Lineare Algebra I

Wilfried Buchholz

Skriptum einer 4-std. Vorlesung im Wintersemester 2009/10

Mathematisches Institut der Universität München

§1 Lineare Gleichungssysteme und Matrizen

Einige Abkürzungen.

$\mathbb{N} = \{0, 1, 2, \ldots\}$ (Menge der *natürlichen* Zahlen)

$\mathbb{Z} = \mathbb{N} \cup \{-n : n \in \mathbb{N}\}$ (Menge der *ganzen* Zahlen)

$\mathbb{Q} = \{\frac{x}{y} : x, y \in \mathbb{Z} \,\&\, y \neq 0\}$ (Menge der *rationalen* Zahlen)

$\mathbb{R}$ (Menge der *reellen* Zahlen)

$\mathbb{N}_1 := \{n \in \mathbb{N} : n \neq 0\}$.

Die Buchstaben i, j, k, l, m, n, p bezeichnen im folgenden stets natürliche Zahlen.

$\sum\limits_{i=m}^{n} a_i := a_m + a_{m+1} + \ldots + a_n$ (falls $m \leq n$)

Definitionen. Seien $m, n \neq 0$.

Ein rechteckiges Schema reeller Zahlen $a_{ij} \in \mathbb{R}$

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \ldots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \ldots & a_{2n} \\ \vdots & \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & a_{m3} & \ldots & a_{mn} \end{pmatrix}$$

heißt *$m{\times}n$-Matrix* mit *Koeffizienten a_{ij}* in $\mathbb{R}$.

Hierfür schreibt man auch $A = (a_{ij})_{\substack{i=1,\ldots,m \\ j=1,\ldots,n}} = (a_{ij})_{i,j} = (a_{ij})$. $\big((a)\big)$

Für $i \in \{1, ..., m\}$ und $j \in \{1, ..., n\}$ heißt

$(a_{i1}\ a_{i2}\ \ldots\ a_{in})$ die i-te *Zeile* von A und $\begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{pmatrix}$ die j-te *Spalte* von A.

$\mathbb{R}^{m\times n} := \{A : A$ ist $m{\times}n$-Matrix mit Koeffizienten in $\mathbb{R}\}$.

$\mathbb{R}^{1\times 1}$ wird mit $\mathbb{R}$ identifiziert.

$\mathbb{R}^{m\times 1}$ (bzw. $\mathbb{R}^{1\times n}$) heißt *m-dimensionaler Spaltenraum* (bzw. *n-dimensionaler Zeilenraum*).

Die Elemente von $\mathbb{R}^{m\times 1}$ ($\mathbb{R}^{1\times n}$) heißen *Spaltenvektoren der Länge m* (*Zeilenvektoren der Länge n*).

Bemerkung. Die Spalten (bzw. Zeilen) einer $m{\times}n$-Matrix sind Elemente von $\mathbb{R}^{m\times 1}$ (bzw. $\mathbb{R}^{1\times n}$).

Abkürzung. $\mathbb{R}^n := \mathbb{R}^{n\times 1}$ *(n-dimensionaler Spaltenraum)*

Schreibweise.

Sind $a_1, \ldots, a_n \in \mathbb{R}^m = \mathbb{R}^{m\times 1}$, so bezeichnet $\big(a_1\ \ldots\ a_n\big)$ die $m{\times}n$-Matrix mit den Spalten $a_1, \ldots, a_n$.

Sind $b_1, \ldots, b_m \in \mathbb{R}^{1\times n}$, so bezeichnet $\begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$ die $m{\times}n$-Matrix mit den Zeilen $b_1, \ldots, b_m$.

Eine Matrix, deren sämtliche Koeffizienten gleich 0 sind, heißt *Nullmatrix* und wird mit $\mathbf{0}$ bezeichnet.

Zwischen der Matrix $A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \in \mathbb{R}^{m\times n}$ und der Spalte $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{R}^n$

erklärt man ein Produkt, das eine Spalte der Länge m ergibt:

$$A \cdot x := \begin{pmatrix} a_{11}x_1 + & \dots & + a_{1n}x_n \\ \vdots & & \vdots \\ a_{m1}x_1 + & \dots & + a_{mn}x_m \end{pmatrix} = \begin{pmatrix} \sum_{j=1}^n a_{1j}x_j \\ \vdots \\ \sum_{j=1}^n a_{mj}x_j \end{pmatrix} \in \mathbb{R}^m.$$

Das *lineare Gleichungssystem*

$$(*) \quad \begin{array}{ccccccc} a_{11}x_1 & + & \dots & + & a_{1n}x_n & = & b_1 \\ a_{21}x_1 & + & \dots & + & a_{2n}x_n & = & b_2 \\ \vdots & & & & & & \vdots \\ a_{m1}x_1 & + & \dots & + & a_{mn}x_n & = & b_m \end{array}$$

kann man dann in der Form $\quad A \cdot x = b \quad$ mit $b := \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$ schreiben.

A heißt die *Koeffizientenmatrix*, und $(A\ b) := \begin{pmatrix} a_{11} & \dots & a_{1n} & b_1 \\ \vdots & & \vdots & \vdots \\ a_{m1} & \dots & a_{mn} & b_m \end{pmatrix}$ die *erweiterte Koeffizientenmatrix* des linearen Gleichungssystems $(*)$.

$\text{Lös}(A; b) := \{x \in \mathbb{R}^n : A \cdot x = b\}$ heißt *die Lösungsmenge* oder *der Lösungsraum* von $(*)$.

Definition.

Unter *elementaren Zeilenumformungen* einer Matrix A versteht man folgende Umformungen von A:

(I) Vertauschen zweier Zeilen.

(II) Addition des λ-fachen der j-ten Zeile zur i-ten Zeile, wobei $\lambda \in \mathbb{R}$ und $i \neq j$.

(III) Multiplikation der i-ten Zeile mit einem $\lambda \in \mathbb{R} \setminus \{0\}$.

Abkürzungen:

$A \overset{\text{EZU}}{\longmapsto} A' \quad :\Longleftrightarrow \quad A'$ entsteht aus A durch eine endliche Folge elementarer Zeilenumformungen.

$A \overset{\text{X}}{\longmapsto} A' \quad :\Longleftrightarrow \quad A'$ entsteht aus A durch elementare Zeilenumformungen vom Typ X .

Lemma 1.1. Aus $A, A' \in \mathbb{R}^{m\times n}$, $b, b' \in \mathbb{R}^m$ und $(A\ b) \overset{\text{EZU}}{\longmapsto} (A'\ b')$ folgt $\text{Lös}(A; b) = \text{Lös}(A'; b')$.

Beweis:

Offenbar reicht es, die Inklusion $\text{Lös}(A; b) \subseteq \text{Lös}(A'; b')$ zu zeigen, denn mit $(A\ b) \overset{\text{EZU}}{\longmapsto} (A'\ b')$ gilt auch $(A'\ b') \overset{\text{EZU}}{\longmapsto} (A\ b)$. Für Umformungen der Typen (I), (III) ist die Behauptung trivial.

Sei jetzt $(A'\ b')$ aus $(A\ b)$ durch Addition des λ-fachen der k-ten Zeile zur l-ten Zeile entstanden.

Dann gilt: $x \in \text{Lös}(A; b) \ \Rightarrow \ \sum\limits_{j=1}^n a_{ij}x_j = b_i \ (i \neq l, k) \ \& \ \sum\limits_{j=1}^n a_{lj}x_j = b_l \ \& \ \sum\limits_{j=1}^n a_{kj}x_j = b_k \ \Rightarrow$

$$\Rightarrow \sum_{j=1}^n a_{ij}x_j = b_i \ (i \neq l) \ \& \ \sum_{j=1}^n (a_{lj} + \lambda a_{kj})x_j = b_l + \lambda b_k \ \Rightarrow \ \sum_{j=1}^n a'_{ij}x_j = b'_i \ (i = 1, ..., n) \ \Rightarrow \ x \in \text{Lös}(A; b).$$

Beispiel

$$\begin{array}{r} x_1 + 2x_2 + 4x_3 = 1 \\ 2x_1 + 3x_2 + 5x_3 = 0 \\ 3x_1 + 4x_2 + 8x_3 = 5 \end{array} \iff \begin{array}{r} x_1 + 2x_2 + 4x_3 = 1 \\ - \ \ x_2 - 3x_3 = -2 \\ 3x_1 + 4x_2 + 8x_3 = 5 \end{array} \iff \begin{array}{r} x_1 + 2x_2 + 4x_3 = 1 \\ - \ \ x_2 - 3x_3 = -2 \\ - 2x_2 - 4x_3 = 2 \end{array} \iff$$

$$\begin{array}{rcl} x_1 + 2x_2 + 4x_3 = 1 \\ x_2 + 3x_3 = 2 \\ x_2 + 2x_3 = -1 \end{array} \iff \begin{array}{r} x_1 + 2x_2 + 4x_3 = 1 \\ x_2 + 3x_3 = 2 \\ -x_3 = -3 \end{array} \iff \begin{array}{l} x_1 = 3 \\ x_2 = -7 \\ x_3 = 3 \end{array}$$

Definition.

1. $\delta_{ij} := \begin{cases} 1 & \text{falls } i = j \\ 0 & \text{sonst} \end{cases}$ *(Kronecker-Symbol)*
2. $e_j^n := \begin{pmatrix} \delta_{1j} \\ \vdots \\ \delta_{nj} \end{pmatrix} \in \mathbb{R}^n$ heißt j*-ter Einheitsvektor* des $\mathbb{R}^n$. Meist schreibt man kurz e_j statt e_j^n.

Definition.

Eine $m \times n$-Matrix $A = (a_{ij})$ heißt in *Zeilenstufenform* (oder kurz *Stufenmatrix*),

wenn es natürliche Zahlen $r \leq m$ und $1 \leq j_1 < j_2 < \ldots < j_r \leq n$ gibt, so daß gilt:

1. $a_{1j_1}, \ldots, a_{rj_r} \neq 0$,
2. $a_{ij} = 0$ falls $(1 \leq i \leq r$ und $1 \leq j < j_i)$ oder $r < i \leq m$;

d.h. wenn A von der folgenden Form ist (wobei auch $r = 0$, d.h. $A = \mathbf{0}$ sein kann):

$$\begin{pmatrix} 0 \ldots 0\ a_{1j_1} \ldots\ldots\ldots\ldots\ldots\ a_{1n} \\ 0 \ldots\ldots\ldots 0\ a_{2j_2} \ldots\ldots\ldots\ a_{2n} \\ \vdots \\ 0 \ldots\ldots\ldots\ldots\ldots 0\ a_{rj_r} \ldots\ a_{rn} \\ 0 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots 0 \\ \vdots \\ 0 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots 0 \end{pmatrix} \quad \text{mit } r \leq m,\ 1 \leq j_1 < \ldots < j_r \leq n \text{ und } a_{1j_1}, \ldots, a_{rj_r} \neq 0.$$

$a_{1j_1}, \ldots, a_{rj_r}$ heißen Angelpunkte (*Pivots*), und die Spalten zu $j_1, ..., j_r$ heißen *Stufenspalten.*

Sind die Stufenspalten die Einheitsvektoren $e_1, \ldots, e_r$, d.h. gilt $a_{ij_k} = \delta_{ik}$ für $k = 1, ..., r$ und $i = 1, ..., m$, so nennen wir A eine *ausgezeichnete* Stufenmatrix.

Beispiele.

1. $\begin{pmatrix} 0 & 5 & 0 & 4 & 1 & 0 & 5 \\ 0 & 0 & 1 & 7 & 5 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 4 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \in \mathbb{R}^{4\times 7}$ ist Stufenmatrix mit $r = 3$, $j_1 = 2$, $j_2 = 3$, $j_3 = 6$.
2. $\begin{pmatrix} 5 & 1 & 2 \\ 0 & 4 & 3 \\ 0 & 0 & 7 \end{pmatrix}$ ist Stufenmatrix mit $j_1 = 1$, $j_2 = 2$, $j_3 = 3$.
3. $\begin{pmatrix} 0 & 1 & 4 & 2 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 2 \end{pmatrix}$ ist *keine* Stufenmatrix.

Lemma 1.2.

(a) Jede Matrix $A \in \mathbb{R}^{m\times n}$ läßt sich durch elementare Zeilenumformungen der Typen (I) und (II) in eine Stufenmatrix $A' \in \mathbb{R}^{m\times n}$ überführen.

(b) Jede Stufenmatrix $A \in \mathbb{R}^{m\times n}$ läßt sich durch elementare Zeilenumformungen der Typen (II) und (III) in eine ausgezeichnete Stufenmatrix $A' \in \mathbb{R}^{m\times n}$ überführen.

Beweis von (a) durch Induktion nach m:

Fall 1: $A = \mathbf{0}$ oder $m = 1$. Dann ist A eine Stufenmatrix.

Fall 2: $A \neq \mathbf{0}$ und $1 < m$. Sei $j_1 := \min\{j : \exists i(a_{ij} \neq 0)\}$ und sei $i \in \{1, ..., m\}$ mit $a_{ij_1} \neq 0$.

Durch Abziehen des $\frac{a_{kj_1}}{a_{ij_1}}$-fachen der i-ten Zeile von der k-ten Zeile (für $k \in \{1, ..., m\} \setminus \{i\}$), sowie anschließendes Vertauschen der ersten mit der i-ten Zeile erhält man

$$A_1 = \begin{pmatrix} 0 & \dots & 0 & a_{ij_1} & * \cdots\cdots * \\ 0 & \dots & 0 & 0 & \\ \vdots & & \vdots & \vdots & B \\ 0 & \dots & 0 & 0 & \end{pmatrix}.$$

Nach I.V. (Induktionsvoraussetzung) kann B durch elementare Zeilenumformungen auf Stufenform B' gebracht werden. Anwenden der entsprechenden Zeilenumformungen auf A_1 liefert die Stufenmatrix

$$A' = \begin{pmatrix} 0 & \dots & 0 & a_{ij_1} & * \cdots\cdots * \\ 0 & \dots & 0 & 0 & \\ \vdots & & \vdots & \vdots & B' \\ 0 & \dots & 0 & 0 & \end{pmatrix}.$$

(b) ist klar.

Beispiel.

$$\begin{matrix} 0 & 0 & 1 & 2 & 9 \\ 0 & 3 & 4 & 5 & 9 \\ 0 & 6 & 7 & 8 & 9 \\ 0 & 9 & 9 & 9 & 9 \end{matrix} \mapsto \begin{matrix} 0 & 3 & 4 & 5 & 9 \\ 0 & 0 & 1 & 2 & 9 \\ 0 & 0 & -1 & -2 & -9 \\ 0 & 0 & -3 & -6 & -18 \end{matrix} \mapsto \begin{matrix} 0 & 3 & 4 & 5 & 9 \\ 0 & 0 & 1 & 2 & 9 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 9 \end{matrix} \mapsto \begin{matrix} 0 & 3 & 4 & 5 & 9 \\ 0 & 0 & 1 & 2 & 9 \\ 0 & 0 & 0 & 0 & 9 \\ 0 & 0 & 0 & 0 & 0 \end{matrix} \mapsto$$

$$\begin{matrix} 0 & 3 & 4 & 5 & 0 \\ 0 & 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{matrix} \mapsto \begin{matrix} 0 & 3 & 0 & -3 & 0 \\ 0 & 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{matrix} \mapsto \begin{matrix} 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{matrix}$$

Lemma 1.3'.

Sei $A \in \mathbb{R}^{m \times n}$ eine ausgezeichnete Stufenmatrix mit den Pivots $a_{11} = \ldots = a_{rr} = 1$.

Sei ferner $b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \in \mathbb{R}^m$. Dann gilt für das Gleichungssystem $A \cdot x = b$:

(a) Ist $b_i \neq 0$ für mindestens ein $i \in \{r+1, \ldots, m\}$, so ist das Gleichungssystem unlösbar, d.h. $\text{Lös}(A; b) = \emptyset$.

(b) Andernfalls ist das Gleichungssystem lösbar und

$$\text{Lös}(A; b) = \{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} : x_i = b_i - \sum_{j=r+1}^{n} a_{ij} x_j \ (i = 1, \ldots, r)\}.$$

Beweis:

(a) Sei $r+1 \leq i \leq m$ und $b_i \neq 0$. Dann gilt $a_{i1} = \ldots = a_{in} = 0$ und somit $\sum_{j=1}^n a_{ij} x_j = 0$ für beliebige $x_1, ..., x_n \in \mathbb{R}$. Folglich ist die Gleichung $\sum_{j=1}^n a_{ij} x_j = b_i$ und damit das ganze System $A \cdot x = b$ unlösbar.

(b) Es gilt: $x \in \text{Lös}(A; b) \Leftrightarrow A \cdot x = b \Leftrightarrow \sum\limits_{j=1}^{n} a_{ij} x_j = b_i \ (i = 1, \ldots, r)$. Nach Voraussetzung über A ist aber $a_{ij} = \delta_{ij}$ $(i, j \in \{1, \ldots, r\})$ und deshalb $\sum\limits_{j=1}^{n} a_{ij} x_j = \sum\limits_{j=1}^{r} \delta_{ij} x_j + \sum\limits_{j=r+1}^{n} a_{ij} x_j = x_i + \sum\limits_{j=r+1}^{n} a_{ij} x_j \ (i = 1, \ldots, r)$.

Folglich: $\text{Lös}(A; b) = \{x : \sum_{j=1}^n a_{ij} x_j = b_i \ (i = 1, \ldots, r)\} = \{x : x_i = b_i - \sum\limits_{j=r+1}^{n} a_{ij} x_j \ (i = 1, \ldots, r)\}$.

Lemma 1.3.

Sei $A \in \mathbb{R}^{m\times n}$ eine ausgezeichnete Stufenmatrix mit den Pivots $a_{1j_1} = \ldots = a_{rj_r} = 1$ $(1 \le j_1 < \ldots < j_r \le n)$.

Sei ferner $b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \in \mathbb{R}^m$, und seien $j_{r+1} < \ldots < j_n$, so daß $\{j_1, \ldots, j_n\} = \{1, \ldots, n\}$.

Dann gilt für das Gleichungssystem $A \cdot x = b$:

(a) Ist $b_i \neq 0$ für mindestens ein $i \in \{r{+}1, \ldots, m\}$, so ist das Gleichungssystem unlösbar, d.h. $\text{Lös}(A;b) = \emptyset$.

(b) Andernfalls ist das Gleichungssystem lösbar und

$$\text{Lös}(A;b) = \{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} : x_{j_i} = b_i - \sum_{k=r+1}^{n} a_{ij_k} x_{j_k} \ (i = 1, \ldots, r)\}.$$

Beweis:

(a) Wie bei Lemma 1.3'.

(b) Es gilt: $x \in \text{Lös}(A;b) \Leftrightarrow A{\cdot}x = b \Leftrightarrow \sum\limits_{j=1}^{n} a_{ij}x_j = b_i \ (i = 1, \ldots, r)$. Da A ausgezeichnete Stufenmatrix ist, gilt aber $a_{ij_k} = \delta_{ik}$ $(i, k \in \{1, ..., r\})$ und deshalb $\sum\limits_{j=1}^{n} a_{ij}x_j = \sum\limits_{k=1}^{r} a_{ij_k}x_{j_k} + \sum\limits_{k=r+1}^{n} a_{ij_k}x_{j_k} = x_{j_i} + \sum\limits_{k=r+1}^{n} a_{ij_k}x_{j_k}$.

Folglich: $\text{Lös}(A;b) = \{x : \sum\limits_{j=1}^{n} a_{ij}x_j = b_i \ (i = 1, \ldots, r)\} = \{x : x_{j_i} = b_i - \sum\limits_{k=r+1}^{n} a_{ij_k}x_{j_k} \ (i = 1, \ldots, r)\}$.

Beispiel.

$$A = \begin{pmatrix} 1 & 0 & 2 & 0 & 0 & 6 \\ 0 & 1 & -1 & 0 & 0 & -5 \\ 0 & 0 & 0 & 1 & 0 & -2 \\ 0 & 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad b = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Hier ist $m = 5$, $n = 6$, $r = 4$, $j_1 = 1$, $j_2 = 2$, $j_3 = 4$, $j_4 = 5$, $j_5 = 3$, $j_6 = 6$.

$\text{Lös}(A;0) = \{x \in \mathbb{R}^6 : x_1 = -2x_3 - 6x_6 \ \&\ x_2 = x_3 + 5x_6 \ \&\ x_4 = 2x_6 \ \&\ x_5 = -2x_6\} =$

$$= \left\{ \begin{pmatrix} -2x_3 - 6x_6 \\ x_3 + 5x_6 \\ x_3 \\ 2x_6 \\ -2x_6 \\ x_6 \end{pmatrix} : x_3, x_6 \in \mathbb{R} \right\} = \left\{ \begin{pmatrix} -2s - 6t \\ s + 5t \\ s \\ 2t \\ -2t \\ t \end{pmatrix} : s, t \in \mathbb{R} \right\}.$$

Eliminationsverfahren von GAUSS zur Lösung eines Systems von m linearen Gleichungen mit n Unbekannten:

1. Man schreibe die erweiterte Koeffizientenmatrix $(A\ b)$ auf.
2. Man transformiere A durch elementare Zeilenumformungen in eine ausgezeichnete Stufenmatrix und forme dabei die Spalte b mit um. – Das Ergebnis sei $(A'\ b')$.
3. Aus Lemma 1.3 erhält man die Lösungsmenge $\text{Lös}(A';b')$, und nach Lemma 1.1 ist $\text{Lös}(A;b) = \text{Lös}(A';b')$.

Definition (Addition und Skalarmultiplikation von Matrizen)

Für $m, n \ge 1$, $A = \left(a_{ij}\right)_{\substack{i=1,\ldots,m \\ j=1,\ldots,n}} \in \mathbb{R}^{m\times n}$, $B = \left(a_{ij}\right)_{\substack{i=1,\ldots,m \\ j=1,\ldots,n}} \in \mathbb{R}^{m\times n}$ und $\lambda \in \mathbb{R}$ seien

$$A + B := \left(a_{ij} + b_{ij}\right)_{\substack{i=1,\ldots,m \\ j=1,\ldots,n}} \in \mathbb{R}^{m\times n} \quad \text{und} \quad \lambda A := \lambda{\cdot}A := \left(\lambda a_{ij}\right)_{\substack{i=1,\ldots,m \\ j=1,\ldots,n}} \in \mathbb{R}^{m\times n}.$$

Ferner sei $-A := (-1)\cdot A$, $A - B := A + (-B)$ für $A, B \in \mathbb{R}^{m\times n}$.

Die Matrix $E_n := (\delta_{i,j})_{i,j} \in \mathbb{R}^{n\times n}$ heißt *(n-reihige Einheitsmatrix).*

Die j-te Spalte von E_n ist e_j^n, der j-ter Einheitsvektor des $\mathbb{R}^n$.

Lemma 1.4.
Seien $m, n \geq 1$. Dann gilt für alle $A, B, C \in \mathbb{R}^{m\times n}$ und $\lambda, \mu \in \mathbb{R}$:

(a) $(A + B) + C = A + (B + C)$ (Assoziativgesetz)

(b) $A + B = B + A$ (Kommutativgesetz)

(c) $A + \mathbf{0} = A$ (neutrales Element)

(d) $A + (-A) = \mathbf{0}$ (inverses Element)

(e) $(\lambda\mu)A = \lambda(\mu A)$

(f) $(\lambda + \mu)A = \lambda A + \mu A$

(g) $\lambda(A + B) = \lambda A + \lambda B$

Beweis klar.

Bemerkung. Unter Verwendung der eben eingeführten Operationen kann die Lösungsmenge in obigem Beispiel auch folgendermaßen geschrieben werden:

$$\text{Lös}(A;0) = \left\{ s \begin{pmatrix} -2 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + t \begin{pmatrix} -6 \\ 5 \\ 0 \\ 2 \\ -2 \\ 1 \end{pmatrix} : s, t \in \mathbb{R} \right\}.$$

Definition (Multiplikation von Matrizen).
Für $m, n, p \geq 1$, $A = \big(a_{ij}\big)_{\substack{i=1,\dots,m \\ j=1,\dots,n}} \in \mathbb{R}^{m\times n}$, $B = \big(b_{jk}\big)_{\substack{j=1,\dots,n \\ k=1,\dots,p}} \in \mathbb{R}^{n\times p}$ sei

$$AB := A\cdot B := \Big(\sum_{j=1}^{n} a_{ij}b_{jk}\Big)_{\substack{i=1,\dots,m \\ k=1,\dots,p}} = \big(a_{i1}b_{1k} + \ldots + a_{in}b_{nk}\big)_{\substack{i=1,\dots,m \\ k=1,\dots,p}} \in \mathbb{R}^{m\times p}.$$

Bemerkungen.

1. $A\cdot B$ ist nur definiert, wenn die Zeilenlänge von A gleich der Spaltenlänge von B ist!!!
2. Für $B \in \mathbb{R}^n$ (d.h. im Fall $p = 1$) stimmt diese Definition mit der auf Seite 1 gegebenen Definition des Produkts einer Matrix mit einem Spaltenvektor überein.
3. Für $A = (a_1 \ \dots \ a_n) \in \mathbb{R}^{1\times n}$ und $B = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \in \mathbb{R}^{n\times 1}$ gilt: $A\cdot B = a_1b_1 + \ldots + a_nb_n = \sum_{j=1}^{n} a_jb_j \in \mathbb{R}$.

Definition. Für $A = (a_{ij})_{i,j} \in \mathbb{R}^{m\times n}$ sei $[A]_{ij} := a_{ij}$.

Sind $A, B \in \mathbb{R}^{m\times n}$, so gilt: $A = B \Leftrightarrow [A]_{ij} = [B]_{ij}$ für alle $i \in \{1, ..., m\}$, $j \in \{1, ..., n\}$.

Lemma 1.5.
Für $A \in \mathbb{R}^{m\times n}$ und $B \in \mathbb{R}^{n\times p}$ mit den Spalten $a_1, \dots, a_n \in \mathbb{R}^m$ bzw. $b_1, \dots, b_p \in \mathbb{R}^n$ gilt:

(a) $A\cdot B = \big(A\cdot b_1 \ \dots \ A\cdot b_p\big)$, (b) $A \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \sum_{j=1}^{n} x_ja_j$, (c) $A \cdot e_j = a_j$.

Beweis:

(a) $[AB]_{ik} = \sum_{j=1}^{n} a_{ij}b_{jk} = [A\cdot b_k]_{i1} = [\big(A\cdot b_1 \ \dots \ A\cdot b_n\big)]_{ik}$

(b) $[A\cdot x]_{i1} = \sum_{j=1}^{n} a_{ij}x_j = \sum_{j=1}^{n} x_j[a_j]_{i1} = [\sum_{j=1}^{n} x_ja_j]_{i1}$. (c) folgt aus (b).

Beispiele:

$$\underbrace{\begin{pmatrix} 1 & 0 & -1 \\ 2 & 1 & 3 \end{pmatrix}}_{\in\mathbb{R}^{2\times 3}} \cdot \underbrace{\begin{pmatrix} 1 & 0 & 2 \\ 2 & -1 & 1 \\ 1 & 0 & 0 \end{pmatrix}}_{\in\mathbb{R}^{3\times 3}} = \begin{pmatrix} 0 & 0 & 2 \\ 7 & -1 & 5 \end{pmatrix} \in \mathbb{R}^{2\times 3}$$

$$\begin{pmatrix} 2 & 0 & -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \\ 1 \\ 3 \end{pmatrix} = 2 \in \mathbb{R} \quad (= \mathbb{R}^{1\times 1})$$

$$\underbrace{\begin{pmatrix} 1 \\ -2 \\ 0 \end{pmatrix}}_{\in\mathbb{R}^{3\times 1}} \cdot \underbrace{\begin{pmatrix} 2 & 1 & 3 & 0 \end{pmatrix}}_{\in\mathbb{R}^{1\times 4}} = \begin{pmatrix} 2 & 1 & 3 & 0 \\ -4 & -2 & -6 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \in \mathbb{R}^{3\times 4}.$$

Beachte: Für $A \in \mathbb{R}^{m\times n}$ und $B \in \mathbb{R}^{q\times p}$ (mit $m, n, p, q \geq 1$) gilt:

(i) $A + B$ ist nur definiert, wenn $m = q$ & $n = p$.

