + 1$ und $\text{dim}\mathcal{P}(\mathbb{R}) =\text{dim}C^1(\mathbb{R}, \mathbb{R}) =\text{dim}C(\mathbb{R}, \mathbb{R}) =\text{dim}F(\mathbb{R}, \mathbb{R}) = \infty$.

2.4.14 Beispiel

Die komplexen Zahlen $\mathbb{C}$ sind ein 2-dimensionaler Vektorraum über $\mathbb{R}$ und ein 1-dimensionaler Raum über $\mathbb{C}$.

2.4.15 Korollar

In linearen Räumen X mit $n :=\text{dim}X$ gilt:

(a) Weniger als n Vektoren aus X sind kein EZS.

(b) Mehr als n Vektoren aus X sind linear abhängig.

(c) Jedes EZS mit n Elementen ist eine Basis.

(d) Jede linear unabhängige Menge mit n Elementen ist eine Basis.

Beweis:

(a) jedes EZS enthält laut Satz 2.4.8 eine Basis. Für jedes aus weniger als n Vektoren bestehenden EZS gäbe es dann auch eine Basis mit Weniger als n Elementen. Dies widerspricht Satz 2.4.11.

(b) Laut Proposition 2.4.9 ist jede linear unabhängige Menge Teil einer Basis. Somit hätte man mit einer linear unabhängigen Familie von mehr als n Vektoren auch eine Basis mit mehr als n Elementen - im Widerspruch zu 2.4.11.

(c) Ein EZS enthält wegen Satz 2.4.8 eine Basis und ist wegen Satz 2.4.11 bereits eine solche.

(d) Mit Proposition 2.4.9 ist eine linear unabhängige Familie Teilmenge einer Basis und mit Satz 2.4.11 eine Basis.

2.4.16 Korollar

Für jeden Unterraum Y eines endlich-dimensionalen Raumes X ist $\dim Y \leq \dim X$, Gleichheit gilt genau für $X = Y$.