(ii) $A \cdot B$ ist nur definiert, wenn $n = q$.

Lemma 1.6 (Rechenregeln für die Matrizenmultiplikation).
Seien $m, n, p, q \geq 0$. Dann gilt für alle $A, A' \in \mathbb{R}^{m\times n}$, $B, B' \in \mathbb{R}^{n\times p}$, $C \in \mathbb{R}^{p\times q}$, $\lambda \in \mathbb{R}$:

(a) $(A + A')B = AB + A'B$ und $A(B + B') = AB + AB'$ (Distributivgesetze)

(b) $AE_n = A = E_m A$

(c) $\lambda(AB) = (\lambda A)B = A(\lambda B)$

(d) $(AB)C = A(BC)$ (Assoziativgesetz)

Beweis.

(a) $[(A + A')B]_{i,k} = \sum\limits_{j=1}^{n} (a_{ij} + a'_{ij})b_{jk} = \sum\limits_{j=1}^{n} a_{ij}b_{jk} + \sum\limits_{j=1}^{n} a'_{ij}b_{jk} = [AB]_{i,k} + [A'B]_{i,k} = [AB + A'B]_{i,k}$.

(b) $[AE_n]_{i,j} = \sum_{k=1}^{n} a_{ik}\delta_{kj} = a_{ij} = \sum_{k=1}^{m} \delta_{ik}a_{kj} = [E_m A]_{i,j}$

(c) $[\lambda(AB)]_{i,k} = \lambda \sum_{j=1}^{n} a_{ij}b_{jk} = \sum_{j=1}^{n} (\lambda a_{ij})b_{kj} = [(\lambda A)B]_{i,k}$

(d) $[(AB)C]_{i,l} = \sum\limits_{k=1}^{p} [AB]_{i,k}c_{kl} = \sum\limits_{k=1}^{p} (\sum\limits_{j=1}^{n} a_{ij}b_{jk})c_{kl} = \sum\limits_{k=1}^{p} \sum\limits_{j=1}^{n} a_{ij}b_{jk}c_{kl} \overset{!!!}{=} \sum\limits_{j=1}^{n} \sum\limits_{k=1}^{p} a_{ij}b_{jk}c_{kl} =$
$= \sum\limits_{j=1}^{n} a_{ij}(\sum\limits_{k=1}^{p} b_{jk}c_{kl}) = \sum\limits_{j=1}^{n} a_{ij}[BC]_{j,l} = [A(BC)]_{i,l}$

Definition.
Wegen der Assoziativität der Matrizenmultiplikation ist folgende Definition für Matrizen $A \in \mathbb{R}^{n\times n}$ sinnvoll:
$A^0 := E_n$ und $A^k := \underbrace{A \cdot A \cdot \ldots \cdot A}_{k \text{ mal}}$ für $k \geq 1$.

Bemerkungen.

1. Nach Lemma 1.4 und Lemma 1.6 gelten viele der üblichen Rechenregeln auch für Matrizen.

   Die Matrizenmultiplikation ist aber **nicht kommutativ**, denn es gilt z.B.:

   $$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

2. Die weiter oben vorgenommene Identifikation von $\lambda \in \mathbb{R}$ und $\big(\lambda\big) \in \mathbb{R}^{1\times 1}$ ist verträglich mit den Rechenoperationen für Matrizen, denn für alle $\lambda, \mu \in \mathbb{R}$ und $A \in \mathbb{R}^{1\times n}$ gilt:
$\big(\lambda\big) + \big(\mu\big) = \big(\lambda + \mu\big), \quad (\lambda)\cdot(\mu) = (\lambda\mu), \quad \big(\lambda\big)\cdot A = \lambda A.$

Definition.

1. $\mathcal{Z} \in \mathrm{EZU}_m \;:\Leftrightarrow\; \mathcal{Z}$ ist eine auf $m \times n$-Matrizen ($n \geq 1$ beliebig) anwendbare elementare Zeilenumformung.

2. Für $\mathcal{Z} \in \mathrm{EZU}_m$ und $A \in \mathbb{R}^{m\times n}$ bezeichne $\mathcal{Z}(A)$ die durch Anwendung von $\mathcal{Z}$ auf A entstehende Matrix.

Lemma 1.7. Für $\mathcal{Z} \in \mathrm{EZU}_m$ gilt:

(a) $\mathcal{Z}(AB) = \mathcal{Z}(A)\cdot B$, falls $A \in \mathbb{R}^{m\times n}$, $B \in \mathbb{R}^{n\times p}$.

(b) $\mathcal{Z}(A) = \mathcal{Z}(E_m)\cdot A$, falls $A \in \mathbb{R}^{m\times n}$.

Beweis:

(a) Seien $b_1, ..., b_p$ die Spalten von B und $c_1, ..., c_p$ die Spalten von AB. Dann sind $\mathcal{Z}(c_1), ..., \mathcal{Z}(c_p)$ die Spalten von $\mathcal{Z}(AB)$ und nach L.1.5a gilt $Ab_j = c_j$, d.h. $b_j \in \mathrm{Lös}(A; c_j)$ für $j = 1, ..., p$. Mit L.1.1 folgt daraus $b_j \in \mathrm{Lös}(\mathcal{Z}(A); \mathcal{Z}(c_j))$, d.h. $\mathcal{Z}(A)b_j = \mathcal{Z}(c_j)$ für $j = 1, ..., p$. L.1.5a liefert schließlich die Behauptung.

(b) $\mathcal{Z}(A) = \mathcal{Z}(E_m A) \overset{\text{(a)}}{=} \mathcal{Z}(E_m)\cdot A$.

§2 Grundbegriffe der Logik und Mengenlehre

Aussagen, logische Verknüpfungen

Eine *Aussage* ist ein "sprachliches Gebilde",das entweder *wahr* oder *falsch* ist.

Ist die Aussage $\mathcal{A}$ wahr (bzw. falsch), so sagt man $\mathcal{A}$ habe den *Wahrheitswert* 1 (bzw. 0).

Statt "$\mathcal{A}$ ist wahr" sagt man auch "$\mathcal{A}$ gilt".

Zur Bildung zusammengesetzter Aussagen verwendet man in der Mathematik gewisse Abkürzungen:

$\mathcal{A}\ \&\ \mathcal{B}$: "$\mathcal{A}$ und $\mathcal{B}$" (Statt "&" schreibt man oft auch "$\wedge$".)

$\mathcal{A} \vee \mathcal{B}$: "$\mathcal{A}$ oder $\mathcal{B}$"

$\mathcal{A} \Rightarrow \mathcal{B}$: "$\mathcal{A}$ impliziert $\mathcal{B}$", "wenn $\mathcal{A}$, dann $\mathcal{B}$", "aus $\mathcal{A}$ folgt $\mathcal{B}$", "$\mathcal{B}$ folgt aus $\mathcal{A}$"

$\mathcal{A} \Leftrightarrow \mathcal{B}$: "$\mathcal{A}$ genau dann, wenn $\mathcal{B}$"

$\neg\mathcal{A}$: "nicht $\mathcal{A}$"

Erläuterungen:

1. Mit $\vee$ (oder) ist stets das "nicht ausschließende oder" gemeint,
   d.h. $\mathcal{A} \vee \mathcal{B}$ ist auch dann wahr, wenn $\mathcal{A}$ und $\mathcal{B}$ beide wahr sind.
2. $\mathcal{A} \Rightarrow \mathcal{B}$ ist genau dann wahr, wenn $\mathcal{B}$ wahr oder (nicht ausschließend!) $\mathcal{A}$ falsch ist.
   (Die Aussage "4 ist Primzahl $\Rightarrow$ $1 < 0$" ist z.B. wahr).
3. $\neg\mathcal{A}$ ist genau dann wahr, wenn $\mathcal{A}$ falsch ist.
4. $\mathcal{A} \Leftrightarrow \mathcal{B}$ ist genau dann wahr, wenn $\mathcal{A}$ und $\mathcal{B}$ denselben Wahrheitswert haben. In diesem Fall nennt man die Aussagen $\mathcal{A}$, $\mathcal{B}$ *äquivalent (zueinander).*
5. $\mathcal{A} \Leftrightarrow \mathcal{B}$ ist äquivalent zu $(\mathcal{A} \Rightarrow \mathcal{B})\ \&\ (\mathcal{B} \Rightarrow \mathcal{A})$, $\mathcal{A} \Rightarrow \mathcal{B}$ ist äquivalent zu $\neg\mathcal{A} \vee \mathcal{B}$.

Die Bedeutung der Symbole $\&$, $\vee, \Rightarrow, \Leftrightarrow, \neg$ läßt sich durch folgende "Wahrheitstafel" beschreiben:

$\mathcal{A}$	$\mathcal{B}$	$\mathcal{A}\ \&\ \mathcal{B}$	$\mathcal{A} \vee \mathcal{B}$	$\mathcal{A} \Rightarrow \mathcal{B}$	$\mathcal{A} \Leftrightarrow \mathcal{B}$	$\neg\mathcal{A}$
1	1	1	1	1	1	0
1	0	0	1	0	0	0
0	1	0	1	1	0	1
0	0	0	0	1	1	1

Ist $\mathcal{A}(\star)$ ein Ausdruck, der eine Aussage darstellt, wenn für $\star$ ein beliebiges Objekt x (einer vorgegebenen Gesamtheit von Objekten) eingesetzt wird, so nennen wir $\mathcal{A}(\star)$ eine *Eigenschaft* und sagen "x hat die Eigenschaft $\mathcal{A}(\star)$" für "$\mathcal{A}(x)$ ist wahr".

Abkürzung:

$\forall x \mathcal{A}(x)$: "für alle x gilt $\mathcal{A}(x)$"

$\exists x \mathcal{A}(x)$: "es gibt ein x, so daß $\mathcal{A}(x)$", "für mindestens ein x gilt $\mathcal{A}(x)$".

Das Symbol $\forall$ ($\exists$) heißt "Allquantor" ("Existenzquantor").

Für beliebige Aussagen $\mathcal{A}, \mathcal{B}$ bzw. Eigenschaften $\mathcal{A}(\star)$ gilt:

$\neg(\mathcal{A}\ \&\ \mathcal{B}) \Leftrightarrow \neg\mathcal{A} \vee \neg\mathcal{B}$, $\qquad \neg\neg\mathcal{A} \Leftrightarrow \mathcal{A}$,

$\neg(\mathcal{A} \vee \mathcal{B}) \Leftrightarrow \neg\mathcal{A} \,\&\, \neg\mathcal{B}$, $\qquad \neg\forall x\mathcal{A}(x) \Leftrightarrow \exists x\neg\mathcal{A}(x)$,

$\neg(\mathcal{A} \Rightarrow \mathcal{B}) \Leftrightarrow \mathcal{A} \,\&\, \neg\mathcal{B}$, $\qquad \neg\exists x\mathcal{A}(x) \Leftrightarrow \forall x\neg\mathcal{A}(x)$.

Einige Sprechweisen:

$\mathcal{B} \Rightarrow \mathcal{A}$ heißt die *Umkehrung* von $\mathcal{A} \Rightarrow \mathcal{B}$;

$\neg\mathcal{B} \Rightarrow \neg\mathcal{A}$ heißt die *Kontraposition* von $\mathcal{A} \Rightarrow \mathcal{B}$;

$\mathcal{A} \Rightarrow \mathcal{B}$: "$\mathcal{A}$ ist hinreichend für $\mathcal{B}$" *oder* "$\mathcal{B}$ ist notwendig für $\mathcal{A}$";

$\mathcal{A} \Leftrightarrow \mathcal{B}$: "$\mathcal{A}$ ist notwendig und hinreichend für $\mathcal{B}$";

$\mathcal{A} :\Leftrightarrow \mathcal{B}$: "$\mathcal{A}$ ist per Definition äquivalent zu $\mathcal{B}$".

Eine wahre Aussage nennt man in der Mathematik einen "Satz" oder ein "Theorem" oder ein "Lemma".

Beweis durch Widerspruch (indirekter Beweis)
Eine Aussage $\mathcal{A} \Rightarrow \mathcal{B}$ kann man u.U. dadurch beweisen, daß man aus der Voraussetzung $\mathcal{A}$ und der Annahme $\neg\mathcal{B}$ einen Widerspruch $\mathcal{C}\&\neg\mathcal{C}$ ableitet. (Begründung: $\mathcal{A} \Rightarrow \mathcal{B}$ ist äquivalent zu $(\mathcal{A} \,\&\, \neg\mathcal{B}) \Rightarrow \mathcal{C}\&\neg\mathcal{C}$.)
Insbesondere kann man $\mathcal{A} \Rightarrow \mathcal{B}$ beweisen, indem man die Gültigkeit der *Kontraposition* $\neg\mathcal{B} \Rightarrow \neg\mathcal{A}$ nachweist.

Abkürzung: $\exists! x\mathcal{A}(x) :\Leftrightarrow \exists x(\mathcal{A}(x) \,\&\, \forall y(\mathcal{A}(y) \Rightarrow x = y)$ (es gibt *genau* ein x mit $\mathcal{A}(x)$)

Es gilt: $\exists! x\mathcal{A}(x) \Leftrightarrow \exists x\forall y(\mathcal{A}(y) \Leftrightarrow x = y)$ und $\exists! x\mathcal{A}(x) \Leftrightarrow \exists x\mathcal{A}(x) \,\&\, \forall x\forall y(\mathcal{A}(x) \,\&\, \mathcal{A}(y) \Rightarrow x = y)$.

Naiver Mengenbegriff nach Cantor (1895):
Unter einer 'Menge' verstehen wir jede Zusammenfassung M von wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens (welche die 'Elemente' von M genannt werden) zu einem Ganzen.

"a ist Element von M" bedeutet also dasselbe wie "a gehört zu M".

Abkürzungen:
$a \in M \;:\Longleftrightarrow\;$ a ist Element von M [a gehört zu M]
$a \notin M \;:\Longleftrightarrow\; \neg(a \in M)$ [a ist nicht Element von M]
$a \neq b \;:\Longleftrightarrow\; \neg(a = b)$ [a ungleich b, a verschieden von b]
Für endlich viele Objekte $a_1, \ldots, a_n$ bezeichnet $\{a_1, \ldots, a_n\}$ diejenige Menge M, die genau die Elemente $a_1, \ldots, a_n$ hat.

Erläuterungen
Jede Menge ist ein Objekt unseres Denkens, kann also selbst wieder Element einer anderen Menge sein.

Bei der Zusammenfassung von Objekten zu einer Menge kommt es nicht auf die Reihenfolge der Elemente an, und auch nicht darauf, ob ein Element nur einmal oder mehrmals vorkommt. Anders gesagt, eine Menge M ist eindeutig bestimmt, wenn festgelegt ist, welche Objekte a Element von M sind und welche nicht.

Für Mengen M, N gilt also: $\boxed{M = N \iff \forall x(x \in M \Leftrightarrow x \in N)}$ (Extensionalität).

Beispiele:
1. $M := \{1, 0, \{3, \{0\}\}, 4\}$ ist eine Menge. Die vier Elemente von M sind $1, 0, \{3, \{0\}\}, 4$.
2. Es gilt $\{3, 6, 9, 12\} = \{12, 3, 3, 6, 9, 12\} \neq \{3, 3, 9, 12\}$.

Definition.

Ist M eine Menge und $\mathcal{A}(\star)$ eine Eigenschaft, so bezeichnet $\{x \in M : \mathcal{A}(x)\}$ die Menge aller Elemente x von M, für die die Aussage $\mathcal{A}(x)$ wahr ist (gilt). Wenn M aus dem Zusammenhang hervorgeht, so schreiben manchmal auch nur $\{x : \mathcal{A}(x)\}$ statt $\{x \in M : \mathcal{A}(x)\}$.

Für jedes Objekt a gilt also: $\boxed{a \in \{x \in M : \mathcal{A}(x)\} \Leftrightarrow a \in M \,\&\, \mathcal{A}(a)}$.

Ist $t(x)$ für alle $x \in M$ definiert, so sei $\boxed{\{t(x) : x \in M\} := \{y : \exists x \in M(y = t(x))\}}$.

Zum Beispiel ist $\{2n{+}1 : n \in \mathbb{N}\}$ die Menge aller ungeraden natürlichen Zahlen.

Analog definiert man $\{t(x) : \mathcal{A}(x)\}$ bzw. $\{t(x_1, ..., x_n) : \mathcal{A}(x_1, ..., x_n)\}$. Beispiel: $\{2^n \cdot 3^x : n \in \mathbb{N} \,\&\, x \in \mathbb{Z}\}$.

Abkürzungen:

$\forall x \in M\, \mathcal{A}(x) \;:\Longleftrightarrow\; \forall x(x \in M \Rightarrow \mathcal{A}(x))$

$\exists x \in M\, \mathcal{A}(x) \;:\Longleftrightarrow\; \exists x(x \in M \,\&\, \mathcal{A}(x))$

$\emptyset := \{x : x \neq x\}$ (die *leere Menge*)

Es gilt: $\neg\forall x \in M\mathcal{A}(x) \iff \exists x \in M\neg\mathcal{A}(x)$ und $\neg\exists x \in M\mathcal{A}(x) \iff \forall x \in M\neg\mathcal{A}(x)$.

Bemerkungen.

Die leere Menge $\emptyset$ besitzt überhaupt keine Elemente.

Jede Aussage der Form $\forall x \in M\, \mathcal{A}(x)$ mit $M = \emptyset$ ist wahr.

04.11.2009

Es gilt $\{a_1, ..., a_n\} = \{x : x = a_1 \vee \ldots \vee x = a_n\}$.

Man beachte:

Die Menge $\{a\}$ ist nicht dasselbe wie das Objekt a; auch nicht, wenn a ebenfalls eine Menge ist.

Definition. Seien X, Y Mengen.

X heißt *Teilmenge von* Y (in Zeichen $X \subseteq Y$), falls jedes Element von X auch Element von Y ist:

$\boxed{X \subseteq Y \;:\Longleftrightarrow\; \forall x \in X(x \in Y)}$. Offenbar gilt: $\boxed{X = Y \Leftrightarrow X \subseteq Y \,\&\, Y \subseteq X}$.

Für $X \subseteq Y$ sagt man auch "X ist in Y enthalten" oder "Y umfaßt X".

Abkürzung: $X \not\subseteq Y \;:\Longleftrightarrow\;$ X ist nicht Teilmenge von Y.

$X \subsetneqq Y \;:\Longleftrightarrow\; X \subseteq Y \,\&\, X \neq Y$ (X ist *echte Teilmenge* von Y)

Es gilt:

(a) $X \not\subseteq Y \;\Leftrightarrow\; \exists x \in X(x \notin Y)$.

(b) $X \neq Y \;\Leftrightarrow\; X \not\subseteq Y \vee Y \not\subseteq X$ $[\, \exists x \in X(x \notin Y) \vee \exists x \in Y(x \notin X)\,]$.

Definition. Für Mengen X, Y definieren wir:

$X \cap Y := \{x : x \in X \,\&\, x \in Y\}$ (Durchschnitt von X und Y)

$X \cup Y := \{x : x \in X \vee x \in Y\}$ (Vereinigung von X und Y)

$X \setminus Y := \{x : x \in X \,\&\, x \notin Y\} = \{x \in X : x \notin Y\}$ (Differenz von X und Y, X ohne Y)

Man beachte: Im allgemeinen gilt *nicht* $X \setminus Y = Y \setminus X$!

Beispiele:
$\{1,2,3\} \cap \{2,3,13,14\} = \{2,3\}$,
$\{0,1\} \cap \{2,3\} = \emptyset$,
$\{1,2,3\} \cup \{2,3,13,14\} = \{1,2,3,13,14\}$
$\{1,2,3\} \setminus \{2,3,13,14\} = \{1\}$
$\{2,3,13,14\} \setminus \{1,2,3\} = \{13,14\}$
$\{0,1\} \setminus \{2,3\} = \{0,1\}$
$\{0,1,1,0\} \setminus \{2,0,3,1\} = \emptyset$.

Lemma 2.1.
(a) $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$.
(b) $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$.
(c) $M \setminus (M \setminus X) = M \cap X$.
(d) $M \setminus (X \cup Y) = (M \setminus X) \cap (M \setminus Y) = (M \setminus X) \setminus Y$.
(e) $M \setminus (X \cap Y) = (M \setminus X) \cup (M \setminus Y)$.

Beweis:
(a) Für beliebiges x ist die Äquivalenz der Aussagen "$x \in X \cap (Y \cup Z)$" und "$x \in (X \cap Y) \cup (X \cap Z)$" zu beweisen. Sei also x gegeben.
Fall 1: $x \in X$. Dann: $x \in X \cap (Y \cup Z) \Leftrightarrow x \in Y \cup Z \Leftrightarrow x \in (X \cap Y) \cup (X \cap Z)$.
Fall 2: $x \notin X$. Dann: $x \notin X \cap (Y \cup Z)$ und $x \notin (X \cap Y) \cup (X \cap Z)$.

(c) Fall 1: $x \in M$. Dann: $x \in M \setminus (M \setminus X) \Leftrightarrow x \notin M \setminus X \Leftrightarrow x \in X \Leftrightarrow x \in M \cap X$.
Fall 2: $x \notin M$. Dann $x \notin M \setminus (M \setminus X)$ und $x \notin M \cap X$.

(d) $x \in M \setminus (X \cup Y) \Leftrightarrow x \in M \;\&\; x \notin X \cup Y \Leftrightarrow x \in M \;\&\; (x \notin X \;\&\; x \notin Y) \Leftrightarrow$
$\Leftrightarrow (x \in M \;\&\; x \notin X) \;\&\; (x \in M \;\&\; x \notin Y) \Leftrightarrow x \in M \setminus X \;\&\; x \in M \setminus Y \Leftrightarrow x \in (M \setminus X) \cap (M \setminus Y)$.
$x \in M \setminus (X \cup Y) \overset{\text{siehe oben}}{\Leftrightarrow} (x \in M \;\&\; x \notin X) \;\&\; x \notin Y \Leftrightarrow x \in M \setminus X \;\&\; x \notin Y \Leftrightarrow x \in (M \setminus X) \setminus Y$.

Definition. Unter dem *(kartesischen) Produkt* $X \times Y$ zweier Mengen X, Y versteht man die Menge aller *geordneten Paare* (x, y) mit $x \in X$, $y \in Y$: $X \times Y := \{(x, y) : x \in X \;\&\; y \in Y\}$.

Die Gleichheit geordneter Paare ist definiert durch: $(x, y) = (x', y') :\Leftrightarrow x = x' \;\&\; y = y'$.

Analog definiert man für beliebiges $n \geq 1$:

$X_1 \times \ldots \times X_n := \{(x_1, ..., x_n) : x_1 \in X_1 \;\&\; \ldots \;\&\; x_n \in X_n\}$ (*kartesisches Produkt*)

Die Elemente von $X_1 \times \ldots \times X_n$ heißen *n-Tupel*.

Die Gleichheit von n-Tupeln ist definiert durch: $(x_1, \ldots, x_n) = (x'_1, \ldots, x'_n) :\Leftrightarrow x_1 = x'_1 \;\&\; \ldots \;\&\; x_n = x'_n$.

Eine Menge von n-Tupeln nennt man eine *n-stellige Relation.*

Abkürzung: $X^n := \underbrace{X \times \ldots \times X}_{n \text{ mal}}$ $(n \geq 1)$.

Jede Teilmenge von X^n nennt man eine *n-stellige Relation auf X*.

Definition. Seien X, Y Mengen.

Eine *Abbildung* (oder *Funktion*) von X nach Y, ist eine Vorschrift f, die jedem $x \in X$ genau ein Element $f(x) \in Y$ zuordnet. Man schreibt dafür $f : X \to Y,\ x \mapsto f(x)$.

$\mathrm{Def}(f) := X$ heißt der *Definitionsbereich* oder die *Quelle*, und Y das *Ziel* von f.

Ist $x \in X$, so nennt man $f(x)$ das *Bild von x unter f* oder den *Funktionswert* von f an der Stelle x.

Für $f : X \to Y$ und $g : X' \to Y'$ gilt: $\boxed{f = g \iff X = X' \ \&\ Y = Y' \ \&\ \forall x \in X(\, f(x) = g(x)\,)}$.

Eine spezielle Abbildung ist für jede Menge X die *identische Abbildung von X:* $\mathrm{id}_X : X \to X,\ x \mapsto x$.

Mit $\mathrm{Abb}(X, Y)$ bezeichnen wir die Menge aller Abbildungen von X nach Y.

Definition. Sei $f : X \to Y$ und $M \subseteq X$, $N \subseteq Y$.

$f(M) := \{f(x) : x \in M\} = \{y \in Y : \exists x \in M(f(x) = y)\}$ *(Bild von M unter f)*;

$f^{-1}(N) := \{x \in X : f(x) \in N\}$ *(Urbild von N unter f)*.

09.11.2009

$\mathrm{Im}(f) := f(X)$ heißt *Bild* oder *Wertemenge* von f.

$\mathrm{Graph}(f) := \{(x, f(x)) : x \in X\} = \{(x, y) \in X \times Y : y = f(x)\}$ heißt *Graph* von f.

Definition. Für $f : X \to Y$ und $g : Y \to Z$ definiert man die *Hintereinanderausführung* oder *Komposition* $g \circ f$ von g und f durch $g \circ f : X \to Z,\ (g \circ f)(x) := g(f(x))$.

(Man beachte die Reihenfolge $g \circ f$: g wird nach f ausgeführt.)

Für $g \circ f$ sagt man auch g *komponiert mit* f.

Bemerkung.

Für $f : X \to Y,\ \ g : Y \to Z,\ \ h : Z \to M$ gilt:

(i) $h \circ (g \circ f) = (h \circ g) \circ f$ (Assoziativität)

(ii) $\mathrm{id}_Y \circ f = f = f \circ \mathrm{id}_X$.

Definition. Sei $f : X \to Y$.

f ist *injektiv* $:\Leftrightarrow \forall x, x' \in X(x \neq x' \Rightarrow f(x) \neq f(x'))$ $[\Leftrightarrow \forall x, x' \in X(f(x) = f(x') \Rightarrow x = x')]$

f ist *surjektiv* $:\Leftrightarrow \forall y \in Y \exists x \in X(\, f(x) = y\,)$ [d.h. $f(X) = Y$]

f ist *bijektiv* $:\Leftrightarrow$ f ist injektiv und surjektiv [d.h. $\forall y \in Y \exists! x \in X(\, f(x) = y\,)$].

Statt “f ist surjektiv” sagt man auch “f ist eine Funktion von X *auf* Y”.

Statt “f ist injektiv (surjektiv, bijektiv)” sagt man auch “f ist eine Injektion (Surjektion, Bijektion)”.

Bemerkung. Für $f : X \to Y$ und $g : Y \to X$ gilt: $g \circ f = \mathrm{id}_X \implies f$ injektiv und g surjektiv.

Beweis:

1. $x, x' \in X \ \&\ f(x) = f(x') \ \Rightarrow\ x = \mathrm{id}_X(x) = (g \circ f)(x) = g(f(x)) = g(f(x')) = (g \circ f)(x') = \mathrm{id}_X(x') = x'$.
2. $\forall x \in X(\, f(x) \in Y \ \&\ g(f(x)) = (g \circ f)(x) = \mathrm{id}_X(x) = x) \ \Rightarrow\ \forall x \in X \exists y \in Y(g(y) = x)$.

Beispiele. Sei $\mathbb{R}_+ := \{x \in \mathbb{R} : 0 \leq x\}$.

$f_0 : \mathbb{R} \to \mathbb{R},\ x \mapsto x^2$ ist weder injektiv noch surjektiv;

$f_1 : \mathbb{R} \to \mathbb{R}_+,\ x \mapsto x^2$ ist surjektiv, aber nicht injektiv;

$f_2 : \mathbb{R}_+ \to \mathbb{R},\ x \mapsto x^2$ ist injektiv, aber nicht surjektiv;

$f_3 : \mathbb{R}_+ \to \mathbb{R}_+,\ x \mapsto x^2$ ist bijektiv.

Definition (Umkehrabbildung).

Sei $f : X \to Y$ bijektiv. Dann existiert zu jedem $y \in Y$ genau ein $x \in X$ mit $f(x) = y$; dieses x nennt man auch *Urbild von y bzgl. f*. Die Funktion, welche jedem $y \in Y$ sein Urbild x bzgl. f zuordnet, nennt man *die Umkehrfunktion von f* und bezeichnet sie mit $f^{-1} : Y \to X$.

Lemma 2.2. Für bijektives $f : X \to Y$ gilt:

(a) $f^{-1} : Y \to X$ ist bijektiv & $f^{-1} \circ f = \mathrm{id}_X$ & $f \circ f^{-1} = \mathrm{id}_Y$;

(b) $\mathrm{Graph}(f^{-1}) = \{(y, x) \in Y \times X : (x, y) \in \mathrm{Graph}(f)\}$;

(c) $\forall x \in X, y \in Y (\, f(x) = y \;\Leftrightarrow\; x = f^{-1}(y)\,)$;

(d) $(f^{-1})^{-1} = f$;

(e) Ist auch $g : Y \to Z$ bijektiv, so $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Bemerkung. Ist $f : X \to Y$ bijektiv und $N \subseteq Y$, so hat $f^{-1}(N)$ zwei Bedeutungen, die aber übereinstimmen:

1. das Urbild von N unter f, i.e. $f^{-1}(N) = \{x \in X : f(x) \in N\}$,
2. das Bild von N unter f^{-1}, i.e. $f^{-1}(N) = \{f^{-1}(y) : y \in N\}$.

(Für alle $x \in X$ gilt: $f(x) \in N \Leftrightarrow \exists y \in N(f(x) = y) \Leftrightarrow \exists y \in N(x = f^{-1}(y))$.)

11.11.2009

Lemma 2.3. Sei $f : X \to Y$ und $M_0, M_1 \subseteq X$, $N_0, N_1 \subseteq Y$.

(a) $f(M_0 \cup M_1) = f(M_0) \cup f(M_1)$ und $f(M_0 \cap M_1) \subseteq f(M_0) \cap f(M_1)$.

(b) $f^{-1}(N_0 \cup N_1) = f^{-1}(N_0) \cup f^{-1}(N_1)$ und $f^{-1}(N_0 \cap N_1) = f^{-1}(N_0) \cap f^{-1}(N_1)$.

(c) Ist f injektiv, so gilt $f(M_0) \cap f(M_1) = f(M_0 \cap M_1)$.

Beweis:

(a) 1. $f(M_0 \cup M_1) = f(M_0) \cup f(M_1)$: siehe Übungen.

2. $f(M_0 \cap M_1) = \{y : \exists x(x \in M_0 \;\&\; x \in M_1 \;\&\; y = f(x))\} \overset{!!!}{\subseteq}$
$\{y : \exists x(x \in M_0 \;\&\; y = f(x)) \;\&\; \exists x(x \in M_1 \;\&\; y = f(x))\} =$
$\{y : \exists x(x \in M_0 \;\&\; y = f(x))\} \cap \{y : \exists x(x \in M_1 \;\&\; y = f(x))\} = f(M_0) \cap f(M_1)$.

(b) siehe Übungen.

(c) $y \in f(M_0) \cap f(M_1) \;\Rightarrow\; \exists x_0 \in M_0(y = f(x_0)) \;\&\; \exists x_1 \in M_1(y = f(x_1)) \;\Rightarrow$
$\Rightarrow\; \exists x_0, x_1(x_0 \in M_0 \;\&\; x_1 \in M_1 \;\&\; f(x_0) = y = f(x_1)) \overset{\text{f injektiv}}{\Rightarrow}$
$\Rightarrow\; \exists x(x \in M_0 \;\&\; x \in M_1 \;\&\; y = f(x)) \;\Rightarrow\; y \in f(M_0 \cap M_1)$.

Bemerkung.

1. Formal gesehen ist jede Matrix $A \in \mathbb{R}^{m \times n}$ eine Abbildung $A : \{1, ..., m\} \times \{1, ..., n\} \to \mathbb{R}$, $(i, j) \mapsto a_{ij}$.
2. Eine Abbildung $f : I \to X$, $\iota \mapsto x_\iota$ (wobei I eine beliebige Menge ist) nennt man auch eine *Familie* und bezeichnet sie mit $(x_\iota)_{\iota \in I}$. Die Menge I nennt man auch *Indexmenge* der Familie. Ist $I = \mathbb{N}$, so nennt man f eine *(unendliche) Folge*.

Definitionen.

- Ist $\mathcal{M}$ eine Menge von Mengen, so sei

  $\bigcup \mathcal{M} := \{x : \exists X \in \mathcal{M}(x \in X)\}$ und (falls $\mathcal{M} \neq \emptyset$) $\bigcap \mathcal{M} := \{x : \forall X \in \mathcal{M}(x \in X)\}$.

- Ist $(X_\iota)_{\iota\in I}$ eine Familie von Mengen, so sei

  $\bigcup\limits_{\iota\in I} X_i := \bigcup\{X_\iota : \iota \in I\} \ = \{x : \exists\iota \in I(x \in X_\iota)\}$,

  $\bigcap\limits_{\iota\in I} X_i := \bigcap\{X_\iota : \iota \in I\} \ = \{x : \forall\iota \in I(x \in X_\iota)\} \ \ (I \neq \emptyset)$.

- Für jede Menge X sei $\mathcal{P}(X) := \{Y : Y \subseteq X\}$ *(Potenzmenge von X)*.

- Für $f : X \to X$ definiert man $f^n : X \to X$ rekursiv durch: $f^0 := \mathrm{id}_X$, $f^{n+1} := f \circ f^n$.

  Offenbar gilt dann $f^{n+m} = f^n \circ f^m$.

- Ist $f : X \to Y$ und $M \subseteq X$, so nennt man $f|M : M \to Y$, $x \mapsto f(x)$ die *Einschränkung* (oder *Beschränkung*) von f auf M.

§3 Gruppen, Ringe, Körper

Definition. Sei G eine Menge und $\bullet : G \times G \to G$, $(x, y) \mapsto x \bullet y$ eine Abbildung.

$(G, \bullet)$ (oder kurz G) heißt *Gruppe*, falls gilt:

(G1) $\forall x, y, z \in G(\, x \bullet (y \bullet z) = (x \bullet y) \bullet z\,)$ (Assoziativgesetz)

(G2) Es gibt ein $e \in G$, so daß

(i) $\forall x \in G(\, e \bullet x = x\,)$

(ii) $\forall x \in G \exists y \in G(\, y \bullet x = e\,)$.

Hierbei heißt $\bullet$ auch *Produkt* oder *(innere) Verknüpfung* auf G, und e heißt *neutrales Element von* G.

Die Gruppe $(G, \bullet)$ heißt *kommutativ* oder *abelsch*, falls $x \bullet y = y \bullet x$ für alle $x, y \in G$.

Schreibweise: $xy := x \bullet y$.

Bemerkung. Ist G eine Gruppe mit neutralem Element e, so gilt:

(1) $\forall x, y \in G(yx = e \;\Rightarrow\; xy = e)$.

(2) $\forall x \in G(xe = x)$.

(3) $\tilde{e} \in G \;\&\; \forall x \in G(\tilde{e}x = x) \;\Rightarrow\; e = \tilde{e}$ *(Eindeutigkeit des neutralen Elements).*

(4) $\forall x \in G \exists! y \in G(yx = e)$.

Beweis:

(1) Sei $yx = e$. Nach (G2ii) existiert ein y' mit $y'y = e$. Es folgt:
$xy \overset{(G2i)}{=} e(xy) = (y'y)(xy) \overset{(G1)}{=} y'(y(xy)) \overset{(G1)}{=} y'((yx)y) = y'(ey) \overset{(G2i)}{=} y'y = e$.

(2) Nach (G2ii) existiert ein $x' \in G$ mit $x'x = e$ und – wegen (1) – $xx' = e$. Daraus folgt $xe = xx'x = ex = x$.

(3) $e = \tilde{e}e \overset{(2)}{=} \tilde{e}$.

(4) $yx = e \;\&\; y'x = e \overset{(1)}{\Rightarrow} xy = e \;\&\; y'x = e \;\Rightarrow\; y \overset{(G2i)}{=} ey = (y'x)y \overset{(G1)}{=} y'(xy) = y'e \overset{(2)}{=} y'$.

Definition. Sei $(G, \bullet)$ eine Gruppe mit neutralem Element e, und sei $x \in G$.

1. Das nach (4) eindeutig bestimmte $y \in G$ mit $yx = e$ heißt *Inverses von* x und wird mit x^{-1} bezeichnet.
2. Für $n \in \mathbb{N}$ definiert man x^n rekursiv durch: $x^0 := e$, $x^{n+1} := x^n \bullet x$.
   Ferner setzt man $x^{-n} := (x^n)^{-1}$ für $n \geq 1$. Damit ist x^p für alle $p \in \mathbb{Z}$ definiert.

Lemma 3.1. Ist G eine Gruppe (mit neutralem Element e), so gilt für alle $x, y \in G$:

(a) $xy = e \;\Rightarrow\; x^{-1} = y \;\&\; y^{-1} = x$.

(b) $(xy)^{-1} = y^{-1}x^{-1} \;\&\; (x^{-1})^{-1} = x$.

(c) $x^{p+q} = x^p x^q \;\&\; x^{pq} = (x^p)^q \quad (\forall p, q \in \mathbb{Z})$.

Beweis:

(a) $xy = e \;\Rightarrow\; y = ey = x^{-1}xy = x^{-1}e = x^{-1} \;\&\; x = xe = xyy^{-1} = ey^{-1} = y^{-1}$.

(b) $(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = xx^{-1} = e \overset{(a)}{\Rightarrow} (xy)^{-1} = y^{-1}x^{-1}$. $\quad x^{-1}x = e \overset{(a)}{\Rightarrow} (x^{-1})^{-1} = x$.

(c) Beweis von $\forall p, q \in \mathbb{Z}(x^{p+q} = x^p x^q)$.

1. $x^{m+n} = x^m x^n$ [Ind. nach n: $x^{m+0} = x^m = x^m e = x^m x^0$; $x^{m+n+1} = x^{m+n}x \overset{\text{I.V.}}{=} x^m x^n x = x^m x^{n+1}$.]

2. $x^{-m+n} = x^{-m}x^n$:

2.1. $-m+n \geq 0$: $x^{-m+n} = x^{-m}x^m x^{-m+n} \overset{1.}{=} x^{-m}x^n$.
2.2. $-m+n < 0$: $x^{-m+n} = (x^{-n+m})^{-1} \overset{2.1.}{=} (x^{-n}x^m)^{-1} = (x^m)^{-1}(x^{-n})^{-1} = x^{-m}x^n$.
3. $\forall p \in \mathbb{Z}(x^{p+n} = x^p x^n)$: folgt aus 1. und 2.
4. $x^{p-n} = x^{p-n}x^n x^{-n} \overset{3.}{=} x^{p-n+n}x^{-n} = x^p x^{-n}$.

Beispiel. Sei M eine Menge und $\mathbf{S}(M)$ die Menge der bijektiven Abbildungen von M auf sich selbst. Dann ist $(\mathbf{S}(M), \circ)$, wobei $\circ$ die Komposition von Abbildungen bezeichnet, eine Gruppe. Man nennt sie die *symmetrische Gruppe* der Menge M. Neutrales Element ist die Identität $\mathrm{id}_M : M \to M$, und das inverse Element zu $f \in \mathbf{S}(M)$ ist die Umkehrabbildung f^{-1}. Die Elemente von $\mathbf{S}(M)$ heißen *Permutationen.*

Bemerkung. Hat M mindestens drei Elemente, so ist $\mathbf{S}(M)$ nicht abelsch.
Sei z.B. $M = \{0, 1, 2\}$ und $f, g \in \mathbf{S}(M)$ mit $f(0) = 0$, $f(1) = 2$, $f(2) = 1$, $g(0) = 1$, $g(1) = 0$, $g(2) = 2$.
Dann gilt $(g \circ f)(0) = 1 \neq 2 = (f \circ g)(0)$, also $g \circ f \neq f \circ g$.

16.11.2009

Kürzungsregel. In jeder Gruppe G gilt: Wenn $xz = yz$ oder $zx = zy$, dann $x = y$.

Beispiele. Kommutative Gruppen sind u.a.:
$(\mathbb{Z}, +)$ (neutrales Element ist 0, das Inverse von $a \in \mathbb{Z}$ ist $-a$)
$(\mathbb{R}, +)$ (neutrales Element ist 0, das Inverse von $a \in \mathbb{R}$ ist $-a$)
$(\mathbb{R}^*, \cdot)$ (neutrales Element ist 1, das Inverse von $a \in \mathbb{R}^*$ ist $\frac{1}{a}$), wobei $\mathbb{R}^* := \mathbb{R} \setminus \{0\}$.

Bemerkung. Das Pluszeichen $+$ wird nur bei abelschen Gruppen zur Bezeichnung der Gruppenverknüpfung verwendet. Das neutrale Element wird dann mit 0, und das inverse Element zu a mit $-a$ bezeichnet.

Definition.
Eine Matrix $A \in \mathbb{R}^{n\times n}$ heißt *invertierbar*, wenn es ein $A' \in \mathbb{R}^{n\times n}$ mit $A \cdot A' = A' \cdot A = E_n$ gibt.

Lemma 3.2.
Die Menge $\mathrm{GL}(n; \mathbb{R}) := \{A \in \mathbb{R}^{n\times n} : A \text{ invertierbar }\}$ mit der Matrizenmultiplikation als Verknüpfung ist eine Gruppe mit neutralem Element E_n. Sie heißt die *allgemeine lineare Gruppe.*

Das Inverse von $A \in \mathrm{GL}(n; \mathbb{R})$ wird mit A^{-1} bezeichnet.

Beweis :

1. Zuerst muß gezeigt werden, daß $\mathrm{GL}(n; \mathbb{R})$ abgeschlossen unter $\cdot$ ist,
d.h. daß $\forall A, B \in \mathrm{GL}(n; \mathbb{R})(A \cdot B \in \mathrm{GL}(n; \mathbb{R}))$ gilt: $AA' = A'A = E$ & $BB' = B'B = E \Rightarrow$
$\Rightarrow (AB)(B'A') = A(BB')A' = AEA' = E$ & $(B'A')(AB) = B'(A'A)B = B'EB = E$.

2. Assoziativgesetz: Lemma 1.6d.

3.1. $E_n A = A$.

3.2. Zu jedem $A \in \mathrm{GL}(n; \mathbb{R})$ existiert ein $A' \in \mathbb{R}^{n\times n}$ mit $A'A = AA' = E_n$.
Offenbar gilt dann auch $A' \in \mathrm{GL}(n; \mathbb{R})$.

Definition. Sei $(G, \bullet)$ eine Gruppe mit neutralem Element e, und sei $H \subseteq G$.
H heißt *Untergruppe* von $G :\iff e \in H$ & $\forall x, y \in H(x \bullet y \in H)$ & $\forall x \in H(x^{-1} \in H)$.

Bemerkung. Ist $(G, \bullet)$ eine Gruppe und $H \subseteq G$, so ist H genau dann eine Untergruppe von $(G, \bullet)$, wenn H mit der Einschränkung von $\bullet$ auf H eine Gruppe ist. In diesem Fall stimmt das neutrale Element von H mit dem neutralen Element von G überein, und das inverse Element von x in H ist gleich dem inversen Element von x in G.

Definition. Seien $(G, \bullet)$ und $(G', \bullet')$ Gruppen.

Eine Abbildung $\varphi : G \to G'$ heißt *(Gruppen)homomorphismus*, falls $\varphi(x \bullet y) = \varphi(x) \bullet' \varphi(y)$ für alle $x, y \in G$. Ein bijektiver Homomorphismus heißt Isomorphismus. G und G' heißen *isomorph* zueinander (in Zeichen $G \cong G'$), falls es einen Isomorphismus $\varphi : G \to G'$ gibt.

Lemma 3.3.

Für jeden Gruppenhomomorphismus $\varphi : G \to G'$ gilt:

(a) $\varphi(e) = e'$, wobei e bzw. e' das neutrale Element in G bzw. G' sei.

(b) $\varphi(x^{-1}) = \varphi(x)^{-1}$ für alle $x \in G$.

(c) φ Isomorphismus $\Rightarrow$ φ^{-1} Isomorphismus.

Beweis:

(a) $\varphi(e) \bullet' \varphi(e) = \varphi(e \bullet e) = \varphi(e) = \varphi(e) \bullet' e' \overset{\text{Kuerzungsregel}}{\Rightarrow} \varphi(e) = e'$.

(b) $\varphi(x) \bullet' \varphi(x^{-1}) = \varphi(x \bullet x^{-1}) = \varphi(e) = e' \Rightarrow \varphi(x)^{-1} = \varphi(x^{-1})$.

(c) Zu zeigen: $\varphi^{-1}(x \bullet' y) = \varphi^{-1}(x) \bullet \varphi^{-1}(y)$ für alle $x, y \in G'$.

$\varphi(\varphi^{-1}(x) \bullet \varphi^{-1}(y)) = \varphi(\varphi^{-1}(x)) \bullet' \varphi(\varphi^{-1}(y)) = x \bullet' y \overset{2.2c}{\Longrightarrow} \varphi^{-1}(x) \bullet \varphi^{-1}(y) = \varphi^{-1}(x \bullet' y)$.

Beispiele.

1. Ist $(G, \bullet)$ eine Gruppe und $a \in G$, so ist die Abbildung $\mathbb{Z} \to G$, $p \mapsto a^p$ ein Homomorphismus von $(\mathbb{Z}, +)$ auf $(G, \bullet)$.
2. Für $1 \neq a \in \mathbb{R}_+^* := \{x \in \mathbb{R} : x > 0\}$ ist die Abbildung $\mathbb{R} \to \mathbb{R}_+^*$, $x \mapsto a^x$ ein Isomorphismus von $(\mathbb{R}, +)$ auf $(\mathbb{R}_+^*, \cdot)$.

18.11.2009

Definition. Eine Menge R zusammen mit zwei Verknüfungen

$+ : R \times R \to R$, $(x, y) \mapsto x + y$ und $\cdot : R \times R \to R$, $(x, y) \mapsto x \cdot y$,

heißt *Ring*, wenn folgendes gilt:

(R1) $(R, +)$ ist eine abelsche Gruppe.

(R2) $\forall x, y, z \in R(\, x \cdot (y \cdot z) = (x \cdot y) \cdot z \,)$ *(Assoziativität der Multiplikation)*

(R3) $\forall x, y, z \in R(\, x \cdot (y + z) = x \cdot y + x \cdot z \;\&\; (x + y) \cdot z = x \cdot z + y \cdot z \,)$ *(Distributivgesetze)*

Ein Ring R heißt *kommutativ*, wenn $x \cdot y = y \cdot x$ für alle $x, y \in R$.

Ein Element $1 \in R$ heißt *Einselement*, wenn $1 \cdot x = x \cdot 1 = x$ für alle $x \in R$.

Ein Ring R heißt *nullteilerfrei*, wenn gilt $\forall x, y \in R(\, x \cdot y = 0 \Rightarrow x = 0 \vee y = 0 \,)$.

Man verwendet die üblichen Regeln zur Klammerersparnis, insbesondere *"Punkt vor Strich"* (z.B. $x{\cdot}y{+}z{\cdot}d = (x \cdot y) + (z \cdot d)$). Außerdem schreibt man meist xy statt $x \cdot y$.

Lemma 3.4. Ist $(R, +, \cdot)$ ein Ring, so gilt für alle $x, y \in R$:

(a) $0 \cdot x = x \cdot 0 = 0$,

(b) $x(-y) = (-x)y = -(xy)$ und $(-x)(-y) = xy$.

Beweis:

(a) $0 \cdot x = (0 + 0) \cdot x = 0 \cdot x + 0 \cdot x \Rightarrow 0 \cdot x = 0$.

(b) $xy + (-x)y = (x + (-x))y = 0{\cdot}y = 0$ und $(-x)(-y) = -(x(-y)) = -(-(xy)) = xy$.

Beispiele.

(1) Die Mengen $\mathbb{Z}$ der ganzen Zahlen, $\mathbb{Q}$ der rationalen Zahlen und $\mathbb{R}$ der reellen Zahlen sind zusammen mit der üblichen Addition und Multiplikation kommutative Ringe.

(2) Ist I eine Menge und R die Menge aller Abbildungen von I in $\mathbb{R}$, so werden durch
$(f+g)(x) := f(x)+g(x)$ und $(f\cdot g)(x) := f(x)\cdot g(x)$
Verknüpfungen $+$ und $\cdot$ auf R erklärt, und R wird damit zu einem kommutativen Ring.

(3) $\mathbb{R}^{n\times n}$ mit der in §1 definierten Addition und Multiplikation von Matrizen ist ein Ring.

Definition (Körper).

Ein kommutativer Ring K mit Einselement $1 \neq 0$ heißt *Körper*, wenn gilt: $\forall x \in K \setminus \{0\} \exists x' \in K (x'x = 1)$

Bemerkung.

1. Jeder Körper ist nullteilerfrei.
2. Ist $(K,+,\cdot)$ ein Körper, so ist $(K^*,\cdot)$ mit $K^* := K \setminus \{0\}$ eine abelsche Gruppe.

Beispiele. $\mathbb{Q}$ (rationale Zahlen), $\mathbb{R}$ (reelle Zahlen) und $\mathbb{C}$ (komplexe Zahlen) sind Körper.

Definition.

Die *Charakteristik* $\operatorname{char}(K)$ eines Körpers K wird definiert durch

$$\operatorname{char}(K) := \begin{cases} 0 & \text{falls } n{\cdot}1_K \neq 0_K \text{ für alle } n \geq 1 \\ \min\{n \geq 1 : n{\cdot}1_K = 0_K\} & \text{sonst} \end{cases}, \quad \text{wobei } n{\cdot}1_K := \underbrace{1_K + \ldots + 1_K}_{n-\text{mal}}.$$

Lemma 3.5. Die Charakteristik eines Körpers ist entweder 0 oder eine Primzahl.

Beweis:

Annahme: $\operatorname{char}(K) = n = l{\cdot}m \neq 0$ mit $1 < l, m < n$. Wie man leicht nachrechnet, ist dann $(l\cdot 1_K)(m{\cdot}1_K) = n{\cdot}1_K$. Aus $n{\cdot}1_K = 0_K$ folgt also $l{\cdot}1_K = 0_K$ oder $m{\cdot}1_K = 0_K$ im Widerspruch zur Minimalität von n.

Beispiel. $\mathbb{F}_2 := (\{0,1\},+,\cdot)$ mit $0+0=0$, $0+1=1+0=1$, $1+1=0$, $0{\cdot}0=0$, $0{\cdot}1=1{\cdot}0=0$, $1\cdot 1=1$ ist ein Körper der Charakteristik 2.

Lemma 3.6. $\sqrt{2} \notin \mathbb{Q}$, d.h. es gibt keine rationale Zahl a mit $a^2 = 2$.

Beweis: Annahme: $a \in \mathbb{Q}$ und $a^2 = 2$. Dann existieren $p, q \in \mathbb{Z}\setminus\{0\}$ mit $a = p/q$ und p, q nicht beide gerade. Aus $a^2 = 2$ folgt nun $p^2 = 2q^2$. Folglich ist p^2 gerade und somit auch p gerade, d.h. es existiert $\tilde{p} \in \mathbb{Z}$ mit $p = 2\tilde{p}$. Es folgt $4\tilde{p}^2 = 2q^2$ und weiter $2\tilde{p}^2 = q^2$. Also ist auch q gerade. Widerspruch.

Lemma 3.7.

$\mathbb{Q}(\sqrt{2}) := \{a + b\sqrt{2} : a, b \in \mathbb{Q}\} \subseteq \mathbb{R}$ mit den von $\mathbb{R}$ induzierten Verknüpfungen $+$ und $\cdot$ ist ein Körper.

Beweis:

Offenbar reicht es, folgendes zu zeigen:

(1) $0, 1 \in \mathbb{Q}(\sqrt{2})$, (2) $\forall x, y \in \mathbb{Q}(\sqrt{2})[\, x+y,\ -x,\ x{\cdot}y \in \mathbb{Q}(\sqrt{2})\,]$, (3) $\forall x \in \mathbb{Q}(\sqrt{2}) \setminus \{0\} \exists x' \in \mathbb{Q}(\sqrt{2})(x'x = 1)$.

zu (2): $(a+b\sqrt{2}) + (c+d\sqrt{2}) = (a+c) + (b+d)\sqrt{2}$, $\quad -(a+b\sqrt{2}) = (-a) + (-b)\sqrt{2}$,
$(a+b\sqrt{2})\cdot(c+d\sqrt{2}) = (ac+2bd) + (ad+bc)\sqrt{2}$.

zu (3): Sei $x = a + b\sqrt{2} \neq 0$ $(a, b \in \mathbb{Q})$. Mit Lemma 3.6 folgt dann $a^2 - 2b^2 \neq 0$.
Dann ist $x' := (a - b\sqrt{2})(a^2 - 2b^2)^{-1} \in \mathbb{Q}(\sqrt{2})$ und $x'x = (a^2 - (b\sqrt{2})^2)(a^2 - 2b^2)^{-1} = 1$.

23.11.2009

Bemerkung zur Konstruktion von $\mathbb{C}$ aus $\mathbb{R}$ durch Adjunktion von $\sqrt{-1}$

Der Beweis von Lemma 3.7 motiviert folgenden Weg zur Konstruktion eines Erweiterungskörpers $\mathbb{C}$ von $\mathbb{R}$, in dem $\sqrt{-1}$ existiert. Man setze $\mathbb{C} := \mathbb{R} \times \mathbb{R} = \{(a,b) : a,b \in \mathbb{R}\}$ und definiere Addition bzw. Multiplikation auf $\mathbb{C}$ durch $(a,b) + (c,d) := (a+c, b+d)$ und $(a,b) \cdot (c,d) := (ac - bd, ad + bc)$.
(Das Paar (a,b) entspricht der Zahl $a + b\sqrt{2}$ in 3.7. Die Definition von $(a,b)\cdot(c,d)$ wird durch die folgende formale Rechnung nahegelegt: $(a+b\sqrt{-1})(c+d\sqrt{-1}) = ac + (b\sqrt{-1})(d\sqrt{-1}) + ad\sqrt{-1} + bc\sqrt{-1} = ac + bd(\sqrt{-1})^2 + (ad+bc)\sqrt{-1} = (ac - bd) + (ad+bc)\sqrt{-1}$.)

Man kann dann zeigen, daß $\mathbb{C}$ mit diesen Verknüpfungen eine Körper bildet. Dabei ist $0_{\mathbb{C}} = (0,0)$ und $1_{\mathbb{C}} = (1,0)$. Außerdem ist $-(a,b) = (-a,-b)$ und, falls $(a,b) \neq 0_{\mathbb{C}}$, $(a,b) \cdot (\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}) = (1,0) = 1_{\mathbb{C}}$.
Mit $i := (0,1)$ gilt schließlich $i^2 = (-1,0) = -1_{\mathbb{C}}$. Identifiziert man dann noch $a \in \mathbb{R}$ mit $(a,0) \in \mathbb{C}$, so ist $\mathbb{C}$ tatsächlich ein Erweiterungskörper von $\mathbb{R}$, in dem $\sqrt{-1}$ existiert.

Durch die Identifikation von $a \in \mathbb{R}$ mit $(a,0) \in \mathbb{C}$ erhält man auch die vertraute Darstellung der komplexen Zahlen: $(a,b) = (a,0) + (0,b) = (a,0) + i\cdot(b,0) = a + i\cdot b$.

Lemma 3.8.
Jeder *endliche*, nullteilerfreie, kommutative Ring K mit Einselement $1 \neq 0$ ist ein Körper.

Beweis: Wir müssen zeigen, daß zu jedem $a \in K^*$ ein $x \in K^*$ mit $x \cdot a = 1$ existiert. Sei also $a \in K^*$. Dann ist die Abbildung $K^* \to K^*$, $x \mapsto x\cdot a$ injektiv und deshalb auch surjektiv, da die Menge K^* endlich ist (siehe Lemma 3.9d). Somit $\exists x \in K^* (x\cdot a = 1)$.

Nachtrag zu §2

Definition.
Eine Menge X heißt *endlich*, wenn es ein $n \in \mathbb{N}$ und eine Bijektion $f : \{i \in \mathbb{N} : i < n\} \to X$ gibt; dieses n ist dann eindeutig bestimmt; es heißt die *Mächtigkeit* oder *Anzahl der Elemente* von X und wird mit $|X|$ bezeichnet. Eine Menge X heißt *unendlich*, wenn sie nicht endlich ist. Für unendliches X sei $|X| := \infty$.

Lemma 3.9.
Für endliche Mengen X, Y gilt:
(a) $|X| = |Y| \Leftrightarrow$ es gibt eine bijektive Abbildung $f : X \to Y$.
(b) $X \subsetneqq Y \Rightarrow |X| < |Y|$.
(c) $f : X \to Y \Rightarrow |f(X)| \leq |X|$.
(d) $f : X \to Y$ & $|X| = |Y| \Rightarrow$ (f injektiv $\Leftrightarrow$ f surjektiv).

Beweis von (d):
"$\Rightarrow$": $f : X \to Y$ injektiv $\Rightarrow$ $f : X \to f(X)$ bijektiv $\overset{\text{(a)}}{\Rightarrow}$ $|f(X)| = |X| = |Y|$ $\overset{\text{(b)}}{\Rightarrow}$ $f(X) = Y$.
"$\Leftarrow$": Sei $x_0 \in X$ und $X_1 := X \setminus \{x_0\}$. Dann $|f(X_1)| \overset{\text{(c)}}{\leq} |X_1| \overset{\text{(b)}}{<} |X| = |Y| \overset{f \text{ surj}}{=} |f(X)|$, also $f(X_1) \subsetneqq f(X)$ und somit $f(x_0) \notin f(X_1)$, d.h. $f(x_0) \neq f(x)$ für alle $x \neq x_0$.

§4 Vektorräume

Definition. Seien K ein Körper, V eine Menge und

$+ : V \times V \to V$ *(Vektoraddition)*, $\cdot : K \times V \to V$ *(skalare Multiplikation)* zwei Abbildungen.

Wir schreiben λv für $\lambda \cdot v$. Ferner soll $\cdot$ stärker binden als $+$; z.B. steht $\lambda v + \mu w$ für $(\lambda{\cdot}v) + (\mu{\cdot}w)$.

V (genauer das Tripel $(V, +, \cdot)$) heißt ein K-*Vektorraum* (oder *Vektorraum über dem Körper* K), wenn gilt:

(V1) $(V, +)$ ist eine abelsche Gruppe (neutrales Element $\mathbf{0}_V$ oder $\mathbf{0}$);

(V2) für alle $v, w \in V$ und $\lambda, \mu \in K$ gilt:

$(\lambda + \mu)v = \lambda v + \mu v,$

$\lambda(v + w) = \lambda v + \lambda w,$

$\lambda(\mu v) = (\lambda\mu)v,$

$1v = v.$

Die Elemente von V nennt man *Vektoren*, die von K *Skalare*.

Wir schreiben wie üblich $v - w$ für $v + (-w)$.

Beispiele.

1. $K^{m\times n}$ mit $\big(a_{ij}\big)_{i,j} + \big(b_{ij}\big)_{i,j} := \big(a_{ij} + b_{ij}\big)_{i,j}$ und $\lambda \cdot \big(a_{ij}\big)_{i,j} := \big(\lambda a_{ij}\big)_{i,j}$ ist K-Vektorraum.

   Spezialfälle: $K^n := K^{n\times 1}$ (Spaltenraum) und K $(= K^1)$.

2. Für Mengen X und Y sei $Y^X := \mathrm{Abb}(X, Y) :=$ Menge aller Abbildungen von X nach Y.

   Ist V ein K-Vektorraum und I eine nichtleere Menge, so ist die Menge V^I zusammen mit den *punktweise* definierten Verknüpfungen

   $f + g : I \to V$, $(f + g)(\iota) := g(\iota) + g(\iota)$ und $\lambda{\cdot}f : I \to V$, $(\lambda{\cdot}f)(\iota) := \lambda \cdot f(\iota)$

   ebenfalls ein K-Vektorraum.

25.11.2009

3. $C(\mathbb{R}) := \{f : \ f : \mathbb{R} \to \mathbb{R} \text{ stetig}\}$ und $D(\mathbb{R}) := \{f : \ f : \mathbb{R} \to \mathbb{R} \text{ differenzierbar}\}$ zusammen mit der punktweise definierten Addition und Multiplikation sind $\mathbb{R}$-Vektorräume.

4. $\mathbb{R}$ ist ein $\mathbb{Q}$-Vektorraum.

Bemerkung.

Sei V ein K-Vektorraum. Dann gilt für alle $\lambda, \lambda_i \in K$, $v, v_i \in V$:

(a) $0{\cdot}v = \mathbf{0}_V$ $\quad [0v = (0 + 0)x = 0v + 0v \Rightarrow 0v = \mathbf{0}_V]$

(b) $\lambda{\cdot}\mathbf{0}_V = \mathbf{0}_V$ $\quad [\lambda\mathbf{0}_V = \lambda(\mathbf{0}_V + \mathbf{0}_V) = \lambda\mathbf{0}_V + \lambda\mathbf{0}_V \Rightarrow \lambda\mathbf{0}_V = \mathbf{0}_V]$

(c) $\lambda{\cdot}v = \mathbf{0}_V \Rightarrow \lambda = 0 \vee v = \mathbf{0}_V$ $\quad [\lambda v = \mathbf{0}_V \,\&\, \lambda \neq 0 \Rightarrow v = 1v = (\lambda^{-1}\lambda)v = \lambda^{-1}(\lambda v) = \lambda^{-1}\mathbf{0}_V = \mathbf{0}_V]$

(d) $(-\lambda) \cdot v = \lambda \cdot (-v) = -(\lambda{\cdot}v)$ $\quad [\lambda v + (-\lambda)v = (\lambda + (-\lambda))v = \mathbf{0}_V,\ \lambda v + \lambda(-v) = \lambda(v + (-v)) = \mathbf{0}_V]$

(e) $\lambda \sum\limits_{i=1}^{n} v_i = \sum\limits_{i=1}^{n} \lambda v_i$

(f) $(\sum\limits_{i=1}^{n} \lambda_i)v = \sum\limits_{i=1}^{n} \lambda_i v$

(g) $\sum\limits_{i=1}^{n} v_i + \sum\limits_{i=1}^{n} w_i = \sum\limits_{i=1}^{n} (v_i + w_i)$

Konvention. Für $n < n_0$ sei $\sum\limits_{i=n_0}^{n} v_i := \mathbf{0}$.

Definition. Sei V ein K-Vektorraum.

Eine Teilmenge $U \subseteq V$ heißt *Unterverktorraum* oder kurz *Unterraum* von V, falls gilt:

(UV1) $\mathbf{0}_V \in U$; **(UV2)** $\forall v, w \in U(\ v + w \in U\ )$; **(UV3)** $\forall v \in U \forall \lambda \in K(\ \lambda v \in U\ )$.

Bemerkung.

Ist U ein Unterraum des K-Vektorraums V, so ist U zusammen mit der von V induzierten Addition und skalaren Multiplikation ebenfalls ein K-Vektorraum. Ferner gilt $\forall v, w \in U(v - w \in U)$.

Beispiele.

1. Für jeden Vektorraum V gilt: $\{\mathbf{0}_V\}$ und V sind Unterräume von V.
2. Für $A \in K^{m\times n}$ ist $\text{Lös}(A; 0)$ ein Unterraum von K^n.
3. $C(\mathbb{R})$ und $D(\mathbb{R})$ sind Unterräume von $\mathbb{R}^{\mathbb{R}}$, und $C(\mathbb{R})$ ist auch Unterraum von $D(\mathbb{R})$.

Vereinbarung. Wenn keine Mißverständnisse zu befürchten sind, schreiben wir von jetzt an 0 für $\mathbf{0}_V$.

Lemma 4.1.

Seien V ein K-Vektorraum und $(U_\iota)_{\iota\in I}$ eine nichtleere Familie von Unterräumen von V.

Dann ist auch $U := \bigcap_{\iota\in I} U_\iota$ ein Unterraum von V.

Beweis:

1. $\forall \iota \in I(0 \in U_\iota) \ \Rightarrow\ 0 \in \bigcap_{\iota\in I} U_\iota$.
2. $v, w \in \bigcap_{\iota\in I} U_\iota \ \Rightarrow\ \forall \iota \in I(v, w \in U_\iota) \ \Rightarrow\ \forall \iota \in I(v + w \in U_\iota) \ \Rightarrow\ v + w \in \bigcap_{\iota\in I} U_\iota$.
3. $v \in \bigcap_{\iota\in I} U_i$ und $\lambda \in K \Rightarrow \forall \iota{\in}I(v \in U_\iota \ \&\ \lambda \in K) \Rightarrow \forall \iota{\in}I(\lambda v \in U_\iota) \Rightarrow \lambda v \in \bigcap_{\iota\in I} U_\iota$.

Definition.

Sei V ein K-Vektorraum und $M \subseteq V$.

$v \in V$ heißt eine *Linearkombination* von $v_1, \ldots, v_k \in V$, wenn es $\lambda_1, \ldots, \lambda_k \in K$ gibt, so daß $v = \sum\limits_{i=1}^{k} \lambda_i v_i$.

Die Menge aller Linearkombinationen von Vektoren aus M wird mit $\text{span}(M)$ bezeichnet:

$\text{span}(M) := \{\sum\limits_{i=1}^{k} \lambda_i v_i : k \geq 0 \ \&\ v_1, \ldots, v_k \in M \ \&\ \lambda_1, \ldots, \lambda_k \in K\}$.

Hier ist auch $k = 0$ zugelassen. Demzufolge gilt in jedem Fall $0 = \sum\limits_{i=1}^{0} \lambda_i v_i \in \text{span}(M)$.

Insbesondere ist $\text{span}(\emptyset) = \{0\}$.

Für eine Familie $(v_\iota)_{\iota\in I}$ von Vektoren aus V sei $\text{span}(v_\iota)_{\iota\in I} := \text{span}\{v_\iota : \iota \in I\}$.

Für endliche Familien $(v_1, ..., v_k)$ verwendet man oft die Notation $Kv_1 + \ldots + Kv_k := \text{span}(v_1, ..., v_k)$.

Offenbar ist $\text{span}(v_1, ..., v_k) = \{\sum\limits_{i=1}^{k} \lambda_i v_i : \lambda_1, \ldots, \lambda_k \in K\}$.

Lemma 4.2. Sei V ein K-Vektorraum und $M \subseteq V$.

(a) $U := \text{span}(M)$ ist der kleinste Unterraum von V, der M umfaßt, d.h. es gilt:
   U ist Unterraum von V & $M \subseteq U$ & für jeden Unterraum W von V gilt: $M \subseteq W \ \Rightarrow\ U \subseteq W$.
   Man nennt $\text{span}(M)$ den von M *aufgespannten (oder erzeugten) Unterraum.*

(b) $N \subseteq \text{span}(M) \implies \text{span}(N) \subseteq \text{span}(M)$.

(c) Ist M ein Unterraum, so $\text{span}(M) = M$. Folglich gilt auch $\text{span}(\text{span}(M)) = \text{span}(M)$.

(d) $M \subseteq N \subseteq \text{span}(M) \ \Rightarrow\ \text{span}(N) = \text{span}(M)$.

Beweis:

(a) 1. Wie oben erwähnt, ist $0 \in U$.

2. Sind $v, w \in U$, so gibt es $v_1, ..., v_k \in M$ und $\lambda_1, ..., \lambda_k \in K$ mit $v = \sum_{i=1}^k \lambda_i v_i$, sowie $w_1, ..., w_m \in M$ und $\mu_1, ..., \mu_m \in K$ mit $w = \sum_{i=1}^m \mu_i w_i$. Es folgt $v + w = \lambda_1 v_1 + ... + \lambda_k v_k + \mu_1 w_1 + ... + \mu_m w_m \in U$.

3. Die Abgeschlossenheit von U unter skalarer Multiplikation folgt aus $\mu \sum_{i=1}^k \lambda_i v_i = \sum_{i=1}^k (\mu\lambda_i) v_i$.

4. $M \subseteq U$: klar.

5. Ist W ein Unterraum von V mit $M \subseteq W$, so gilt offenbar
$\mathrm{span}(M) = \{\sum_{i=1}^k \lambda_i v_i : k \geq 0 \;\&\; v_1, \ldots, v_k \in M \;\&\; \lambda_1, \ldots, \lambda_k \in K\} \subseteq W$.

(b), (c) und (d) folgen aus (a).

Definition.

Seien V ein K-Vektorraum und $(U_i)_{i \in I}$ eine Familie von Unterräumen von V.

$\sum_{i \in I} U := \mathrm{span}(\bigcup_{i \in I} U_i)$ heißt *Summe der Unterräume* $(U_i)_{i \in I}$.

Im Fall $I = \{1, ..., n\}$ schreibt man $\sum\limits_{i=1}^{n} U_i$ oder $U_1 + \ldots + U_n$.

Bemerkung. $\sum\limits_{i=1}^{n} U_i = \{\sum\limits_{i=1}^{n} u_i : u_1 \in U_1 \;\&\; \ldots \;\&\; u_n \in U_n\}$.

Beweis:

Sei $M := \{\sum\limits_{i=1}^{n} u_i : u_1 \in U_1 \;\&\; \ldots \;\&\; u_n \in U_n\}$.

Offenbar ist $M \subseteq \mathrm{span}(\bigcup\limits_{i=1}^{n} U_i)$, und da die U_i Unterräume sind, gilt auch $\mathrm{span}(\bigcup\limits_{i=1}^{n} U_i) \subseteq M$.

Lineare Abhängigkeit, Basis, Dimension

Vereinbarung: Im folgenden bezeichne K stets einen Körper und V einen Vektorraum über K.

Definition.

1. Eine endliche Familie $(v_1, \ldots, v_m)$ von Vektoren aus V heißt *linear unabhängig*, wenn gilt:
   $\forall \lambda_1, ..., \lambda_m \in K \big(\sum\limits_{i=1}^{m} \lambda_i v_i = 0 \;\Rightarrow\; \lambda_1 = \ldots = \lambda_m = 0 \big)$.

30.11.2009

2. Eine beliebige Familie $(v_\iota)_{\iota \in I}$ von Vektoren aus V heißt *linear unabhängig*, wenn jede endliche Teilfamilie $(v_{\iota_1}, ..., v_{\iota_m})$ linear unabhängig ist.
3. Die Familie $(v_\iota)_{\iota \in I}$ heißt *linear abhängig*, wenn sie nicht linear unabhängig ist.
4. v heißt *linear abhängig von* $(v_\iota)_{\iota \in I}$ $:\Longleftrightarrow$ $v \in \mathrm{span}(v_\iota)_{\iota \in I}$.

Statt *“$(v_1, ..., v_m)$ ist linear (un)abhängig”* sagt man auch *“die Vektoren $v_1, ..., v_m$ sind linear (un)abhängig”*.

Bemerkungen.

(1) $(v_1, ..., v_m)$ linear abhängig $\Longleftrightarrow$ $\exists \lambda_1, ..., \lambda_m \in K(\sum\limits_{i=1}^{m} \lambda_i v_i = 0 \;\&\; \exists i \in \{1, ..., m\}(\lambda_i \neq 0))$.

(2) (v_1, v_2) linear abhängig $\Longleftrightarrow$ $\exists \lambda \in K(v_1 = \lambda v_2$ oder $v_2 = \lambda v_1)$.

(3) (v_1) linear abhängig $\Longleftrightarrow$ $v_1 = 0$.

(4) $0 \in \{v_1, \ldots v_m\}$ oder $\exists i, j \in \{1, ..., m\}(i \neq j \;\&\; v_i = v_j)$ $\Longrightarrow$ $(v_1, \ldots, v_m)$ linear abhängig.

Lemma 4.3. Für $v_1, ..., v_m, u \in V$ gilt:

(a) $(v_1, ..., v_m)$ linear abhängig $\iff$ $\exists\, k \in \{1, ..., m\} \big(v_k \in \operatorname{span}(v_1, ..., v_{k-1}, v_{k+1}, ..., v_m) \big)$.

(b) $(v_1, ..., v_m)$ linear unabhängig $\iff$ $\begin{cases} \text{Für alle } \lambda_1, \ldots, \lambda_m, \mu_1, \ldots, \mu_m \in K \text{ gilt:} \\ \sum\limits_{i=1}^m \lambda_i v_i = \sum\limits_{i=1}^m \mu_i v_i \;\Rightarrow\; \lambda_i = \mu_i \text{ für } i = 1, ..., m. \end{cases}$

(c) $(v_1, ..., v_m)$ linear unabhängig und $(v_1, ..., v_m, u)$ linear abhängig $\Longrightarrow$ $u \in \operatorname{span}(v_1, ..., v_m)$.

Beweis :

(a) "$\Rightarrow$": $\sum_{i=1}^m \lambda_i v_i = 0$ und $k \in \{1, ..., m\}$ mit $\lambda_k \neq 0$ $\Rightarrow$ $v_k = \sum\limits_{\substack{i=1\\ i\neq k}}^m \dfrac{-\lambda_i}{\lambda_l} v_i$.

"$\Leftarrow$": $v_k = \sum\limits_{\substack{i=1\\ i\neq k}}^m \mu_i v_i \;\Rightarrow\; 0 = \sum\limits_{i=1}^m \mu_i v_i$ wobei $\mu_k := -1$.

(b) "$\Rightarrow$": $v = \sum_{i=1}^m \lambda_i v_i$ & $v = \sum_{i=1}^m \mu_i v_i \;\Rightarrow\; 0 = v - v = \sum_{i=1}^m (\lambda_i - \mu_i) v_i \overset{\text{lin.unabh.}}{\Rightarrow} \lambda_i - \mu_i = 0$.

"$\Leftarrow$": Wegen $0 = \sum_{i=1}^m 0 \cdot v_i$ folgt aus der Vorauss.: $\forall \lambda_1, ..., \lambda_m (\sum_{i=1}^m \lambda_i v_i = 0 \Rightarrow \lambda_1 = 0 \,\&\, ... \,\&\, \lambda_m = 0)$.

(c) $v_1, ..., v_m$ linear unabhängig und $\lambda_1 v_1 + ... + \lambda_m v_m + \lambda_{m+1} u = 0$ mit $\exists i \in \{1, ..., m{+}1\} (\lambda_i \neq 0)$ $\Rightarrow$
$\Rightarrow$ $\lambda_{m+1} \neq 0$ $\Rightarrow$ $u = \sum_{i=1}^m \dfrac{-\lambda_i}{\lambda_{m+1}} v_i \in \operatorname{span}(v_1, ..., v_m)$.

Beispiel.

Ist $A = (a_{ij}) \in K^{m \times n}$ eine Stufenmatrix, so sind ihre Stufenspalten $a_{j_1}, \ldots, a_{j_r}$ linear unabhängig.

Beweis:

Sei $\sum_{\nu=1}^r \lambda_\nu a_{j_\nu} = 0$. Durch Induktion nach $r - k$ zeigen wir $\lambda_i = 0$ für $k < i \leq r$.
Der Induktionsanfang $k = r$ ist trivial. Sei also jetzt $0 < k \leq r$ und gelte $\lambda_i = 0$ für $k < i \leq r$ (I.V.).
Zu zeigen: $\lambda_k = 0$. Aus $\sum_{\nu=1}^r \lambda_\nu a_{j_\nu} = 0$ folgt mit I.V. $\sum_{\nu=1}^k \lambda_\nu a_{j_\nu} = 0$. Wir haben also $\sum_{\nu=1}^k \lambda_\nu a_{kj_\nu} = 0$, sowie $a_{kj_k} \neq 0$ und $a_{kj} = 0$ für $1 \leq j < j_k$. Daraus folgt $\lambda_k a_{kj_k} = 0$ und weiter $\lambda_k = 0$.

Definition (Erzeugendensystem, Basis).

1. Sei $\mathcal{B} = (v_\iota)_{\iota \in I}$ eine Familie von Vektoren in V.

   $\mathcal{B}$ heißt *Erzeugendensystem von* V $:\iff$ $V = \operatorname{span}(v_\iota)_{\iota \in I}$.

   $\mathcal{B}$ heißt *Basis* von V $:\iff$ $\mathcal{B}$ ist ein linear unabhängiges Erzeugendensystem von V.

2. V heißt *endlich erzeugt* (oder *endlichdimensional*), wenn V ein endliches Erzeugendensystem besitzt.

3. Ist $(v_1, \ldots, v_n)$ eine Basis von V, so nennt man n die *Länge der Basis.*

4. Die leere Folge () ist Basis des Vektorraums $\{0\}$ und hat die Länge ist 0.

5. Eine Menge $M \subseteq V$ heißt Erzeugendensystem von V, wenn $V = \operatorname{span}(M)$ ist.

Beispiele.

1. $(1, \sqrt{2})$ ist eine Basis des $\mathbb{Q}$-Vektorraums $\mathbb{Q}(\sqrt{2})$.
2. $(1, i)$ ist eine Basis von $\mathbb{C}$ als $\mathbb{R}$-Vektorraum.

2.12.2009

Lemma 4.4.

(a) Für $v_1, ..., v_n \in V$ gilt: $(v_1, ..., v_n)$ ist Basis von V $\iff$ $\forall v \in V \exists! (\lambda_1, ..., \lambda_n) \, (v = \sum\limits_{i=1}^n \lambda_i v_i)$.

(b) Die Einheitsvektoren $e_1, ..., e_n \in K^n$ bilden eine Basis von K^n, die sog. *Standardbasis.*

Beweis :

(a) folgt aus Lemma 4.3b.

(b) Erzeugendensystem: $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \sum_{i=1}^n x_i e_i$.

Linear unabhängig: $\sum_{i=1}^n \lambda_i e_i = 0 \in K^n \;\Rightarrow\; \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = 0 \in K^n \;\Rightarrow\; \lambda_1 = \ldots = \lambda_n = 0$.

Satz 4.5 (Basisauswahlsatz).

Ist M ein endliches Erzeugendensystem von V, so existiert eine Basis $(v_1, ..., v_n)$ von V mit $v_1, ..., v_n \in M$.

Korollar.

Jeder endlich erzeugte Vektorraum besitzt eine endliche Basis.

Beweis des Satzes durch Induktion nach $|M|$:

Seien $M = \{v_1, ..., v_m\}$ mit $m = |M|$. Ist $(v_1, ..., v_m)$ linear unabhängig, so fertig. Andernfalls existiert (nach 4.3a) ein $l \in \{1, ..., m\}$, so daß $v_l \in \mathrm{span}(v_1, ..., v_{l-1}, v_{l+1}, ..., v_m)$ und folglich $V = \mathrm{span}(v_1, ..., v_m) = \mathrm{span}(v_1, ..., v_{l-1}, v_{l+1}, ..., v_m)$ (vgl. L.4.2d). Daraus folgt nach I.V. die Behauptung.

Lemma 4.6. (Austauschlemma).

Ist $(v_1, ..., v_n)$ eine Basis von V, $w = \sum\limits_{i=1}^{n} \lambda_i v_i$ und $j \in \{1, ..., n\}$ mit $\lambda_j \neq 0$, so ist auch $(v_1, ..., v_{j-1}, w, v_{j+1}, ..., v_n)$ Basis von V.

Beweis:

o.E.d.A.: $j = n$.

1. Es gilt $v_n = \frac{1}{\lambda_n}(w - \sum_{i=1}^{n-1} \lambda_i v_i) \in \mathrm{span}(v_1, ..., v_{n-1}, w)$, woraus folgt:
$V = \mathrm{span}(v_1, ..., v_n) \subseteq \mathrm{span}(v_1, ..., v_{n-1}, w)$.

2. Wären $v_1, ..., v_{n-1}, w$ linear abhängig, so nach 4.3c $w \in \mathrm{span}(v_1, ..., v_{n-1})$ und damit $\mathrm{span}(v_1, ..., v_{n-1}) = \mathrm{span}(v_1, ..., v_{n-1}, w) = V$, also $v_n \in \mathrm{span}(v_1, ..., v_{n-1})$. Widerspruch zu "$(v_1, ..., v_n)$ linear unabhängig".

Satz 4.7 (Basisergänzungssatz).

Sei M ein endliches Erzeugendensystem von V und sei $(w_1, \ldots, w_k)$ ein linear unabhängiges Tupel in V. Dann gibt es $v_1, \ldots, v_n \in M$, so daß $(w_1, \ldots, w_k, v_1, \ldots, v_n)$ eine Basis von V und $k + n \leq |M|$ ist.

Beweis durch Induktion nach k:

1. $k = 0$: siehe Lemma 4.5.

2. $0 < k$: Mit $(w_1, \ldots, w_k)$ ist offenbar auch $(w_1, \ldots, w_{k-1})$ linear unabhängig. Nach I.V. gibt es deshalb $v_1, \ldots, v_n \in M$, so daß $(w_1, \ldots, w_{k-1}, v_1, \ldots, v_n)$ Basis von V und $k - 1 + n \leq |M|$ ist.

Nun gibt es $\lambda_1, ..., \lambda_{k-1}, \mu_1, \ldots, \mu_n \in K$, so daß $w_k = \sum_{i=1}^{k-1} \lambda_i w_i + \sum_{i=1}^n \mu_i v_i$.
Da $(w_1, \ldots, w_k)$ linear unbhängig ist, existiert ein $j \in \{1, \ldots, n\}$ mit $\mu_j \neq 0$.
Nach Lemma 4.6 ist dann auch $(w_1, \ldots, w_{k-1}, w_k, v_1, \ldots, v_{j-1}, v_{j+1}, \ldots, v_n)$ eine Basis von V.

Korollar (Invarianz der Basislänge).

Je zwei Basen eines endlich erzeugten K-Vektorraums V haben die gleiche Länge, d.h.,
sind $(v_1, ..., v_n)$ und $(w_1, ..., w_m)$ Basen von V, so ist $n = m$.

Definition (Dimension).
Sei V ein endlich erzeugter K-Vektorraum. Nach den Korollaren zu 4.5 und 4.7 können wir definieren: Die *Dimension von* V (in Zeichen $\dim(V)$) ist die Länge einer beliebigen Basis von V.

Ist V nicht endlich erzeugt, so sei $\dim(V) := \infty$.

V heißt n-dimensional, falls $\dim(V) = n \in \mathbb{N}$.

Folgerung.
Ist $(v_1, ..., v_n)$ eine Basis von V, so ist $\dim(V) = n$. Insbesondere gilt $\dim(\{0\}) = 0$.

Mit Hilfe der Sätze 4.5 und 4.7 erhalten wir die folgenden zwei Lemmata.

Lemma 4.8. Seien $v_1, ..., v_m \in V$. Dann gilt:
(a) $(v_1, ..., v_m)$ linear unabhängig $\Rightarrow$ $m \leq \dim(V)$.
(b) $(v_1, ..., v_m)$ Erzeugendensystem von V $\Rightarrow$ $\dim(V) \leq m$.

Lemma 4.9. Seien $v_1, ..., v_n \in V$ und $\dim(V) = n$. Dann gilt:
$(v_1, ..., v_n)$ linear unabhängig $\iff$ $(v_1, ..., v_n)$ ist ein Erzeugendensystem von V.

Lemma 4.10.
Ist U ein Unterraum des Vektorraums V, so gilt:
(a) $\dim(U) \leq \dim(V)$;
(b) $\dim(U) = \dim(V) < \infty \Rightarrow U = V$.

Beweis:
(a) Sei $\dim(V) = n < \infty$ (sonst ist die Behauptung trivial). Wegen $U \subseteq V$ und Lemma 4.8a hat dann jedes linear unabhängige Tupel in U eine Länge $\leq n$. Sei $(v_1, ..., v_m)$ ein linear unabhängiges Tupel in U mit maximaler Länge. Nach Lemma 4.3c muß dies eine Basis von U sein. Also $\dim(U) = m \leq n$.

(b) Sei $n := \dim(U) = \dim(V)$. Dann besitzt U eine Basis $(v_1, ..., v_n)$. Mit Lemma 4.9 folgt, daß diese auch Basis von V ist. Also $V = \mathrm{span}(v_1, ..., v_n) = U$.

7.12.2009

Summen von Vektorräumen

Definition. Seien V ein K-Vektorraum und $U_1, ..., U_n$ Unterräume von V.
V heißt *direkte Summe* von $U_1, ..., U_n$ (in Zeichen: $V = U_1 \oplus \ldots \oplus U_n$ oder $V = \bigoplus_{i=1}^n U_i$), wenn gilt:
(1) $V = U_1 + \ldots + U_n$
(2) $\forall x_1 \in U_1 \ldots \forall x_n \in U_n (x_1 + \ldots + x_n = 0 \Rightarrow x_1 = ... = x_n = 0)$. ("Direktheit")

Lemma 4.11. Sind $U_1, ..., U_n$ Unterräume des K-Vektorraums V, so gilt:

$$V = U_1 \oplus \ldots \oplus U_n \iff \begin{cases} \text{Jedes } x \in V \text{ läßt sich eindeutig in der Form } x = u_1 + ... + u_n \\ \text{mit } u_i \in U_i \text{ für } i = 1, ..., n \text{ darstellen.} \end{cases}$$

Beweis :
"$\Rightarrow$": Seien $u_i, u_i' \in U_i$ $(i = 1, ..., n)$, so daß $u_1 + ... + u_n = u_1' + ... + u_n'$. Dann gilt $u_i - u_i' \in U_i$ $(i = 1, ..., n)$ mit $(u_1 - u_1') + \ldots + (u_n - u_n') = 0$, woraus nach Voraussetzung $u_i - u_i' = 0$ für $i = 1, ..., n$ folgt.

"$\Leftarrow$": Seien $u_i \in U_i$ $(i = 1, ..., n)$, so daß $u_1 + ... + u_n = 0$. Zusammen mit $0 + ... + 0 = 0$ folgt daraus nach Voraussetzung $u_1 = 0$ & $\ldots$ & $u_n = 0$.

Satz 4.12.
Seien $U_1, ..., U_k$ Unterräume des endlichdimensionalen K-Vektorraums V und sei $V = U_1 + ... + U_k$.
Sei ferner $\overline{v} = (v_{11}, ..., v_{1n_1}, ..., v_{k1}, ..., v_{kn_k})$ mit $v_{i1}, ..., v_{in_i} \in U_i$ für $i = 1, ..., k$. Dann gilt:

(a) Ist $(v_{i1}, ..., v_{in_i})$ Basis von U_i für $i = 1, .., k$, so gilt: $V = U_1 \oplus ... \oplus U_k \iff \overline{v}$ Basis von V.

(b) Gilt $V = U_1 \oplus ... \oplus U_k$ und ist $\overline{v}$ Basis von V, so ist $(v_{i1}, ..., v_{in_i})$ Basis von U_i für $i = 1, .., k$.

Beweis :
(a) "$\Rightarrow$" Nach Voraussetzung ist $\overline{v}$ Erzeugendensystem von V. Es muß daher nur noch die lineare Unabhängigkeit von $\overline{v}$ bewiesen werden. Sei also $\mu_{11}v_{11} + ... + \mu_{1n_1}v_{1n_1} + ... + \mu_{k1}v_{k1} + ... + \mu_{kn_k}v_{kn_k} = 0$. Dann $u_1 + ... + u_k = 0$ mit $u_i := \mu_{i1}v_{i1} + ... + \mu_{in_i}v_{in_i} \in U_i$. Es folgt $u_1 = \ldots = u_k = 0$ und weiter $\mu_{i1} = \ldots = \mu_{in_i} = 0$ für $i = 1, ..., k$.
"$\Leftarrow$" Sei $u_1 + ... + u_k = 0$ mit $u_i \in U_i$ $(i = 1, ..., k)$. Dann existieren μ_{ij}, so daß $u_i = \mu_{i1}v_{i1} + ... + \mu_{in_i}v_{in_i}$ $(i = 1, ..., k)$. Folglich $\mu_{11}v_{11} + ... + \mu_{1n_1}v_{1n_1} + ... + \mu_{k1}v_{k1} + ... + \mu_{kn_k}v_{kn_k} = 0$, und deshalb $\mu_{ij} = 0$ für alle i, j, woraus $u_1 = ... = u_k = 0$ folgt.

(b) Nach Voraussetzung gilt: $\dim(V) = n_1 + ... + n_k$ und $(v_{i1}, ..., v_{in_i})$ linear unabhängig $(i = 1, ..., k)$.
Aus letzterem folgt $n_i \leq \dim(U_i)$. Mit dem unten stehenden Korollar (in dessen Beweis 4.12b nicht benutzt wird) folgt außerdem $\dim(V) = \dim(U_1) + ... + \dim(U_k)$. Insgesamt erhalten wir nun $\dim(U_i) = n_i$ $(i = 1, ..., k)$ und damit die Behauptung.

Korollar
Sind $U_1, ..., U_k$ Unterräume des endlichdimensionalen K-Vektorraums V und ist $V = U_1 + ... + U_k$, so gilt:
$V = U_1 \oplus ... \oplus U_k \iff \dim(V) = \dim(U_1) + ... + \dim(U_k)$.

Beweis :
Wir wählen für jedes U_i eine Basis $(v_{i1}, ..., v_{in_i})$. Wie oben sei $\overline{v} := (v_{11}, ..., v_{1n_1}, ..., v_{k1}, ..., v_{kn_k})$.
Ferner $n := \dim(U_1) + ... + \dim(U_k) = n_1 + ... + n_k$.
Da $\overline{v}$ Erzeugendensystem von V der Länge n ist, folgt mit Lemma 4.9: $\dim(V) = n \iff \overline{v}$ Basis von V.
Nach 4.12a gilt: $V = U_1 \oplus ... \oplus U_k \iff \overline{v}$ Basis von V.

Lemma 4.13.
Sind U, W Unterräume von V, so gilt: $V = U \oplus W \iff V = U + W \;\&\; U \cap W = \{0\}$.

Beweis :
"$\Rightarrow$": $u \in U \cap W \Rightarrow 0 = u + (-u)$ mit $u \in U \;\& \; -u \in W \overset{\text{Vorauss.}}{\Rightarrow} u = 0$.
"$\Leftarrow$": $u + w = 0$ mit $u \in U \;\&\; w \in W \Rightarrow w = -u \in U \cap W \overset{\text{Vorauss.}}{\Rightarrow} u = 0 \;\&\; w = 0$.

Lemma 4.14.
Sind $(u_1, ..., u_k)$ und $(w_1, ..., w_m)$ linear unabhängige Familien im K-Vektorraum V, so gilt:
$(u_1, ..., u_k, w_1, ..., w_m)$ linear unabhängig $\iff \operatorname{span}(u_1, ..., u_k) \cap \operatorname{span}(w_1, ..., w_m) = \{0\}$.

Beweis: Lemmata 4.12a, 4.13.

Satz 4.15 (Dimensionssatz für Untervektorräume).
Für endlichdimensionale Unterräume U, W von V gilt: $\dim(U + W) = \dim(U) + \dim(W) - \dim(U \cap W)$.

Beweis :
Sei $v_1, ..., v_l$ eine Basis von $U \cap W$. Wir ergänzen diese zu einer Basis $v_1, ..., v_l, u_1, ..., u_m$ von U, sowie zu einer Basis $v_1, ..., v_l, w_1, ..., w_n$ von W. Dann ist $U + W = \operatorname{span}(v_1, ..., v_l, u_1, ..., u_m, w_1, ..., w_n)$ $(*)$.
$\operatorname{span}(\vec{v}, \vec{u}) \cap \operatorname{span}(\vec{w}) \subseteq U \cap W \cap \operatorname{span}(\vec{w}) = \operatorname{span}(\vec{v}) \cap \operatorname{span}(\vec{w}) \overset{4.14}{=} \{0\} \overset{4.14+(*)}{\Longrightarrow}$
$v_1, ..., v_l, u_1, ..., u_m, w_1, ..., w_n$ ist Basis von $U + W \Longrightarrow$
$\dim(U + W) = l + m + n = (l + m) + (l + n) - l = \dim(U) + \dim(W) - \dim(U \cap W)$.

9.12.2009

Lemma 4.16.

(a) Gelte $a_1, \ldots, a_l, a'_1, \ldots, a'_l \in K^m$ und $(a_1 \ldots a_l) \overset{\text{EZU}}{\longmapsto} (a'_1 \ldots a'_l)$.

Dann gilt: $(a_1, \ldots, a_l)$ linear unabhängig $\Leftrightarrow$ $(a'_1, \ldots, a'_l)$ linear unabhängig.

(b) Seien $v_1, \ldots, v_n \in K^m$ und gelte $(v_1 \ldots v_n) \overset{\text{EZU}}{\longrightarrow} A$, wobei $A \in K^{m\times n}$ eine Stufenmatrix mit den Stufenspalten $a_{j_1}, \ldots, a_{j_r}$. Dann ist $(v_{j_1}, \ldots, v_{j_r})$ eine Basis von $\operatorname{span}(v_1, ..., v_n) \subseteq K^m$.

Beweis:

(a) Mit $A := (a_1 \ldots a_l)$, $A' := (a'_1 \ldots a'_l)$ gilt:

$(a_1, \ldots, a_l)$ lin.unabh. $\Leftrightarrow$ $\text{Lös}(A; 0) = \{0\} \overset{\text{L.1.1}}{\Leftrightarrow} \text{Lös}(A'; 0) = \{0\}$ $\Leftrightarrow$ $(a'_1, \ldots, a'_l)$ lin.unabh.

(b) Wie auf S.24 gezeigt, ist $(a_{j_1}, \ldots, a_{j_r})$ lin.unabh.; ferner gilt $\operatorname{span}(a_{j_1}, \ldots, a_{j_r}) \subseteq \operatorname{span}(a_1, \ldots, a_n) \subseteq \operatorname{span}(e_1, \ldots, e_r)$ und $\dim \operatorname{span}(e_1, \ldots, e_r) = r$. Mit L.4.10b folgt nun $\operatorname{span}(a_{j_1}, \ldots, a_{j_r}) = \operatorname{span}(a_1, \ldots, a_n)$. Also ist $(a_{j_1}, \ldots, a_{j_r})$ Basis von $\operatorname{span}(a_1, \ldots, a_n)$. Mit (a) folgt daraus die Behauptung.

Beispiel:

$$v_1 = \begin{pmatrix} 0 \\ 2 \\ 1 \\ 3 \end{pmatrix}, v_2 = \begin{pmatrix} 1 \\ 0 \\ -1 \\ 2 \end{pmatrix}, v_3 = \begin{pmatrix} -2 \\ 2 \\ 3 \\ -1 \end{pmatrix}, v_4 = \begin{pmatrix} 2 \\ 4 \\ 0 \\ 9 \end{pmatrix}. \quad (v_1\ v_2\ v_3\ v_4) \overset{\text{EZU}}{\longrightarrow} \begin{pmatrix} 1 & -1 & 3 & 0 \\ 0 & 1 & -2 & 2 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Also ist (v_1, v_2, v_4) eine Basis von $\operatorname{span}(v_1, v_2, v_3, v_4)$.

§5 Lineare Abbildungen

Definition.

Seien V, W Vektorräume über K. Eine Abbildung $f : V \to W$ heißt *linear* oder *Homomorphismus*, wenn $f(x+y) = f(x) + f(y)$ und $f(\lambda x) = \lambda f(x)$ für alle $x, y \in V,\ \lambda \in K$ gilt.

Bemerkungen.

1. $f : V \to W$ ist genau dann linear, wenn gilt $\forall x, y \in V \forall \lambda, \mu \in K\big((f(\lambda x + \mu y) = \lambda f(x) + \mu f(y)\big)$.
2. Ist $f : V \to W$ linear, so $f(x-y) = f(x) - f(y)$, $f(0) = 0$ und $f(\sum_{i=1}^n \lambda_i v_i) = \sum_{i=1}^n \lambda_i f(v_i)$.
3. Sind $f : V \to W$ und $g : W \to U$ lineare Abbildungen, dann ist auch $g \circ f : V \to U$ eine lineare Abbildung.

Beispiele. Die folgenden Abbildungen sind linear:

1. $0 : V \to W,\ x \mapsto 0$ und $\mathrm{id}_V : V \to V,\ x \mapsto x$.
2. $g_\alpha : K \to K,\ x \mapsto \alpha x \quad (\alpha \in K)$.
3. $\widehat{h} : V^I \to V^I,\ g \mapsto g \circ h \quad$ (für beliebiges $h : I \to I$).
4. $D(\mathbb{R}) \to \mathbb{R}^\mathbb{R},\ f \mapsto f'$ (Ableitung).
5. $D(\mathbb{R}) \to \mathbb{R},\ f \mapsto f'(x_0) \quad (x_0 \in \mathbb{R})$.
6. $C([a,b], \mathbb{R}) \to \mathbb{R},\ f \mapsto \int\limits_a^b f(x)dx$, wobei $C([a,b],\mathbb{R}) :=$ Raum der stetigen Funktionen von $[a,b]$ nach $\mathbb{R}$.

Definition. Für $A \in K^{m\times n}$ sei $\mathsf{f}_A : K^n \to K^m$, $\mathsf{f}_A(x) := A{\cdot}x$.

Lemma 5.1. Seien $m, n, p \geq 1$.

(a) Für jedes $A \in K^{m\times n}$ ist $\mathsf{f}_A : K^n \to K^m$ eine lineare Abbildung,
und für $j = 1, \ldots, n$ gilt: $\mathsf{f}_A(e_j) = j$-te Spalte von A.

(b) Für jede lineare Abbildung $f : K^n \to K^m$ gibt es genau eine Matrix $A \in K^{m\times n}$ mit $f = \mathsf{f}_A$.

(c) Für $A \in K^{m\times p}$ und $B \in K^{p\times n}$ gilt $\mathsf{f}_A \circ \mathsf{f}_B = \mathsf{f}_{AB}$.

Beweis:

(a) klar nach Lemma 1.6.

(b) *Eindeutigkeit:* Seien $A, A' \in K^{m\times n}$ mit $\mathsf{f}_A = \mathsf{f}_{A'}$. Dann gilt für jedes $j \in \{1, ..., n\}$:
j-te Spalte von $A = A \cdot e_j = \mathsf{f}_A(e_j) = \mathsf{f}_{A'}(e_j) = A' \cdot e_j = j$-te Spalte von A'. Folglich $A = A'$.

Existenz: Wir definieren $A = (a_{ij}) \in K^{m\times n}$, so daß $\begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix} = f(e_j)$.

Für $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ gilt dann: $\mathsf{f}_A(x) = A \cdot x \overset{\text{L.1.5b}}{=} \sum_{j=1}^n x_j f(e_j) = f(\sum_{j=1}^n x_j e_j) = f(x)$.

(c) $(\mathsf{f}_A \circ \mathsf{f}_B)(x) = \mathsf{f}_A(\mathsf{f}_B(x)) = A(Bx) = (AB)x = \mathsf{f}_{AB}(x)$.

Beispiele.

1. Ist $A = \begin{pmatrix} 3 & 1 \\ 1 & 2 \end{pmatrix}$, so gilt $\mathsf{f}_A \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 3 \\ 1 \end{pmatrix}$ und $\mathsf{f}_A \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$.

2. Für $\varphi \in \mathbb{R}$ sei $A(\varphi) = \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}$.

Dann ist $\mathsf{f}_{A(\varphi)} : \mathbb{R}^2 \to \mathbb{R}^2$ die *Drehung* um den Winkel φ, denn für ein $x = \begin{pmatrix} \cos\alpha \\ \sin\alpha \end{pmatrix} \in \mathbb{R}^2$ auf gilt

$$\mathsf{f}_{A(\varphi)}(x) = \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix} \begin{pmatrix} \cos\alpha \\ \sin\alpha \end{pmatrix} = \begin{pmatrix} \cos\varphi\cos\alpha - \sin\varphi\sin\alpha \\ \sin\varphi\cos\alpha + \cos\varphi\sin\alpha \end{pmatrix} = \begin{pmatrix} \cos(\varphi+\alpha) \\ \sin(\varphi+\alpha) \end{pmatrix}.$$

3. Für $A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ ist $\mathsf{f}_A : \mathbb{R}^2 \to \mathbb{R}^2$ die *Spiegelung* an der x_1-Achse:

$$\mathsf{f}_A \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 \\ -x_2 \end{pmatrix}.$$

4. Für $A = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}$ ist $\mathsf{f}_A : \mathbb{R}^2 \to \mathbb{R}^2$ eine *Streckung* in Richtung der x_1- und x_2-Achse:

$$\mathsf{f}_A \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 2x_1 \\ 3x_2 \end{pmatrix}.$$

5. Für $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ ist $\mathsf{f}_A : \mathbb{R}^2 \to \mathbb{R}^2$ die *orthogonale Projektion* auf die x_1-Achse:

$$\mathsf{f}_A \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 \\ 0 \end{pmatrix}.$$

Lemma 5.2. Sei $f : V \to W$ linear und $v_1, ..., v_m \in V$.

(a) $(v_1, ..., v_m)$ linear abhängig $\Rightarrow$ $(f(v_1), ..., f(v_m))$ linear abhängig.

(b) $U = \text{span}(v_1, ..., v_m) \ \Rightarrow \ f(U) = \text{span}(f(v_1), ..., f(v_m))$.

(c) Ist U ein Unterraum von V, so ist $f(U)$ ein Unterraum von W und $\dim f(U) \leq \dim U$.

(d) Ist W' ein Unterraum von W, so ist $f^{-1}(W')$ ein Unterraum von V.

Definition: $\text{Ker}(f) := f^{-1}(\{0\})$.

(e) f injektiv $\iff$ $\text{Ker}(f) = \{0\}$.

Beweis :

(a) $\sum_{i=1}^m \lambda_i v_i = 0 \ \Rightarrow \ \sum_{i=1}^m \lambda_i f(v_i) = f(\sum_{i=1}^m \lambda_i v_i) = 0$.

(b) $f(U) = \{f(\sum_{i=1}^m \lambda_i v_i) : \lambda_1, ..., \lambda_m \in K\} = \{\sum_{i=1}^m \lambda_i f(v_i) : \lambda_1, ..., \lambda_m \in K\} = \text{span}(f(v_1), ..., f(v_m))$.

(c) 1. "$f(U)$ Unterraum von W": Beweis ähnlich wie für (d).

2. "$\dim f(U) \leq \dim U$": Im Fall $\dim U = \infty$ ist die Behauptung trivial. Ist $(u_1, ..., u_m)$ eine Basis von U, so ist nach (b) $f(u_1), \ldots, f(u_m)$ ein Erzeugendensystem von $f(U)$ und somit $\dim f(U) \leq m = \dim U$.

(d) 1. $f(0) = 0 \in W' \Rightarrow 0 \in f^{-1}(W')$. 2. $x \in f^{-1}(W') \ \Rightarrow \ f(x) \in W' \ \Rightarrow \ f(\lambda x) = \lambda f(x) \in W' \ \Rightarrow \ \lambda x \in f^{-1}(W')$. 3. $x, y \in f^{-1}(W') \Rightarrow f(x), f(y) \in W' \Rightarrow f(x+y) = f(x) + f(y) \in W' \Rightarrow x + y \in f^{-1}(W')$.

(e) f injektiv $\iff \forall x, x' \in V(f(x) = f(x') \Rightarrow x = x') \overset{f \text{ lin.}}{\iff} \forall x, x' \in V(f(x - x') = 0 \Rightarrow x - x' = 0) \iff$
$\iff \forall z \in V(z \in \text{Ker}(f) \Rightarrow z = 0) \iff \text{Ker}(f) = \{0\}$.

14.12.2009

Definition. Eine lineare Abbildung $f : V \to W$ heißt ein

Mono-	bzw. *Epi-*	bzw. *Iso-*	bzw. *Endo-*	bzw. *Automorphismus*	, falls gilt
f injektiv	bzw. f surjektiv	bzw. f bijektiv	bzw. $V = W$	bzw. f bijektiv & $V = W$.	

Lemma 5.3.
Ist $f: V \to W$ ein Isomorphismus, so ist auch $f^{-1}: W \to V$ Isomorphismus.

Beweis :

1. f^{-1} bijektiv: siehe §2.
2. f^{-1} linear: Seien $x, y \in W$ und $\lambda \in K$.

$f(f^{-1}(x) + f^{-1}(y)) = f(f^{-1}(x)) + f(f^{-1}(y)) = x + y = f(f^{-1}(x+y)) \;\Rightarrow\; f^{-1}(x) + f^{-1}(y) = f^{-1}(x+y)$.
$f(\lambda f^{-1}(x)) = \lambda f(f^{-1}(x)) = \lambda x = f(f^{-1}(\lambda x)) \;\Rightarrow\; \lambda f^{-1}(x) = f^{-1}(\lambda x)$.

Lemma 5.4. (Lineare Fortsetzung).
Seien V, W Vektorräume über K und $(v_1, ..., v_n)$ eine Basis von V. Dann gibt es zu jedem n-tupel $(w_1, ..., w_n)$ von Vektoren in W genau eine lineare Abbildung $f: V \to W$ mit $f(v_i) = w_i$ für $i = 1, ..., n$.

Beweis :

Existenz: Zu $x \in V$ existieren eindeutig $\lambda_1, ..., \lambda_n$ mit $x = \sum_{i=1}^n \lambda_i v_i$; wir definieren $f(x) := \sum_{i=1}^n \lambda_i w_i$.
Für $x = \sum_{i=1}^n \lambda_i v_i$ und $y = \sum_{i=1}^n \mu_i v_i$ gilt $f(x+y) = f(\sum_{i=1}(\lambda_i + \mu_i)v_i) = \sum_{i=1}^n (\lambda_i + \mu_i) w_i =$
$= \sum_{i=1}^n \lambda_i w_i + \sum_{i=1}^n \mu_i w_i = f(x) + f(y)$. Ferner $f(\mu x) = f(\sum_{i=1}^n \mu \lambda_i v_i) = \sum_{i=1}^n \mu \lambda_i w_i = \mu f(x)$.
Eindeutigkeit: Sei auch $g: V \to W$ linear mit $g(v_i) = w_i$.
Dann $g(x) = g(\sum_{i=1}^n \lambda_i v_i) = \sum_{i=1}^n \lambda_i g(v_i) = \sum_{i=1}^n \lambda_i w_i = f(x)$.

Lemma 5.5.
Seien V, W Vektorräume über K, $(v_1, ..., v_n)$ eine Basis von V und $f: V \to W$ linear. Dann gilt:
(a) f injektiv $\iff$ $f(v_1), ..., f(v_n)$ linear unabhängig.
(b) f Isomorphismus $\iff$ $(f(v_1), ..., f(v_n))$ ist Basis von W.

Beweis :

(a) "$\Rightarrow$": $\sum_{i=1}^n \lambda_i f(v_i) = 0 \;\Rightarrow\; f(\sum_{i=1}^n \lambda_i v_i) = 0 \;\Rightarrow\; \sum_{i=1}^n \lambda_i v_i = 0 \;\Rightarrow\; \lambda_1 = ... = \lambda_n = 0$.
"$\Leftarrow$": Sei $x = \sum_{i=1}^n \lambda_i v_i \in V$ mit $f(x) = 0$. Z.z.: $x = 0$.
$f(\sum_{i=1}^n \lambda_i v_i) = 0 \;\Rightarrow\; \sum_{i=1}^n \lambda_i f(v_i) = 0 \;\Rightarrow\; \lambda_1 = ... = \lambda_n = 0 \;\Rightarrow\; x = 0$.
(b) $f(V) = W$ & f injektiv $\overset{5.2}{\Leftrightarrow}$ span$(f(v_1), ..., f(v_n)) = W$ & f injektiv $\overset{(a)}{\Leftrightarrow}$ $(f(v_1), ..., f(v_n))$ Basis von W.

Lemma 5.6.
Je zwei n-dimensionale Vektorräume V, W über K sind isomorph zueinander,
d.h. es existiert ein Isomorphismus $f: V \to W$.

Beweis :

Sei $(v_1, ..., v_n)$ Basis von V und $(w_1, ..., w_n)$ Basis von W. Nach 5.4 existiert eine lineare Abbildung $f: V \to W$ mit $f(v_i) = w_i$. Nach 5.5 ist f ein Isomorphismus.

Satz 5.7. (Dimensionsformel für lineare Abbildungen)
Sei V endlichdimensionaler Vektorraum und $f: V \to W$ eine lineare Abbildung.
Dann gilt $\dim \mathrm{Ker}(f) + \dim \mathrm{Im}(f) = \dim V$.

Beweis :

Sei $v_1, ..., v_k$ eine Basis von Ker(f). Wir ergänzen diese zu einer Basis $v_1, ..., v_k, ..., v_n$ von V.

Beh.: $f(v_{k+1}), ..., f(v_n)$ ist Basis von $\mathrm{Im}(f)$, und somit $\dim \mathrm{Ker}(f) + \dim \mathrm{Im}(f) = k + (n-k) = n$.

Bew.: Erzeugendensystem: $\mathrm{Im}(f) = \mathrm{span}(f(v_1), ..., f(v_n)) = \mathrm{span}(f(v_{k+1}), ..., f(v_n))$.

Linear unabhängig: $\sum_{i=k+1}^{n} \lambda_i f(v_i) = 0 \;\Rightarrow\; f(\sum_{i=k+1}^{n} \lambda_i v_i) = 0 \;\Rightarrow\; \sum_{i=k+1}^{n} \lambda_i v_i \in \mathrm{Ker}(f) \;\Rightarrow$
$\Rightarrow$ es gibt $\lambda_1, ..., \lambda_k$ mit $-\sum_{i=k+1}^{n} \lambda_i v_i = \sum_{i=1}^{k} \lambda_i v_i \;\Rightarrow\; \sum_{i=1}^{n} \lambda_i v_i = 0 \;\Rightarrow\; \lambda_1 = ... = \lambda_n = 0$.

Lemma 5.8.
Seien $f : V \to W$ und $g : W \to V$ lineare Abbildungen, und sei $\dim V = \dim W < \infty$. Dann gilt:
(a) f injektiv $\iff$ f surjektiv,
(b) $g \circ f = \mathrm{id}_V \implies f$ bijektiv und $g = f^{-1}$, also $f \circ g = \mathrm{id}_W$.

Beweis :
(a) Nach 5.7 gilt: $\dim \mathrm{Ker}(f) + \dim \mathrm{Im}(f) = \dim V = \dim W$. Folglich:
f injektiv $\Leftrightarrow$ $\dim \mathrm{Ker}(f) = 0 \Leftrightarrow \dim \mathrm{Im}(f) = \dim W \Leftrightarrow \mathrm{Im}(f) = W \Leftrightarrow f$ surjektiv.

16.12.2009

(b) $g \circ f = \mathrm{id}_V \Rightarrow f$ injektiv $\overset{(a)}{\Rightarrow} f$ bijektiv $\Rightarrow f^{-1}$ existiert $\overset{\mathrm{id}_V = g\circ f}{\Rightarrow} f^{-1} = (g \circ f) \circ f^{-1} = g \circ \mathrm{id}_W = g$.

Korollar. $A, B \in K^{n\times n}$ & $AB = E \;\Rightarrow\; A, B$ invertierbar.

Beweis: $AB = E \;\Rightarrow\; \mathsf{f}_A \circ \mathsf{f}_B = \mathsf{f}_{AB} = \mathsf{f}_E = \mathrm{id}_{K^n} \;\Rightarrow\; \mathsf{f}_{BA} = \mathsf{f}_B \circ \mathsf{f}_A \overset{5.8b}{=} \mathrm{id}_{K^n} = \mathsf{f}_E \;\Rightarrow\; BA = E$.

Lemma 5.9. Für $A \in K^{n\times n}$ gilt:
(a) A invertierbar $\iff$ $\mathsf{f}_A : K^n \to K^n$ bijektiv;
(b) Ist A invertierbar, so $(\mathsf{f}_A)^{-1} = \mathsf{f}_{A^{-1}}$.

Beweis:
1. A invertierbar $\Rightarrow$ $\mathsf{f}_{A^{-1}} \circ \mathsf{f}_A \overset{5.1c}{=} \mathsf{f}_{A^{-1}A} = \mathsf{f}_E = \mathrm{id}_{K^n} \overset{5.8b}{\Rightarrow} \mathsf{f}_A$ bijektiv & $\mathsf{f}_{A^{-1}} = (\mathsf{f}_A)^{-1}$.
2. f_A bijektiv $\overset{L.5.3,5.1b}{\Rightarrow}$ $(\exists B)\, (\mathsf{f}_A)^{-1} = \mathsf{f}_B \;\Rightarrow\; \mathsf{f}_{AB} = \mathsf{f}_A \circ \mathsf{f}_B = \mathrm{id}_{K^n} = \mathsf{f}_E \;\Rightarrow\; AB = E \;\Rightarrow\; A$ invertierbar.

Lemma 5.10 und Definition (Der Vektorraum $\mathrm{Hom}(V, W)$).
Seien V, W Vektorräume über K, und sei $\mathrm{Hom}(V, W)$ die Menge aller linearen Abbildungen von V nach W.

$\mathrm{Hom}(V, W)$ ist ein Untervektorraum von $\mathrm{Abb}(V, W)$, dem Vektorraum aller Abbildungen von V nach W (mit der punktweisen Addition und skalaren Multiplikation).

Beweis :
1. Die Nullabbildung $\mathbf{0} : V \to W$, $\mathbf{0}(x) := 0$ ist linear.
2. $f, g \in \mathrm{Hom}(V, W) \;\Rightarrow\; f + g \in \mathrm{Hom}(V, W)$:
$(f+g)(x+y) \overset{\mathrm{Def}}{=} f(x+y) + g(x+y) \overset{f,g \text{ linear}}{=} f(x) + f(y) + g(x) + g(y) \overset{\mathrm{Def}}{=} (f+g)(x) + (f+g)(y)$.
$(f+g)(\lambda x) \overset{\mathrm{Def}}{=} f(\lambda x) + g(\lambda x) \overset{f,g \text{ linear}}{=} \lambda f(x) + \lambda g(x) \overset{\mathrm{Def}}{=} \lambda(f+g)(x)$.
3. $f \in \mathrm{Hom}(V, W)$ & $\mu \in K \;\Rightarrow\; \mu{\cdot}f \in \mathrm{Hom}(V, W)$: ähnlich wie 2.

Bemerkungen.
1. Die Abbildung $K^{m\times n} \to \mathrm{Hom}(K^n, K^m)$, $A \mapsto \mathsf{f}_A$ ist ein Isomorphismus. (Dies folgt aus Lemma 5.1a,b und $\mathsf{f}_{\lambda A + \mu B}(x) = (\lambda A + \mu B)x = \lambda Ax + \mu Bx = \lambda \mathsf{f}_A(x) + \mu \mathsf{f}_B(x) = (\lambda \mathsf{f}_A + \mu \mathsf{f}_B)(x)$.)
2. $\mathrm{End}(V) := \mathrm{Hom}(V, V)$ zusammen mit der Komposition von Abbildungen, $(f, g) \mapsto f{\circ}g$, als Multiplikation ist ein Ring, der sog. *Endomorphismenring* von V.

Lemma 5.11 und Definition. Ist $V = U_0 \oplus U_1$, so gilt:

(a) Es gibt genau ein Paar linearer Abbildungen $p_0 : V \to U_0$, $p_1 : V \to U_1$ mit $\forall v \in V\,(\,v = p_0(v) + p_1(v)\,)$.

Man nennt p_0, p_1 die zu der direkten Zerlegung $V = U_0 \oplus U_1$ gehörenden *Projektionen.*

(b) Für die Projektionen p_i aus (a) gilt: (i) $U_i = \mathrm{Im}(p_i) = \mathrm{Ker}(p_{1-i})$ und (ii) $p_i \circ p_i = p_i$.

Beweis :

(a) Nach Lemma 4.11 gibt es zu jedem $v \in V$ genau ein Paar $(u_0, u_1) \in U_0 \times U_1$ mit $v = u_0 + u_1$.
Also existiert genau ein Paar von Abbildungen $p_0 : V \to U_0$, $p_1 : V \to U_1$ mit $\forall v \in V(v = p_0(v) + p_1(v))$.
Bleibt die Linearität von p_i zu zeigen. Aus $p_0(x+y) + p_1(x+y) = x + y = p_0(x) + p_1(x) + p_0(y) + p_1(y) = (p_0(x) + p_0(y)) + (p_1(x) + p_1(y))$ folgt mit Lemma 4.11 $p_i(x+y) = p_i(x) + p_i(y)$. Aus $p_0(\lambda x) + p_1(\lambda x) = \lambda x = \lambda(p_0(x) + p_1(x)) = \lambda p_0(x) + \lambda p_1(x)$ folgt mit Lemma 4.11 $p_i(\lambda x) = \lambda p_i(x)$.

(b) (i) $x \in U_0 \Rightarrow p_0(x) = x \;\&\; p_1(x) = 0 \Rightarrow x \in \mathrm{Im}(p_0) \;\&\; x \in \mathrm{Ker}(p_1)$.
$x \in \mathrm{Ker}(p_1) \Rightarrow p_1(x) = 0 \Rightarrow x = p_0(x) \in \mathrm{Im}(p_0)$.
(ii) Aus $\forall y \in U_i(p_i(y) = y)$ folgt $\forall x \in V(p_i(p_i(x)) = p_i(x))$.

Lemma 5.12.
Ist $f : V \to V$ linear mit $f \circ f = f$, so gilt

(a) $V = \mathrm{Im}(f) \oplus \mathrm{Ker}(f)$,

(b) f und $\mathrm{id}_V - f$ sind die zu der direkten Zerlegung $V = \mathrm{Im}(f) \oplus \mathrm{Ker}(f)$ gemäß 5.11 gehörenden Projektionen.

Beweis :

1. $y \in \mathrm{Im}(f) \cap \mathrm{Ker}(f) \Rightarrow$ es gibt $x \in V$ mit $y = f(x) = f(f(x)) = f(y) = 0$.
2. Für jedes $x \in V$ gilt $x = f(x) + (\mathrm{id} - f)(x)$ und $f((\mathrm{id} - f)(x)) = f(x) - f(f(x)) = f(x) - f(x) = 0$, d.h. $(\mathrm{id} - f)(x) \in \mathrm{Ker}(f)$.

Berechnung der Inversen einer invertierbaren Matrix

Lemma 1.7 kann auf endliche Folgen von elementaren Zeilenumformunge ausgedehnt werden.

Lemma 1.7b'. Für $A \in K^{m\times n}$ und $\vec{\mathcal{Z}} = (\mathcal{Z}_l, \ldots, \mathcal{Z}_1)$ mit $\mathcal{Z}_1, \ldots, \mathcal{Z}_l \in \mathrm{EZU}_m$ gilt: $\vec{\mathcal{Z}}(A) = \vec{\mathcal{Z}}(E_m) \cdot A$.
Dabei sei $\vec{\mathcal{Z}}(A) := \mathcal{Z}_l(\ldots \mathcal{Z}_2(\mathcal{Z}_1(A)) \ldots)$.)

Lemma 5.13. Für alle $A \in K^{n\times n}$ und $\mathcal{Z} \in \mathrm{EZU}_n$ gilt:

(1) $\mathcal{Z}(E_n)$ invertierbar.
(2) A invertierbar $\Rightarrow$ $\mathcal{Z}(A)$ invertierbar.
(3) $\vec{\mathcal{Z}}(A) = E_n \Rightarrow$ A invertierbar und $A^{-1} = \vec{\mathcal{Z}}(E)$.
(4) A invertierbar $\Rightarrow$ es gibt $\vec{\mathcal{Z}}$ mit $\vec{\mathcal{Z}}(A) = E_n$.

Beweis:

(1) Sei $\mathcal{Z}'$ die zu $\mathcal{Z}$ "inverse" elementare Zeilenumformung. Dann $E_n = \mathcal{Z}'(\mathcal{Z}(E_n)) \overset{1.7\mathrm{b}}{=} \mathcal{Z}'(E_n) \cdot \mathcal{Z}(E_n)$.

(2) Nach 1.7b ist $\mathcal{Z}(A) = \mathcal{Z}(E_n) \cdot A$. Mit (1) und Lemma 3.2 folgt daraus die Behauptung.

(3) Die Behauptung folgt aus $E_n = \vec{\mathcal{Z}}(A) \overset{1.7\mathrm{b}'}{=} \vec{\mathcal{Z}}(E_n) \cdot A$.

(4) Es gibt $\vec{\mathcal{Z}}$, so daß $S := \vec{\mathcal{Z}}(A)$ eine ausgezeichnete Stufenmatrix ist.
Nach (2) ist S auch invertierbar; folglich muß $S = E_n$ gelten.

Man erhält also die Inverse einer invertierbaren Matrix $A \in K^{n\times n}$, indem man A durch elementare Zeilenumformungen in die Einheitsmatrix E_n transformiert und parallel dazu dieselben Umformungen an E_n ausführt.

Beispiel. Sei $A = \begin{pmatrix} 1 & 2 & 1 \\ 0 & -1 & 0 \\ 2 & 0 & -1 \end{pmatrix}$. $\begin{pmatrix} 1 & 2 & 1 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 & 1 & 0 \\ 2 & 0 & -1 & 0 & 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & -1 & 0 \\ 0 & -4 & -3 & -2 & 0 & 1 \end{pmatrix} \to$

$\to \begin{pmatrix} 1 & 0 & 1 & 1 & 2 & 0 \\ 0 & 1 & 0 & 0 & -1 & 0 \\ 0 & 0 & 3 & 2 & 4 & -1 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & \frac{1}{3} & \frac{2}{3} & \frac{1}{3} \\ 0 & 1 & 0 & 0 & -1 & 0 \\ 0 & 0 & 1 & \frac{2}{3} & \frac{4}{3} & \frac{-1}{3} \end{pmatrix}$. Also $A^{-1} = \begin{pmatrix} \frac{1}{3} & \frac{2}{3} & \frac{1}{3} \\ 0 & -1 & 0 \\ \frac{2}{3} & \frac{4}{3} & \frac{-1}{3} \end{pmatrix}$.

21.12.2009

Lemma 5.14.

Seien $v_1, \ldots, v_n \in K^n$ und sei $(v_1 \ \ldots \ v_n)$ die $n\times n$-Matrix mit den Spalten $v_1, \ldots, v_n$.

Dann gilt: $(v_1, \ldots, v_n)$ linear unabhängig $\Leftrightarrow$ $(v_1 \ \ldots \ v_n)$ invertierbar.

Beweis:

Sei $A := (v_1 \ \ldots \ v_n)$. Dann $v_j = \mathsf{f}_A(e_j)$ und somit:

$(v_1, \ldots, v_n)$ lin. unabh. $\overset{5.5a}{\Leftrightarrow}$ f_A injektiv $\overset{5.9a}{\Leftrightarrow}$ A invertierbar.

§6 Darstellende Matrix, Basistransformationen

Definition (Darstellende Matrix einer linearen Abbildung).

Seien V, W K-Vektorräume mit den Basen $\overline{v} = (v_1, \ldots, v_n)$, $\overline{w} = (w_1, \ldots, w_m)$, und sei $f \in \mathrm{Hom}(V, W)$.

$\mathcal{M}^{\overline{v}}_{\overline{w}}(f) := \big(a_{ij}\big)_{\substack{i=1,\ldots,m,\\ j=1,\ldots,n}}$ wobei $f(v_j) = \sum\limits_{i=1}^{m} a_{ij} w_i$ für $j = 1, \ldots, n$.

$\mathcal{M}^{\overline{v}}_{\overline{w}}(f)$ heißt die *darstellende Matrix von* f (oder die f *zugeordnete Matrix*) *bzgl. der Basen* $\overline{v}$, $\overline{w}$.

Ist $V = W$ und $\overline{v} = \overline{w}$, so setzt man $\mathcal{M}_{\overline{v}}(f) := \mathcal{M}^{\overline{v}}_{\overline{w}}(f)$ und nennt $\mathcal{M}_{\overline{v}}(f)$ die *darstellende Matrix von* f *bzgl. der Basis* $\overline{v}$.

Für $f \in \mathrm{Hom}(K^n, K^m)$ sei $\mathcal{M}(f)$ die darstellende Matrix von f bzgl. der kanonischen Basen.

Lemma 6.1.

(a) Für jede Matrix A gilt $A = \mathcal{M}(\mathsf{f}_A)$. Für jede lineare Abbildung $f : K^n \to K^m$ gilt $f = \mathsf{f}_{\mathcal{M}(f)}$.

(b) $f \in \mathrm{Hom}(K^n, K^m)$ & $g \in \mathrm{Hom}(K^m, K^p) \Rightarrow \mathcal{M}(g \circ f) = \mathcal{M}(g) \cdot \mathcal{M}(f)$.

Beweis:

(a) 1. $\mathsf{f}_A(e^n_j) = Ae^n_j = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix} = \sum_{i=1}^{m} a_{ij} e^m_i$. 2. Nach L.5.1b existiert A mit $f = \mathsf{f}_A$.
Mit $A = \mathcal{M}(\mathsf{f}_A)$ folgt daraus $f = \mathsf{f}_{\mathcal{M}(f)}$.

(b) Sei $A \in K^{m\times n}$, $B \in K^{p\times m}$ mit $f = \mathsf{f}_A$ und $g = \mathsf{f}_B$. Dann $\mathcal{M}(g \circ f) = \mathcal{M}(\mathsf{f}_{BA}) = BA = \mathcal{M}(g) \cdot \mathcal{M}(f)$.

Definition.

Ist V ein K-Vektorraum und $\overline{v} = (v_1, \ldots, v_n)$ eine Basis von V, so definieren wir

$$\Phi_{\overline{v}} : K^n \to V, \quad \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \sum_{j=1}^{n} x_j v_j.$$

Offenbar ist $\Phi_{\overline{v}} : K^n \to V$ ein Isomorphismus. Man nennt $\Phi_{\overline{v}}$ den *kanonischen Basisisomorphismus zur Basis* $\overline{v}$ oder das *durch* $\overline{v}$ *bestimmte Koordinatensystem in* V.

Für $a \in V$ nennt man $\Phi^{-1}_{\overline{v}}(a)$ den *Koordinatenvektor* oder die *Koordinaten* von a bzgl. $\overline{v}$.

Bemerkungen:

1. $\Phi_{(v_1,\ldots,v_n)}$ ist der nach 5.4, 5.5 eindeutig bestimmte Isomorphismus, der die Einheitsvektoren des K^n auf die Basisvektoren $v_1, \ldots, v_n$ abbildet.
2. Die Spalten der darstellenden Matrix $\mathcal{M}^{\overline{v}}_{\overline{w}}(f)$ einer linearen Abbildung $f : V \to W$ sind die Koordinatenvektoren (bzgl. $\overline{w}$) der Bilder der Basisvektoren $v_1, \ldots, v_n$.
3. Ist $V = K^n$, so $\mathcal{M}(\Phi_{\overline{v}}) = (v_1 \ \ldots \ v_n)$, i.e. die $n \times n$-Matrix mit den Spalten $v_1, \ldots, v_n$.

Lemma 6.2.

Sind V, W K-Vektorräume mit den Basen $\overline{v} = (v_1, \ldots, v_n)$, $\overline{w} = (w_1, \ldots, w_m)$, so gilt für $f \in \mathrm{Hom}(V, W)$:

$$\mathcal{M}^{\overline{v}}_{\overline{w}}(f) = \mathcal{M}(\Phi^{-1}_{\overline{w}} \circ f \circ \Phi_{\overline{v}}) \text{ bzw. } \mathsf{f}_A = \Phi^{-1}_{\overline{w}} \circ f \circ \Phi_{\overline{v}} \text{ mit } A := \mathcal{M}^{\overline{v}}_{\overline{w}}(f).$$

Beweis:

Mit $A := \mathcal{M}^{\overline{v}}_{\overline{w}}(f)$ gilt: $(\Phi^{-1}_{\overline{w}} \circ f \circ \Phi_{\overline{v}})(e_j) = \Phi^{-1}_{\overline{w}}(f(v_j)) = \Phi^{-1}_{\overline{w}}(\sum\limits_{i=1}^{m} a_{ij} w_i) = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix} = \mathsf{f}_A(e_j)$.

Korollar.
Für $f \in \mathrm{Hom}(V,W)$ und $v \in V$ mit den Koordinaten $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ bzgl. $\overline{v}$ gilt:

$\mathcal{M}_{\overline{w}}^{\overline{v}}(f) \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ ist der Koordinatenvektor von $f(v)$ bzgl. $\overline{w}$.

Satz 6.3.
Sei $\overline{v} := (v_1, \ldots, v_n)$ Basis von V, $\overline{u} := (u_1, \ldots, u_p)$ Basis von U, $\overline{w} := (w_1, \ldots, w_m)$ Basis von W, und seien $f : V \to U$, $g : U \to W$ lineare Abbildungen. Dann gilt $\mathcal{M}_{\overline{w}}^{\overline{v}}(g \circ f) = \mathcal{M}_{\overline{w}}^{\overline{u}}(g) \cdot \mathcal{M}_{\overline{u}}^{\overline{v}}(f)$.

Beweis:
$\mathcal{M}_{\overline{w}}^{\overline{v}}(g \circ f) = \mathcal{M}(\Phi_{\overline{w}}^{-1} \circ g \circ f \circ \Phi_{\overline{v}}) = \mathcal{M}(\Phi_{\overline{w}}^{-1} \circ g \circ \Phi_{\overline{u}} \circ \Phi_{\overline{u}}^{-1} \circ f \circ \Phi_{\overline{v}}) \overset{6.1b}{=}$
$= \mathcal{M}(\Phi_{\overline{w}}^{-1} \circ g \circ \Phi_{\overline{u}}) \cdot \mathcal{M}(\Phi_{\overline{u}}^{-1} \circ f \circ \Phi_{\overline{v}}) = \mathcal{M}_{\overline{w}}^{\overline{u}}(g) \cdot \mathcal{M}_{\overline{u}}^{\overline{v}}(f)$.

Satz 6.4.
Sei $\overline{v} = (v_1, \ldots, v_n)$ Basis von K^n, $\overline{w} = (w_1, \ldots, w_m)$ Basis von K^m und $A \in K^{m \times n}$.

Dann gilt $\mathcal{M}_{\overline{w}}^{\overline{v}}(\mathsf{f}_A) = (w_1 \ \ldots \ w_m)^{-1} \cdot A \cdot (v_1 \ \ldots \ v_n)$.

Beweis:
$\mathcal{M}_{\overline{w}}^{\overline{v}}(\mathsf{f}_A) = \mathcal{M}(\Phi_{\overline{w}}^{-1} \circ \mathsf{f}_A \circ \Phi_{\overline{v}}) = \mathcal{M}(\Phi_{\overline{w}}^{-1}) \cdot \mathcal{M}(\mathsf{f}_A) \cdot \mathcal{M}(\Phi_{\overline{v}}) = (w_1 \ \ldots \ w_m)^{-1} \cdot A \cdot (v_1 \ \ldots \ v_n)$.

oder

Sei $C = (c_{ij}) := \mathcal{M}_{\overline{w}}^{\overline{v}}(\mathsf{f}_A)$ und c_j die j-te Spalte von C. Dann gilt: $Av_j = \mathsf{f}_A(v_j) \overset{\text{Def. von } C}{=} \sum_{i=1}^m c_{ij} w_i \overset{\text{L.1.5b}}{=}$
$= (w_1 \ \ldots \ w_m) \cdot c_j$ und somit $(w_1 \ \ldots \ w_m)^{-1} A v_j = c_j$ $(j = 1, ..., n)$.

Beispiel.
Sei $A = \begin{pmatrix} 1 & 1 & -1 \\ 0 & 3 & 5 \end{pmatrix}$, $v_1 := \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$, $v_2 := \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$, $v_3 := \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$, $w_1 := \begin{pmatrix} 3 \\ 4 \end{pmatrix}$, $w_2 := \begin{pmatrix} 2 \\ 1 \end{pmatrix}$.

Sei ferner mit $(c_{ij}) = \mathcal{M}_{\overline{w}}^{\overline{v}}(\mathsf{f}_A)$. Dann gilt $\mathsf{f}_A(v_1) = \begin{pmatrix} 0 \\ 5 \end{pmatrix}$, $\mathsf{f}_A(v_2) = \begin{pmatrix} 1 \\ 8 \end{pmatrix}$, $\mathsf{f}_A(v_3) = \begin{pmatrix} 2 \\ 3 \end{pmatrix}$ und

$\mathsf{f}_A(v_j) = c_{1j} w_1 + c_{2j} w_2 = c_{1j} \begin{pmatrix} 3 \\ 4 \end{pmatrix} + c_{2j} \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ 4 & 1 \end{pmatrix} \cdot \begin{pmatrix} c_{1j} \\ c_{2j} \end{pmatrix}$ $(j = 1, 2, 3)$. Folglich
$\begin{pmatrix} 0 & 1 & 2 \\ 5 & 8 & 3 \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ 4 & 1 \end{pmatrix} \cdot (c_{ij})$ und somit $(c_{ij}) = \begin{pmatrix} 3 & 2 \\ 4 & 1 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 0 & 1 & 2 \\ 5 & 8 & 3 \end{pmatrix} \overset{(*)}{=} \frac{1}{5} \begin{pmatrix} -1 & 2 \\ 4 & -3 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & 2 \\ 5 & 8 & 3 \end{pmatrix}$.

$$(*) \quad \begin{pmatrix} 3 & 2 & 1 & 0 \\ 4 & 1 & 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & \frac{2}{3} & \frac{1}{3} & 0 \\ 4 & 1 & 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & \frac{2}{3} & \frac{1}{3} & 0 \\ 0 & -\frac{5}{3} & -\frac{4}{3} & 1 \end{pmatrix} \to \begin{pmatrix} 1 & \frac{2}{3} & \frac{1}{3} & 0 \\ 0 & 1 & \frac{4}{5} & -\frac{3}{5} \end{pmatrix} \to \begin{pmatrix} 1 & 0 & \frac{-1}{5} & \frac{2}{5} \\ 0 & 1 & \frac{4}{5} & \frac{-3}{5} \end{pmatrix}$$

Abkürzung.
Für $r \leq \min\{m, n\}$ sei $E_r^{m \times n} := \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix} \in K^{m \times n}$,

d.h. $E_r^{m \times n} := (a_{ij}) \in K^{m \times n}$ mit $a_{11} = \ldots = a_{rr} = 1$ und $a_{ij} = 0$ sonst.

Satz 6.5.
Seien V, W endlichdimensionale K-Vektorräume und $f : V \to W$ linear mit $r = \dim \mathrm{Im}(f)$.

Dann gibt es Basen $\overline{v}$ von V und $\overline{w}$ von W, so daß $\mathcal{M}_{\overline{w}}^{\overline{v}}(f) = E_r^{m \times n}$.

Beweis:
Sei $(v_1, \dots, v_n)$ Basis von V, so daß $\mathrm{Ker}(f) = \mathrm{span}(v_{r+1}, \dots, v_n)$. Dann ist $(f(v_1), \dots, f(v_r))$ eine Basis von $\mathrm{Im}(f)$. Folglich existiert eine Basis $\overline{w} = (w_1, \dots, w_m)$ von W mit $f(v_j) = w_j$ für $j = 1, \dots, r$. Die Behauptung ergibt sich nun unmittelbar aus der Definition von $\mathcal{M}_{\overline{w}}^{\overline{v}}(f)$.

11.01.2010

Definition (Basiswechsel).

Seien $\overline{v} = (v_1, \dots, v_n)$ und $\overline{w} = (w_1, \dots, w_n)$ Basen des K-Vektorraums V.

$T_{\overline{w}}^{\overline{v}} := \mathcal{M}_{\overline{w}}^{\overline{v}}(\mathrm{id}_V)$ heißt die *Transformationsmatrix des Basiswechsels* $\overline{v}$*,* $\overline{w}$.

Satz 6.6 (Transformationsformel).

Sei $f : V \to W$ eine lineare Abbildung, und seien $\overline{v}$, $\overline{v'}$ Basen von V, sowie $\overline{w}$, $\overline{w'}$ Basen von W.

Dann gilt: $\mathcal{M}_{\overline{w'}}^{\overline{v'}}(f) = T_{\overline{w'}}^{\overline{w}} \cdot \mathcal{M}_{\overline{w}}^{\overline{v}}(f) \cdot T_{\overline{v}}^{\overline{v'}}$.

Beweis:
$T_{\overline{w'}}^{\overline{w}} \cdot \mathcal{M}_{\overline{w}}^{\overline{v}}(f) \cdot T_{\overline{v}}^{\overline{v'}} = \mathcal{M}_{\overline{w'}}^{\overline{w}}(\mathrm{id}_W) \cdot \mathcal{M}_{\overline{w}}^{\overline{v}}(f) \cdot \mathcal{M}_{\overline{v}}^{\overline{v'}}(\mathrm{id}_V) = \mathcal{M}_{\overline{w'}}^{\overline{v'}}(\mathrm{id}_W \circ f \circ \mathrm{id}_V) = \mathcal{M}_{\overline{w'}}^{\overline{v'}}(f)$.

Korollar.
Ist $f \in \mathrm{Hom}(V, V)$ und sind $\overline{v}$, $\overline{w}$ Basen von V, so gilt $\mathcal{M}_{\overline{w}}(f) = (T_{\overline{v}}^{\overline{w}})^{-1} \cdot \mathcal{M}_{\overline{v}}(f) \cdot T_{\overline{v}}^{\overline{w}}$.

Lemma 6.7.
Sind $\overline{v} = (v_1, \dots, v_n)$ und $\overline{w} = (w_1, \dots, w_n)$ Basen des K-Vektorraums V, so gilt:

(a) $T_{\overline{w}}^{\overline{v}}$ invertierbar und $(T_{\overline{w}}^{\overline{v}})^{-1} = T_{\overline{v}}^{\overline{w}}$.

(b) $T_{\overline{w}}^{\overline{v}} = (c_{ij}) \in K^{n \times n}$ mit $v_j = \sum\limits_{i=1}^{n} c_{ij} w_i$.

(c) Ist $\sum\limits_{j=1}^{n} x_j v_j = \sum\limits_{i=1}^{n} y_i w_i$, so $\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = T_{\overline{w}}^{\overline{v}} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$.

(d) Ist $V = K^n$, so $T_{\overline{w}}^{\overline{v}} = (w_1 \ \dots \ w_n)^{-1} \cdot (v_1 \ \dots \ v_n)$.
Ist insbesondere $\overline{w}$ [bzw. $\overline{v}$] die kanonische Basis, so $T_{\overline{w}}^{\overline{v}} = (v_1 \ \dots \ v_n)$ [bzw. $(w_1 \ \dots \ w_n)^{-1}$].

Beweis:
(a) $T_{\overline{v}}^{\overline{w}} \cdot T_{\overline{w}}^{\overline{v}} = \mathcal{M}_{\overline{v}}^{\overline{w}}(\mathrm{id}_V) \cdot \mathcal{M}_{\overline{w}}^{\overline{v}}(\mathrm{id}_V) \overset{6.3}{=} \mathcal{M}_{\overline{v}}^{\overline{v}}(\mathrm{id}_V) = E_n$. (b) Definition. (c) Korollar zu 6.2.
(d) $T_{\overline{w}}^{\overline{v}} = \mathcal{M}_{\overline{w}}^{\overline{v}}(\mathrm{id}_{K^n}) = \mathcal{M}_{\overline{w}}^{\overline{v}}(\mathsf{f}_E) \overset{6.4}{=} (w_1 \ \dots \ w_n)^{-1} \cdot E \cdot (v_1 \ \dots \ v_n)$.

Lemma 6.8
Seien V und W K-Vektorräume mit Basen $\overline{v} = (v_1, \dots, v_n)$ und $\overline{w} = (w_1, \dots, w_m)$.
(a) Die Abbildung $\mathcal{M}_{\overline{w}}^{\overline{v}} : \mathrm{Hom}(V, W) \to K^{m \times n}$, $f \mapsto \mathcal{M}_{\overline{w}}^{\overline{v}}(f)$ ist ein Isomorphismus.
(b) $\dim \mathrm{Hom}(V, W) = \dim(V) \cdot \dim(W)$

Beweis:
(a) 1. linear: Übung. 2. bijektiv: $A = (a_{ij}) \in K^{m \times n} \overset{\text{L.5.4}}{\Rightarrow} \exists! f \in \mathrm{Hom}(V, W)$ mit $f(v_j) = \sum_{i=1}^{n} a_{ij} w_i$ für $j = 1, \dots, n \Rightarrow \exists! f \in \mathrm{Hom}(V, W)$ mit $\mathcal{M}_{\overline{w}}^{\overline{v}}(f) = A$.
(b) $\dim(\mathrm{Hom}(V, W)) \overset{\text{(a)}}{=} \dim(K^{m \times n}) \overset{(*)}{=} m \cdot n = \dim(V) \cdot \dim(W)$.
$(*)$ $(a_{ij})_{i,j} \mapsto (a_{11}, \dots, a_{1n}, a_{21}, \dots, a_{2n}, \dots, a_{m1}, \dots, a_{mn})$ ist ein Isomorphimus von $K^{m \times n}$ auf $K^{m \cdot n}$.

§7 Rang einer Matrix; Dualraum

Definitionen.

1. Sind V, W Vektorräume über K und ist $f \in \mathrm{Hom}(V,W)$, so sei $\mathrm{rang}(f) := \dim \mathrm{Im}(f)$.
2. Ist $A \in K^{m\times n}$ mit den Spalten $a_1, \ldots, a_n \in K^m$, so sei
   $\mathrm{rang}(A) := \mathrm{rang}(\mathsf{f}_A)$ und $\mathrm{SR}(A) := \mathrm{span}(a_1, ..., a_n) \subseteq K^m$ (Spaltenraum von A).

Lemma 7.1. Für $A \in K^{m\times n}$ gilt:

(a) $\mathrm{SR}(A) = \mathrm{Im}(\mathsf{f}_A)$ und somit $\mathrm{rang}(A) = \dim \mathrm{SR}(A)$.

(b) $m = n \Rightarrow (\, A$ invertierbar $\Leftrightarrow \mathrm{rang}(A) = n\,)$.

Beweis:

(a) $\mathrm{span}(a_1, ..., a_n) = \mathrm{span}(\mathsf{f}_A(e_1), ..., \mathsf{f}_A(e_n)) = \mathsf{f}_A(\mathrm{span}(e_1, ..., e_n)) = \mathrm{Im}(\mathsf{f}_A)$.

(b) A invertierbar $\overset{5.9\mathrm{a}}{\Leftrightarrow}$ f_A bijektiv $\overset{5.8\mathrm{a}}{\Leftrightarrow}$ $\mathrm{Im}(\mathsf{f}_A) = K^n \Leftrightarrow \dim \mathrm{Im}(\mathsf{f}_A) = n$.

-- **13.01.2010**

Lemma 7.2.

Sind V, W K-Vektorräume mit Basen $\overline{v}$, $\overline{w}$, so gilt $\mathrm{rang}(\mathcal{M}^{\overline{v}}_{\overline{w}}(f)) = \mathrm{rang}(f)$ für alle $f \in \mathrm{Hom}(V,W)$.

Beweis:

Sei $A := \mathcal{M}^{\overline{v}}_{\overline{w}}(f)$. Dann gilt $\mathrm{Im}(\mathsf{f}_A) = \mathsf{f}_A(K^n) \overset{\mathrm{L.6.2}}{=} \Phi^{-1}_{\overline{w}}(f(\Phi_{\overline{v}}(K^n))) = \Phi^{-1}_{\overline{w}}(f(V)) = \Phi^{-1}_{\overline{w}}(\mathrm{Im}(f))$.
Da $\Phi_{\overline{w}}$ ein Isomorphismus ist, folgt daraus $\dim \mathrm{Im}(\mathsf{f}_A) = \dim \mathrm{Im}(f)$.

Definition.

$A, B \in K^{m\times n}$ heißen *äquivalent*, wenn es Matrizen $S \in \mathrm{GL}(m;K)$ und $T \in \mathrm{GL}(n;K)$ mit $B = S{\cdot}A{\cdot}T$ gibt.

Lemma 7.3.

Für $A, B \in K^{m\times n}$ sind folgende Aussagen äquivalent zueinander:

(a) A, B sind äquivalent.

(b) Es gibt Basen $\overline{v}$ von K^n und $\overline{w}$ von K^m mit $B = \mathcal{M}^{\overline{v}}_{\overline{w}}(\mathsf{f}_A)$.

(c) $\mathrm{rang}(A) = \mathrm{rang}(B)$.

Beweis:

(a)$\Rightarrow$(b): Gelte $B = SAT$ mit $S \in \mathrm{GL}(m;K)$, $T \in \mathrm{GL}(n;K)$. Sei $S^{-1} = (w_1 \ldots w_m)$ und $T = (v_1 \ldots v_n)$. Nach 5.14 ist dann $\overline{w} := (w_1, \ldots, w_m)$ Basis von K^m und $\overline{v} := (v_1, \ldots, v_n)$ Basis von K^n. Mit 6.4 folgt $\mathcal{M}^{\overline{v}}_{\overline{w}}(\mathsf{f}_A) = S{\cdot}A{\cdot}T = B$.

(b)$\Rightarrow$(c): $\mathrm{rang}(A) = \mathrm{rang}(\mathsf{f}_A) \overset{\mathrm{L.7.2}}{=} \mathrm{rang}(\mathcal{M}^{\overline{v}}_{\overline{w}}(\mathsf{f}_A))$.

(c)$\Rightarrow$(a): Sei $r := \mathrm{rang}(A) = \mathrm{rang}(B)$. Nach 6.5 gibt es Basen $\overline{v}$, $\overline{w}$ mit $\mathcal{M}^{\overline{v}}_{\overline{w}}(\mathsf{f}_A) = E^{m\times n}_r$. Nach 6.4 ist also $E^{m\times n}_r = SAT$. Ebenso gibt es C, D mit $E^{m\times n}_r = CBD$. Es folgt $B = (C^{-1}S)A(TD^{-1})$.

Satz 7.4. Für $A \in K^{m\times n}$ gilt:

(a) $\mathrm{Lös}(A;0) = \mathrm{Ker}(\mathsf{f}_A)$.

(b) $\mathrm{Lös}(A;0)$ ist ein Unterraum von K^n und $\dim \mathrm{Lös}(A;0) = n - \mathrm{rang}(A)$.

(c) Für jedes $b \in K^m$ gilt:

  (i) $v \in \mathrm{Lös}(A;b) \Rightarrow \mathrm{Lös}(A;b) = v + \mathrm{Lös}(A;0)$ $[= \{v + x : x \in \mathrm{Lös}(A;0)\}]$.

  (ii) $\mathrm{Lös}(A;b) \neq \emptyset \iff \mathrm{rang}(A) = \mathrm{rang}(A\ b)$.

(iii) $|\text{Lös}(A;b)| = 1 \iff \text{rang}(A) = \text{rang}(A\ b) = n$.

(iv) $\text{rang}(A) = m \Rightarrow \text{Lös}(A;b) \neq \emptyset$.

(v) $\text{rang}(A) = m = n \Rightarrow |\text{Lös}(A;b)| = 1$.

Beweis:

(a) $x \in \text{Lös}(A;0) \Leftrightarrow Ax = 0 \Leftrightarrow \mathsf{f}_A(x) = 0 \Leftrightarrow x \in \text{Ker}(\mathsf{f}_A)$.

(b) Folgt aus (a) mit Lemma 5.2d und Satz 5.7.

(c) (i) Ist $Av = b$, so: $x \in \text{Lös}(A;b) \Leftrightarrow Ax = Av \Leftrightarrow A(x-v) = 0 \Leftrightarrow x - v \in \text{Lös}(A;0) \Leftrightarrow x \in v + \text{Lös}(A;0)$.

(ii) $\text{Lös}(A;b) \neq \emptyset \Leftrightarrow \exists x(A{\cdot}x = b) \Leftrightarrow b \in \text{SR}(A) \Leftrightarrow \text{SR}(A) = \text{SR}(A\ b) \Leftrightarrow \dim \text{SR}(A) = \dim \text{SR}(A\ b)$.

(iii) $|\text{Lös}(A;b)| = 1 \overset{\text{(i),(ii)}}{\Leftrightarrow} \text{rang}(A) = \text{rang}(A\ b)\ \&\ \text{Lös}(A;0) = \{0\} \overset{\text{(b)}}{\Leftrightarrow} n = \text{rang}(A) = \text{rang}(A\ b)$.

(iv) $\text{rang}(A) = m \Rightarrow \dim \text{Im}(\mathsf{f}_A) = \dim K^m \Rightarrow \text{Im}(\mathsf{f}_A) = K^m \Rightarrow b \in \text{Im}(\mathsf{f}_A) = \{Ax : x \in K^n\}$.

(v) $\text{rang}(A) = m = n \overset{7.1\text{b}}{\Rightarrow} A$ invertierbar $\Rightarrow \forall x \in K^n(Ax = b \Leftrightarrow x = A^{-1}b) \Rightarrow \text{Lös}(A;b) = \{A^{-1}b\}$.

Satz 7.5.

Sei $A = (a_{ij}) \in K^{m\times n}$ eine ausgezeichnete Stufenmatrix. Seien $j_1 < \ldots < j_r$ die Indizes der Stufenspalten und $j_{r+1} < \ldots < j_n$ die Indizes der restlichen Spalten von A (also $\{j_1, \ldots, j_n\} = \{1, \ldots, n\}$).

Die lineare Abbildung $f : K^{n-r} \to K^n$ sei definiert durch:

$$f\left(\begin{pmatrix} y_1 \\ \vdots \\ y_{n-r} \end{pmatrix}\right) := \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \quad \text{mit} \quad x_{j_{r+1}} := y_1, \ldots, x_{j_n} := y_{n-r} \text{ und } x_{j_i} := -\sum_{\nu=1}^{n-r} a_{i\,j_{r+\nu}} y_\nu \text{ für } i = 1, \ldots, r.$$

Dann ist $r = \text{rang}(A)$ und f bildet K^{n-r} isomorph auf $\text{Lös}(A;0)$ ab.

Beweis:

1. Es gilt $\text{SR}(A) = \text{span}(e_1, ..., e_r)$ und folglich $\text{rang}(A) = \dim \text{SR}(A) = r$.

2. $\text{Lös}(A;0) \overset{\text{L.1.3}}{=} \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} : x_{j_i} = -\sum_{k=r+1}^{n} a_{ij_k} x_{j_k} \text{ für } i = 1, \ldots, r \right\} =$

$\left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} : \exists y_1, \ldots, y_{n-r} \in K[x_{j_{r+1}} = y_1, \ldots, x_{j_n} = y_{n-r}\ \&\ x_{j_i} = -\sum_{\nu=1}^{n-r} a_{i\,j_{r+\nu}} y_\nu \text{ für } i = 1, \ldots, r] \right\} =$

$\{x \in K^n : \exists y \in K^{n-r}(x = f(y))\} = \text{Im}(f)$. 3. Nach 1. und 7.4b ist $\dim \text{Lös}(A;0) = n - r$.

18.01.2010

Beispiel.

$$A = \begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 0 & 1 & \frac{1}{2} \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad \begin{array}{l} r = 2,\ j_1 = 1,\ j_2 = 3, \\ j_3 = 2,\ j_4 = 4 \end{array}, \quad f\left(\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}\right) = \begin{pmatrix} y_2 \\ y_1 \\ -\frac{1}{2}y_2 \\ y_2 \end{pmatrix} = y_1 \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + y_2 \begin{pmatrix} 1 \\ 0 \\ -\frac{1}{2} \\ 1 \end{pmatrix}.$$

Definition (Zeilenraum von A).

Für $A \in K^{m\times n}$ sei $\text{ZR}(A) := \text{span}(a_1, \ldots, a_m) \subseteq K^{1\times n}$, wobei $a_1, \ldots, a_m$ die Zeilen von A sind.

Lemma 7.6.

Entsteht A' aus $A \in K^{m\times n}$ durch elementare Zeilenumformungen, so gilt:

$\text{ZR}(A) = \text{ZR}(A')$ und $\text{rang}(A) = \text{rang}(A')$.

Beweis:

1. $\text{ZR}(A) = \text{ZR}(A')$: Für Umformungen der Typen (I),(III) ist die Behauptung klar. Wir nehmen jetzt an,

daß A' aus A durch Addition des λ-fachen der zweiten Zeile zur ersten Zeile entstanden ist.

Dann $\mathrm{ZR}(A) = \mathrm{span}(a_1, \ldots, a_m)$ und $\mathrm{ZR}(A') = \mathrm{span}(a_1 + \lambda a_2, a_2, \ldots, a_m)$, und die Behauptung folgt aus $a_1 + \lambda a_2, a_2, \ldots, a_m \in \mathrm{span}(a_1, \ldots, a_m)$ und $a_1, \ldots, a_m \in \mathrm{span}(a_1 + \lambda a_2, a_2, \ldots, a_m)$.

2. $\mathrm{rang}(A) \overset{7.4b}{=} n - \dim \mathrm{Lös}(A; 0) \overset{L.1.1}{=} n - \dim \mathrm{Lös}(A'; 0) \overset{7.4b}{=} \mathrm{rang}(A')$.

Lemma 7.7.

Ist $A \in K^{m\times n}$ eine Stufenmatrix und r die Anzahl ihrer Stufen, so gilt:

$\dim \mathrm{SR}(A) = r = \dim \mathrm{ZR}(A) =$ Anzahl der von 0 verschiedenen Zeilen von A.

Beweis:

Wie in §4 gezeigt, bilden die Stufenspalten von A eine Basis von $\mathrm{SR}(A)$. Folglich gilt $r = \dim \mathrm{SR}(A)$. Offenbar ist r auch die Anzahl der von 0 verschiedenen Zeilen von A. Wie man leicht zeigt, sind diese linear unabhängig und bilden deshalb eine Basis von $\mathrm{ZR}(A)$.

Aus 7.6, 7.7 und 7.1a folgt nun

Satz 7.8 (Zeilenrang = Spaltenrang).

Für jede Matrix A gilt: $\dim \mathrm{ZR}(A) = \dim \mathrm{SR}(A) = \mathrm{rang}(A)$.

Definition (Transponierte Matrix). Für $A = \big(a_{ij}\big)_{\substack{i=1,\ldots,m\\ j=1,\ldots,n}} \in K^{m\times n}$ sei $A^{\mathtt{t}} := \big(a_{ij}\big)_{\substack{j=1,\ldots,n\\ i=1,\ldots,m}} \in K^{n\times m}$.

Beispiele: $\begin{pmatrix} 1 & 2 & 3 \\ 0 & -1 & 2 \end{pmatrix}^{\mathtt{t}} = \begin{pmatrix} 1 & 0 \\ 2 & -1 \\ 3 & 2 \end{pmatrix}$, $\quad (x_1 \ldots x_n)^{\mathtt{t}} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, $\quad \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}^{\mathtt{t}} = (x_1 \ldots x_n)$.

Lemma 7.9.

(a) Für $A, B \in K^{m\times n}$ und $\lambda \in K$ gilt: $(A + B)^{\mathtt{t}} = A^{\mathtt{t}} + B^{\mathtt{t}}$, $\quad (\lambda\cdot A)^{\mathtt{t}} = \lambda \cdot A^{\mathtt{t}}$, $\quad (A^{\mathtt{t}})^{\mathtt{t}} = A$.

(b) Für $A \in K^{m\times p}$ und $B \in K^{p\times n}$ gilt: $(AB)^{\mathtt{t}} = B^{\mathtt{t}} \cdot A^{\mathtt{t}}$.

(c) Ist $A \in K^{n\times n}$ invertierbar, so ist auch $A^{\mathtt{t}}$ invertierbar und $(A^{\mathtt{t}})^{-1} = (A^{-1})^{\mathtt{t}}$.

(d) Für jede Matrix A gilt $\mathrm{rang}(A^{\mathtt{t}}) = \mathrm{rang}(A)$.

Beweis:

(b) $B^{\mathtt{t}} \cdot A^{\mathtt{t}} = (b_{\nu j})_{j,\nu} \cdot (a_{i\nu})_{\nu,i} = (\sum_\nu b_{\nu j} a_{i\nu})_{j,i} = (\sum_\nu a_{i\nu} b_{\nu j})_{j,i} = (AB)^{\mathtt{t}}$.

(c) $AA^{-1} = E \Rightarrow (A^{-1})^{\mathtt{t}} \cdot A^{\mathtt{t}} = E \Rightarrow A^{\mathtt{t}}$ invertierbar und $(A^{\mathtt{t}})^{-1} = (A^{-1})^{\mathtt{t}}$.

(d) $\mathrm{SR}(A^{\mathtt{t}}) \cong \mathrm{ZR}(A) \Rightarrow \dim \mathrm{SR}(A^{\mathtt{t}}) = \dim \mathrm{ZR}(A) \overset{7.8}{=} \dim \mathrm{SR}(A)$.

Definition.

Ist V ein K-Vektorraum, so heißt $V^* := \mathrm{Hom}(V, K)$ der *Dualraum* von V.

Die Elemente von V^* heißen *Linearformen* auf V.

Beispiel.

Ist V der Vektorraum der auf $[a, b]$ differenzierbaren Funktionen $f : [a, b] \to \mathbb{R}$, so sind

$\sigma : V \to \mathbb{R},\ f \mapsto \int_a^b f(x)dx$ und, für $c \in (a, b)$, $\delta_c : V \to \mathbb{R},\ f \mapsto \frac{df}{dx}(c)$ Linearformen auf V.

Definition.

Für $f \in \mathrm{Hom}(V, W)$ sei $f^* : W^* \to V^*,\ f^*(\psi) := \psi \circ f$ *(die zu f duale Abbildung)*

Lemma 7.10.

(a) $f \in \mathrm{Hom}(V, W) \implies f^* \in \mathrm{Hom}(W^*, V^*)$.

(b) $f \in \mathrm{Hom}(V, W)$ & $g \in \mathrm{Hom}(W, U) \implies (g \circ f)^* = f^* \circ g^*$.

Beweis:

(a) Für alle $\psi, \psi' \in W^*$, $\lambda \in K$ und $v \in V$ gilt:

(1) $(\psi + \psi')(f(v)) = \psi(f(v)) + \psi'(f(v)) = (\psi \circ f)(v) + (\psi' \circ f)(v) = (\psi{\circ}f + \psi'{\circ}f)(v)$ und

(2) $(\lambda\psi)(f(v)) = \lambda(\psi(f(v))) = \lambda(f^*(\psi)(v)) = (\lambda f^*(\psi))(v)$.

Daraus folgt:

$f^*(\psi + \psi') = (\psi + \psi') \circ f \overset{(1)}{=} \psi{\circ}f + \psi'{\circ}f = f^*(\psi) + f^*(\psi')$ und $f^*(\lambda\psi) = (\lambda\psi){\circ}f \overset{(2)}{=} \lambda(\psi{\circ}f) = \lambda f^*(\psi)$.

(b) $(g \circ f)^*(\varphi) = \varphi \circ g \circ f = g^*(\varphi) \circ f = f^*(g^*(\varphi))$.

20.1.2010

Lemma 7.11. Für alle $f \in \mathrm{Hom}(V, W)$ gilt:

(a) f injektiv $\Rightarrow$ f^* surjektiv. (b) f surjektiv $\Rightarrow$ f^* injektiv.

Beweis:

(a) Sei $\psi \in V^*$. Zu zeigen: es existiert ein $\varphi \in W^*$ mit $\varphi \circ f = \psi$. Man wähle einen Unterraum U von W mit $W = f(V) \oplus U$ (vgl. Aufg. 36a) und setze $\varphi(f(x) + u) := \psi(x)$ für $x \in V$ und $u \in U$.

(b) $f^*(\varphi) = 0 \Rightarrow \varphi \circ f = 0 \Rightarrow \forall x \in V(\varphi(f(x)) = 0) \Rightarrow \forall y \in W(\varphi(y) = 0) \Rightarrow \varphi = 0$.

Definition.

Ist $(v_1, \ldots, v_n)$ eine Basis von V, so sei $v_i^* \in V^*$ definiert durch $v_i^*(v_j) := \delta_{ij}$.

Man nennt $(v_1^*, \ldots, v_n^*)$ die zu $(v_1, \ldots, v_n)$ *duale Basis* von V^*.

Lemma 7.12.

$(v_1, \ldots, v_n)$ Basis von $V \implies (v_1^*, \ldots, v_n^*)$ Basis von V^* .

Beweis: Für $\varphi \in V^*$ gilt: $\varphi = \sum_{i=1}^n \lambda_i v_i^* \Leftrightarrow \forall j(\varphi(v_j) = \sum_{i=1}^n \lambda_i v_i^*(v_j)) \Leftrightarrow \forall j(\varphi(v_j) = \lambda_j)$.

Daraus folgt mit L.4.4a die Behauptung.

Lemma 7.13.

Ist $\overline{v}$ Basis von V und $\overline{w}$ Basis von W, so gilt $\mathcal{M}_{\overline{v}^*}^{\overline{w}^*}(f^*) = \mathcal{M}_{\overline{w}}^{\overline{v}}(f)^{\mathtt{t}}$ für alle $f \in \mathrm{Hom}(V, W)$.

Beweis:

Sei $\mathcal{M}_{\overline{w}}^{\overline{v}}(f) = (a_{ij})_{i,j} \in K^{m \times n}$ und $\mathcal{M}_{\overline{v}^*}^{\overline{w}^*}(f^*) = (b_{ji})_{j,i} \in K^{n \times m}$.

Dann $f(v_j) = \sum_l a_{lj} w_l$ & $f^*(w_i^*) = \sum_l b_{li} v_l^*$ und folglich $a_{ij} = w_i^*(f(v_j)) = f^*(w_i^*)(v_j) = b_{ji}$.

Lemma 7.14. $f \in \mathrm{Hom}(V, W)$ & $\mathrm{rang}(f) < \infty \implies \mathrm{rang}(f) = \mathrm{rang}(f^*)$.

Beweis:

$f = f_2 \circ f_1$ mit $f_1 : V \to \mathrm{Im}(f)$, $x \mapsto f(x)$ und $f_2 : \mathrm{Im}(f) \to W$, $y \mapsto y$.

f_1 surjektiv $\Rightarrow$ $f_1^* : \mathrm{Im}(f)^* \to V^*$ injektiv (1)

f_2 injektiv $\Rightarrow$ $f_2^* : W^* \to \mathrm{Im}(f)^*$ surjektiv (2)

$f^* = f_1^* \circ f_2^* \Rightarrow \mathrm{Im}(f^*) = f_1^*(f_2^*(W^*)) \overset{(2)}{=} f_1^*(\mathrm{Im}(f)^*) \overset{(1)}{\Rightarrow} \dim \mathrm{Im}(f^*) = \dim \mathrm{Im}(f)^*$ (3)

$\mathrm{rang}(f) = \dim \mathrm{Im}(f) \overset{7.12}{=} \dim \mathrm{Im}(f)^* \overset{(3)}{=} \dim \mathrm{Im}(f^*) = \mathrm{rang}(f^*)$.

Korollar. Für jede Matrix A gilt: $\mathrm{rang}(A^{\mathtt{t}}) = \mathrm{rang}(A)$.

Beweis ohne Verwendung von 7.8: Sei $A \in K^{m \times n}$ und $\overline{v}$ bzw. $\overline{w}$ die Standardbasis von K^n bzw. K^m. Dann $A = \mathcal{M}_{\overline{w}}^{\overline{v}}(\mathsf{f}_A)$ und somit $\mathrm{rang}(A^{\mathtt{t}}) \overset{7.13}{=} \mathrm{rang}(\mathcal{M}_{\overline{v}^*}^{\overline{w}^*}((\mathsf{f}_A)^*) \overset{7.2}{=} \mathrm{rang}((\mathsf{f}_A)^*) \overset{7.14}{=} \mathrm{rang}(\mathsf{f}_A) = \mathrm{rang}(A)$.

§8 Affine Unterräume; Quotientenvektorräume

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

Für $y \in Y$ nennt man $f^{-1}(\{y\})$ die *Faser von f über y.*

X wird durch die Fasern in disjunkte Teilmengen zerlegt: $X = \bigcup_{y \in \mathrm{Im} f} f^{-1}(\{y\})$ (*Faserung*).

Wenn kein Mißverständnis zu befürchten ist, schreibt man oft nur $f^{-1}(y)$ statt $f^{-1}(\{y\})$.

Im folgenden sei V stets ein K-Vektorraum.

Definition.

Eine Teilmenge $M \subseteq V$ heißt *affiner Unterraum* von V, wenn es ein $a \in V$ und einen Untervektorraum U von V mit $M = a + U$ $(:= \{a + u : u \in U\})$ gibt.

Im Unterschied dazu nennt man Untervektorräume manchmal auch *lineare Unterräume*.

Bemerkung.

(a) Für $f \in \mathrm{Hom}(V, W)$, $b \in W$ und $a \in f^{-1}(b)$ gilt $f^{-1}(b) = a + \mathrm{Ker}(f)$.

(b) Für $A \in K^{m\times n}$, $b \in K^m$ und $a \in \mathrm{Lös}(A; b)$ gilt $\mathrm{Lös}(A; b) = (\mathsf{f}_A)^{-1}(b) = a + \mathrm{Ker}(\mathsf{f}_A) = a + \mathrm{Lös}(A; 0)$.

Beweis von (a): $f^{-1}(b) = \{x \in V : f(x) = b\} = \{x \in V : f(x) = f(a)\} = \{x \in V : f(x - a) = 0\} =$
$= \{x \in V : x - a \in \mathrm{Ker}(f)\} = a + \mathrm{Ker}(f)$.

Lemma 8.1. Sei $M = a + U$ ein affiner Unterraum von V.

(a) $U = \{x - y : x, y \in M\}$. Man nennt U deshalb auch den *Differenzraum von M*.

(b) Für jedes $b \in M$ gilt $M = b + U$.

Beweis:

(a) 1. $x = a+u$ & $y = a+w$ & $u, w \in U \Rightarrow x-y = u-w \in U$. 2. $u \in U \Rightarrow u = (a+u)-a$ & $a+u, a \in M$.

(b) Sei $b = a+u_0$. Dann $b+U = \{a+u_0+u : u \in U\} \subseteq a+U$ und ebenso $a+U = \{b-u_0+u : u \in U\} \subseteq b+U$.

Definitionen.

Zwei affine Unterräume $a_1 + U_1$ und $a_2 + U_2$ von V heißen *parallel*, wenn $U_1 \subseteq U_2$ oder $U_2 \subseteq U_1$ gilt.

Für jeden affinen Unterraum $M = a + U$ sei $\dim(M) := \dim(U)$.

Einen affinen Unterraum der Dimension 1 (bzw. 2) nennt man eine *Gerade* (bzw. *Ebene*).

Einen affinen Unterraum der Dimension $\dim(V) - 1$ nennt man eine *Hyperebene* (falls $\dim(V) < \infty$).

Lemma 8.2.

Seien $M_1 = a_1 + U_1$ und $M_2 = a_2 + U_2$ affine Unterräume von V.

(a) $M_1 \cap M_2 \neq \emptyset \iff a_2 - a_1 \in U_1 + U_2$

(b) $a \in M_1 \cap M_2 \Longrightarrow M_1 \cap M_2 = a + (U_1 \cap U_2)$

(c) Ist $V = U_1 \oplus U_2$, so enthält $M_1 \cap M_2$ genau einen Punkt s. *(Schnittpunkt)*

(d) Ist M_1 eine Hyperebene und M_2 eine Gerade, die nicht parallel zu M_1 ist, so gilt $V = U_1 \oplus U_2$.

Beweis :

(a) Ist $a \in M_1 \cap M_2$, so $a = a_1 + u_1$ und $a = a_2 + u_2$ mit $u_i \in U_i$, also $a_2 - a_1 = u_1 - u_2 \in U_1 + U_2$.
Ist umgekehrt $a_2 - a_1 \in U_1 + U_2$, so $a_2 - a_1 = u_1 - u_2$ mit $u_i \in U_i$, also $a_1 + u_1 = a_2 + u_2 \in M_1 \cap M_2$.

(b) Sei $a \in M_1 \cap M_2$. Nach Lemma 8.1b gilt dann $M_i = a + U_i$ und folglich
$x \in M_1 \cap M_2 \Leftrightarrow x - a \in U_1 \wedge x - a \in U_2 \Leftrightarrow x - a \in U_1 \cap U_2 \Leftrightarrow x \in a + U_1 \cap U_2$.

(c) $V = U_1 \oplus U_2 \Rightarrow a_2 - a_1 \in U_1 + U_2 \overset{(a)}{\Rightarrow} M_1 \cap M_2 \neq \emptyset$. Sei $s \in M_1 \cap M_2$.
Dann $M_1 \cap M_2 = s + U_1 \cap U_2 = s + \{0\} = \{s\}$.
(d) Wäre $U_1 \cap U_2 \neq \{0\}$, so wäre (wegen $\dim(U_2) = 1$) $U_2 \subseteq U_1$, also M_1, M_2 parallel.
Folglich $U_1 \cap U_2 = \{0\}$ und somit (wegen $\dim U_1 + \dim U_2 = \dim V$) $V = U_1 \oplus U_2$.

Lemma 8.3. Für $U, H \subseteq V$ und $\dim(V) < \infty$ gilt:
(a) U ist UVR der Dimension $\dim(V) - 1 \iff \exists \varphi \in V^* \backslash \{0\}(U = \operatorname{Ker}(\varphi))$.
(b) H ist Hyperebene $\iff \exists \varphi \in V^* \backslash \{0\} \exists \lambda \in K(H = \varphi^{-1}(\lambda))$.
Beweis :
(a) "$\Rightarrow$": Wir wählen eine Basis $(v_1, ..., v_n)$ von V, so daß $U = \operatorname{span}(v_1, ..., v_{n-1})$, und definieren $\varphi \in V^*$ durch $\varphi(v_1) := ... := \varphi(v_{n-1}) := 0$, $\varphi(v_n) := 1$. Dann gilt $\operatorname{Ker}(\varphi) = U$. "$\Leftarrow$": Dimensionsformel.
(b) "$\Rightarrow$": Sei $H = a + U$. Nach (a) existiert ein $\varphi \in V^*$ mit $U = \operatorname{Ker}(\varphi)$, also $\varphi^{-1}(\varphi(a)) = a + \operatorname{Ker}(\varphi) = H$.
"$\Leftarrow$": Seien $\varphi \in V^* \setminus \{0\}$ und $\lambda \in K$ gegeben. Dann ist $\operatorname{Im}(\varphi) = K$ und somit existiert ein $a \in \varphi^{-1}(\lambda)$.
Es folgt $\varphi^{-1}(\lambda) = a + \operatorname{Ker}(\varphi)$ und $\dim \operatorname{Ker}(\varphi) = \dim(V) - 1$.

Lemma 8.4. Seien $v_0, v_1, ..., v_k \in V$. Dann ist
$\mathsf{Aff}(v_0, ..., v_k) := v_0 + \operatorname{span}(v_1 - v_0, \ldots, v_k - v_0) = \{ \sum_{i=0}^{k} \alpha_i v_i : \alpha_0, ..., \alpha_k \in K \;\&\; \sum_{i=0}^{k} \alpha_i = 1 \}$
der kleinste affine Unterraum von V, der $v_0, ..., v_k$ enthält.
Man nennt ihn den von $v_0, v_1, ..., v_k$ *aufgespannten affinen Unterraum* oder die *affine Hülle* von $v_0, v_1, ..., v_k$.

Beweis:

$$\begin{aligned} v_0 + \operatorname{span}(v_1 - v_0, \ldots, v_k - v_0) &= \{v_0 + \textstyle\sum_{i=1}^k \alpha_i(v_i - v_0) : \alpha_1, ..., \alpha_k \in K\} \\ &= \{(1 - \textstyle\sum_{i=1}^k \alpha_i)v_0 + \sum_{i=1}^k \alpha_i v_i : \alpha_1, ..., \alpha_k \in K\} \\ &= \{\alpha_0 v_0 + \textstyle\sum_{i=1}^k \alpha_i v_i : \alpha_0, ..., \alpha_k \in K \;\&\; \alpha_0 = 1 - \sum\limits_{i=1}^{k} \alpha_i\} \\ &= \{\textstyle\sum_{i=0}^k \alpha_i v_i : \alpha_0, ..., \alpha_k \in K \;\&\; \sum_{i=0}^k \alpha_i = 1\}. \end{aligned}$$

Ist $M = a + U$ ein affiner Unterraum mit $v_0, \ldots, v_k \in M$, so gilt $v_0 + \operatorname{span}(v_1 - v_0, \ldots, v_k - v_0) \subseteq v_0 + U \overset{8.1}{=} M$.

27.1.2010

Beispiel.
Für $v_0 \neq v_1 \in V$ gilt: $\mathsf{Aff}(v_0, v_1) = v_0 + \mathbb{R}(v_1 - v_0) = \{v_0 + \alpha(v_1 - v_0) : \alpha \in K\} = \{\lambda v_0 + (1-\lambda)v_1 : \lambda \in K\}$ ist die Gerade durch v_0 und v_1. Im Fall $K = \mathbb{R}$ ist $\{\lambda v_0 + (1-\lambda)v_1 : 0 \leq \lambda \leq 1\}$ die Strecke zwischen v_0 und v_1.

Definition.
Eine *binäre* (oder *2-stellige*) *Relation* ist eine Menge von geordneten Paaren. Ist M eine Menge und $R \subseteq M \times M$, so nennt man R eine binäre Relation auf M.

Schreibweise: Ist R eine binäre Relation, so schreibt man oft 'xRy' (oder auch 'Rxy') statt '$(x, y) \in R$'

Eine binäre Relation R auf der Menge M heißt

- *reflexiv*, wenn $\forall x \in M(xRx)$;
- *antireflexiv*, wenn $\forall x(\neg\, xRx)$;
- *symmetrisch*, wenn $\forall x, y(xRy \Rightarrow yRx)$;
- *transitiv*, wenn $\forall x, y, z(xRy \;\&\; yRz \Rightarrow xRz)$.

Eine Relation $R \subseteq M \times M$ heißt *Äquivalenzrelation auf* M, wenn sie reflexiv, symmetrisch und transitiv ist.

Ist R eine Äquivalenzrelation auf M, so sei

$[x]_R := \{y \in M : xRy\}$ (*Äquivalenzklasse von* $x \in M$),

$M/R := \{[x]_R : x \in M\}$ (*Quotientenmenge von* M *nach der Relation* R)

Bemerkung. Die in §7 eingeführte "Äquivalenz" von Matrizen ist eine Äquivalenzrelation.

Lemma 8.5. Ist R eine Äquivalenzrelation auf der Menge M, so gilt:
(a) $x \in [x]_R \quad (\forall x \in M)$,
(b) $xRx' \Leftrightarrow [x]_R = [x']_R \Leftrightarrow [x]_R \cap [x']_R \neq \emptyset \quad (\forall x, x' \in M)$,
(c) $M = \bigcup_{x \in M} [x]_R$.

Beweis:
(a) $x \in M \Rightarrow xRx \Rightarrow x \in [x]$.
(b) xRx' & $y \in [x'] \Rightarrow xRx'$ & $x'Ry \Rightarrow xRy \Rightarrow y \in [x]$.
xRx' & $y \in [x] \Rightarrow x'Rx$ & $xRy \Rightarrow x'Ry \Rightarrow y \in [x']$.
$[x] = [x'] \Rightarrow x \in [x] = [x] \cap [x']$.
$y \in [x] \cap [x'] \Rightarrow xRy$ & $x'Ry \Rightarrow xRy$ & $yRx' \Rightarrow xRx'$.
(c) folgt aus (a).

Lemma 8.6. Sei R eine Äquivalenzrelation auf der Menge M, und sei $\pi_R : M \to M/R$, $x \mapsto [x]_R$.
Dann existiert zu jeder Abbildung $f : M \to N$ mit $\forall x, x' \in M(xRx' \Rightarrow f(x) = f(x'))$
genau eine Abbildung $\overline{f} : M/R \to N$, so daß $\overline{f} \circ \pi_R = f$.

Gilt auch noch $\forall x, x' \in M(f(x) = f(x') \Rightarrow xRx')$, so ist $\overline{f}$ injektiv.

Beweis:
Aus der Voraussetzung folgt $\forall x, x' \in M([x]_R = [x']_R \Rightarrow f(x) = f(x'))$. Also wird durch $\overline{f}([x]_R) := f(x)$
eine Abbildung $\overline{f} : M/R \to N$ definiert, so daß für alle $x \in M$ gilt $(\overline{f} \circ \pi_R)(x) = \overline{f}([x]_R) = f(x)$.

Eindeutigkeit: Sind f_1, f_2 Abbildungen von M/R nach N mit $f = f_i \circ \pi_R$ $(i = 1, 2)$, so gilt
$\forall x \in M(f_1(\pi_R(x)) = f(x) = f_2(\pi_R(x)))$, d.h. $\forall \xi \in M/R(f_1(\xi) = f_2(\xi))$, also $f_1 = f_2$.

Injektivität: $\overline{f}([x]_R) = \overline{f}([x']_R) \Rightarrow f(x) = f(x') \Rightarrow xRx' \Rightarrow [x]_R = [x']_R$.

Im folgenden sei U ein Untervektorraum von V.

Definitionen.
Für $X, Y \subseteq V$ und $\lambda \in K$ sei $X + Y := \{x + y : x \in X \;\&\; y \in Y\}$.
Für $v, v' \in V$ definieren wir: $v \sim_U v' \;:\Leftrightarrow\; v' - v \in U$. Ferner sei $V/U := \{v + U : v \in V\}$.
Die Relation $\sim_U$ wird auch als *Kongruenz modulo U* bezeichnet.
Die Menge $v + U$ nennt man *Restklasse von v modulo U*.

Lemma 8.7.
(a) Für $v, w \in V$ und $\lambda \in K$ gilt $(v + U) + (w + U) := (v + w) + U$.
(b) $\sim_U$ ist eine Äquivalenzrelation auf V.
(c) Für alle $v \in V$ gilt $[v]_{\sim_U} = v + U$,
d.h. die Äquivalenzklasse von v bzgl. $\sim_U$ ist gleich dem affinen Unterraum $v + U$.

Beweis :

(a) $(v+U)+(w+U)=\{v+u_1+w+u_2 : u_1,u_2\in U\}=\{(v+w)+u : u\in U\}=(v+w)+U$.

(b) Reflexivität: $v-v=0\in U$. Symmetrie: $v'-v\in U\Leftrightarrow v-v'\in U$.

Transitivität: $v'-v\in U\ \&\ v''-v'\in U\ \Rightarrow\ v''-v=(v''-v')+(v'-v)\in U$.

(c) $v'\sim_U v\Leftrightarrow v'-v\in U\Leftrightarrow v'\in v+U$.

Definition. Wie man leicht sieht, gilt: $\forall v,v'\in V,\lambda\in K(v+U=v'+U\Rightarrow \lambda v+U=\lambda v'+U)$.

Deshalb wird durch $\lambda\cdot(v+U):=\lambda v+U$ eine Abbildung $\cdot : K\times V/U\to V/U$ definiert.

Satz 8.8.

(a) V/U mit der oben definierten Addition und skalaren Multiplikation ist ein K-Vektorraum. Das Nullelement dieses Vektorraums ist U.

(b) Die kanonische Abbildung $\pi_U : V\to V/U,\ v\mapsto v+U$ ist ein surjektiver Homomorphismus (Epimorphismus), dessen Fasern gerade die Restklassen modulo U in V sind.

(c) $\mathrm{Ker}(\pi_U)=U$.

(d) $\dim(V/U)=\dim(V)-\dim(U)$, falls $\dim(V)<\infty$.

Man nennt V/U den *Quotientenvektorraum* von V *nach* U (oder *modulo* U).

Beweis :

(a),(b) Für alle $v,w\in V$ und $\lambda\in K$ gilt $\pi_U(v+w)=(v+w)+U\overset{8.7a}{=}(v+U)+(w+U)=\pi_U(v)+\pi_U(w)$ und $\pi_U(\lambda v)=\lambda v+U\overset{8.7a}{=}\lambda(v+U)=\lambda\pi_U(v)$. Daraus folgen in einfacher Weise die Behauptungen (a), (b).

(c) $v\in\mathrm{Ker}(\pi_U)\Leftrightarrow\pi_U(v)=0_{V/U}\Leftrightarrow v+U=U\Leftrightarrow v\in U$.

(d) $\dim(V)=\dim(\mathrm{Ker}(\pi_U))+\dim(\mathrm{Im}(\pi_U))=\dim(U)+\dim(V/U)$.

Lemma 8.9. Sei $V=U\oplus W$ und $\pi_U : V\to V/U$ der kanonische Epimorphismus.
Dann ist $\pi':=\pi_U{\restriction}W : W\to V/U$ ein Isomorphismus.

Beweis:

1. π' surjektiv: Sei $v\in V$. Dann existieren $u\in U$ und $w\in W$ mit $v=u+w$, also $\pi'(w)=w+U=v+U$.
2. π' injektiv: $w\in W\ \&\ \pi'(w)=U\ \Rightarrow\ w\in W\ \&\ w+U=U\ \Rightarrow\ w\in U\cap W=\{0\}$.

Satz 8.10 (Homomorphiesatz).

V/U hat die folgende universelle Eigenschaft: Zu jedem K-Vektorraum W und jedem $f\in\mathrm{Hom}(V,W)$ mit $U\subseteq\mathrm{Ker}(f)$ gibt es genau ein $\overline{f}\in\mathrm{Hom}(V/U,W)$ mit $f=\overline{f}\circ\pi_U$. — Weiter ist $\mathrm{Ker}(\overline{f})=\mathrm{Ker}(f)/U$

Beweis:

Wegen $U\subseteq\mathrm{Ker}(f)$ gilt $\forall v,v'\in V(v\sim_U v'\Rightarrow f(v)=f(v'))$. Nach 8.6 existiert genau eine Abbildung $\overline{f} : V/U\to W$ mit $f=\overline{f}\circ\pi_U$; und wie man leicht nachrechnet, ist $\overline{f}$ auch linear.

[$\overline{f}(\pi(v)+\lambda\pi(v'))=\overline{f}(\pi(v+\lambda v'))=f(v+\lambda v')=f(v)+\lambda f(v')=\overline{f}(\pi(v))+\lambda\overline{f'}(\pi(v'))$]

Ferner gilt: $\mathrm{Ker}(\overline{f})=\{\pi(v) : v\in V\ \&\ \overline{f}(\pi(v))=0\}=\{\pi(v) : v\in V\ \&\ f(v)=0\}=\{v+U : v\in\mathrm{Ker}(f)\}$.

Korollar (Isomorphiesatz).

Ist $f\in\mathrm{Hom}(V,W)$, so wird durch $\overline{f}(v+\mathrm{Ker}(f)):=f(v)$ ein Isomorphismus $\overline{f} : V/\mathrm{Ker}(f)\to\mathrm{Im}(f)$ definiert.

Beweis:

Sei $U:=\mathrm{Ker}(f)$. Dann gilt $\forall v,v'\in V(v\sim_U v'\Leftrightarrow f(v)=f(v'))$. Nach 8.6 und 8.10 ist $\overline{f}$ also wohldefiniert, injektiv und linear. Ferner gilt offenbar $\mathrm{Im}(\overline{f})=\mathrm{Im}(f)$.

§9 Determinanten

Definition.

Für $n \in \mathbb{N}$ sei $\mathcal{S}_n := \mathbf{S}(\{1, ..., n\})$, die Gruppe aller Permutationen der Menge $\{1, ..., n\}$.

Man nennt $\mathcal{S}_n$ die *symmetrische Gruppe* (vom Grad n).

Schreibweise für $\sigma \in \mathcal{S}_n$: $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$.

Beispiele ($\mathcal{S}_2$, $\mathcal{S}_3$).

1. $\mathcal{S}_2 = \{\mathrm{id}, \sigma\}$ mit $\sigma = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$, d.h. $\sigma(1) = 2$ und $\sigma(2) = 1$. Wegen $\sigma^2 = \mathrm{id}$ ist $\sigma = \sigma^{-1}$.

2. Sei $\sigma := \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \in \mathcal{S}_3$ und, $\rho := \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \in \mathcal{S}_3$.

Dann $\sigma^2 = \mathrm{id}$ und $\rho^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ $[\rho^2(1) = \rho(3) = 2,\ \rho^2(2) = \rho(1) = 3,\ \rho^2(3) = \rho(2) = 1]$.

Weiter gilt $\rho^3(1) = \rho(2) = 1$, $\rho^3(2) = \rho(3) = 1$, $\rho^3(3) = \rho(1) = 3$, woraus $\rho^3 = \mathrm{id}$ und damit $\rho^{-1} = \rho^2$ folgt.

Definition. Für $1 \leq i \neq j \leq n$ sei $\tau_{i,j} \in \mathcal{S}_n$ definiert durch $\tau_{i,j}(k) := \begin{cases} k & \text{falls } k \neq i, j \\ j & \text{falls } k = i \\ i & \text{falls } k = j \end{cases}$.

$\tau \in \mathcal{S}_n$ heißt *Transposition*, wenn es $i \neq j$ mit $\tau = \tau_{i,j}$ gibt.

Für jede Transposition τ gilt: $\tau^2 = \mathrm{id}$ bzw. $\tau^{-1} = \tau$.

Satz 9.1. Sei $n \geq 1$.

(a) $|\mathcal{S}_n| = n!$.

(b) Zu jedem $\sigma \in \mathcal{S}_n$ gibt es $m \geq 0$ und Transpositionen $\tau_1, \dots, \tau_m$ mit $\sigma = \tau_1\tau_2 \dots \tau_m$ ($\sigma = \mathrm{id}$, falls $m = 0$).

Beweis:

(a) *Definition.* Für jede Menge M sei $S_n(M)$ die Menge aller injektiven Abbildungen von $\{1, \dots, n\}$ in M. Für $\sigma : \{1, \dots, n-1\} \to M$ und $a \in M$ sei $\sigma_a^* : \{1, \dots, n\} \to M$ definiert durch $\sigma_a^*(i) := \begin{cases} a & \text{falls } i = n \\ \sigma(i) & \text{sonst} \end{cases}$.

Durch Induktion nach n zeigen wir: $|M| = n \Rightarrow |S_n(M)| = n!$.

1. $n = 1$: trivial. 2. $n > 1$: $S_n(M) = \bigcup_{a \in M} \{\sigma_a^* : \sigma \in S_{n-1}(M \setminus \{a\})\} \Rightarrow$

$\Rightarrow |S_n(M)| = \sum_{a \in M} |S_{n-1}(M \setminus \{a\})| \overset{\text{I.V.}}{=} \sum_{a \in M} (n-1)! = (n-1)! \cdot n = n!$.

(b) Induktion nach $k := \min\{l \leq n : \sigma(i) = i \text{ für } l < i \leq n\}$.

1. $k = 0$: Dann $\forall i \in \{1, ..., n\}(\sigma(i) = i)$ und somit $\sigma = \mathrm{id}$.

2. $k > 0$: Da σ injektiv ist, gilt dann $\sigma(k) < k$. Mit $\tau := \tau_{k,\sigma(k)}$ gilt außerdem $\tau\sigma(k) = k$ und $\tau\sigma(i) = \tau(i) = i$ für $i = k{+}1, \dots, n$. Nach I.V. haben wir deshalb $\tau\sigma = \tau_1 \dots \tau_m$, und somit $\sigma = \tau\tau_1 \dots \tau_m$.

Definition. Eine Transposition $\tau_{i,j} \in \mathcal{S}_n$ heißt *Nachbarnvertauschung*, falls $j = i{+}1$ oder $i = j{+}1$ ist.

Lemma 9.2. Jede Transposition τ ist das Produkt einer ungeraden Zahl von Nachbarnvertauschungen.

Beweis:

Sei $\tau = \tau_{i,j}$ mit $i < j$. Induktion nach $j - i$:

1. $j - i = 1$: Dann ist τ selbst eine Nachbarnvertauschung.

2. $j - i > 1$: Dann gilt $(*)\ \tau = \tau_{j-1,j} \circ \tau_{i,j-1} \circ \tau_{j-1,j}$ $(i < j{-}1)$, und nach I.V. ist $\tau_{i,j-1}$ Produkt einer ungeraden Zahl von Nachbarnvertauschungen. Daraus folgt die Behauptung für τ.

3.2.2010

Definition.

Ein Paar (i,j) heißt *Fehlstand* der Permutation $\pi \in \mathcal{S}_n$, wenn $1 \le i < j \le n$ und $\pi(j) < \pi(i)$ ist.

Für jede Permutation $\pi \in \mathcal{S}_n$ sei $a(\pi)$ die Anzahl der Fehlstände von π, d.h.

$a(\pi) := |\{(i,j) : 1 \le i < j \le n \wedge \pi(j) < \pi(i)\}|$.

Ferner sei $\operatorname{sign}(\pi) := (-1)^{a(\pi)}$ *(Vorzeichen von π).*

π heißt *gerade* falls $a(\pi)$ gerade, d.h. $\operatorname{sign}(\pi) = 1$ ist. Andernfalls heißt π ungerade.

Lemma 9.3

Ist $\tau \in \mathcal{S}_n$ eine Nachbarnvertauschung, so gilt $a(\tau \circ \pi) \in \{a(\pi)+1, a(\pi)-1\}$ für jedes $\pi \in \mathcal{S}_n$.

Beweis:

Sei $\tau = \tau_{k,k+1}$ und $P := \{(i,j) : 1 \le i < j \le n\}$. Offenbar gibt es genau ein Paar $(i,j) \in P$ mit $\pi(i), \pi(j) \in \{k, k+1\}$; und für dieses Paar gilt: $\pi(j) < \pi(i) \Leftrightarrow (\tau \circ \pi)(i) < (\tau \circ \pi)(j)$. Für alle anderen Paare $(i,j) \in P$ gilt dagegen $\pi(j) < \pi(i) \Leftrightarrow (\tau \circ \pi)(j) < (\tau \circ \pi)(i)$.

Satz 9.4

(a) $\operatorname{sign}(\mathrm{id}) = 1$.

(b) $\operatorname{sign}(\pi \circ \sigma) = \operatorname{sign}(\pi) \cdot \operatorname{sign}(\sigma)$.

(c) $\operatorname{sign}(\tau) = -1$ für jede Transposition τ.

Beweis:

(b) HS. Ist τ eine Nachbarnvertauschung, so $\operatorname{sign}(\tau \circ \sigma) = -\operatorname{sign}(\sigma) = \operatorname{sign}(\tau) \cdot \operatorname{sign}(\sigma)$.

Beweis: $\operatorname{sign}(\tau \circ \sigma) = (-1)^{a(\tau \circ \sigma)} = (-1)^{a(\sigma) \pm 1} = -(-1)^{a(\sigma)} = -\operatorname{sign}(\sigma)$ und $\operatorname{sign}(\tau) = (-1)^1 = -1$.

Nach 9.1b und 9.2 gibt es Nachbarnvertauschungen $\tau_1, ..., \tau_k$ mit $\pi = \tau_1 \circ \ldots \circ \tau_k$.

Mit HS folgt also $\operatorname{sign}(\pi \circ \sigma) = \operatorname{sign}(\tau_1) \cdots \operatorname{sign}(\tau_k) \cdot \operatorname{sign}(\sigma) = \operatorname{sign}(\pi) \cdot \operatorname{sign}(\sigma)$.

(c) Nach 9.2 ist $\tau = \tau_1 \circ \ldots \circ \tau_k$ mit Nachbarnvertauschungen $\tau_1, ..., \tau_k$ und k ungerade.

Folglich $\operatorname{sign}(\tau) = \operatorname{sign}(\tau_1) \cdots \operatorname{sign}(\tau_k) = (-1)^k = -1$.

Folgerung.

Eine Permutation ist genau dann (un)gerade, wenn sie Produkt einer (un)geraden Zahl von Transpositionen ist.

Die geraden Permutationen $\pi \in \mathcal{S}_n$ bilden eine Untergruppe $\mathcal{A}_n$ von $\mathcal{S}_n$ *(alternierende Gruppe).*

Definition.

Sei K ein kommutativer Ring mit Eins, $n \ge 1$ und $d : K^{n \times n} \to K$.

Hat $A \in K^{n \times n}$ die Zeilen $a_1, ..., a_n \in K^{1 \times n}$ so schreiben wir auch $d(a_1, ..., a_n)$ für $d(A)$.

1. d heißt *multilinear*, falls für $k = 1, ..., n$ und alle $a_i, x, y \in K^{1 \times n}$, $\lambda \in K$ gilt:
   $d(a_1, ..., a_{k-1}, x + \lambda y, a_{k+1}, ..., a_n) = d(a_1, ..., a_{k-1}, x, a_{k+1}, ..., a_n) + \lambda \cdot d(a_1, ..., a_{k-1}, y, a_{k+1}, ..., a_n)$.
2. d heißt *alternierend* $:\Leftrightarrow \forall a_1, ..., a_n \in K^{1 \times n} \big[\exists i, j (1 \le i < j \le n \;\&\; a_i = a_j) \Rightarrow d(a_1, ..., a_n) = 0\big]$.
3. d heißt *normiert* $:\Leftrightarrow d(E_n) = 1$.
4. d heißt *Determinantenfunktion* $:\Leftrightarrow$ d ist multilinear, alternierend und normiert.

Lemma 9.5. Ist $d : K^{n\times n} \to K$ multilinear und alternierend, so gilt für alle $A, A' \in K^{n\times n}$:

(a) Entsteht A' aus A durch Vertauschen zweier Zeilen, so ist $d(A') = -d(A)$.

(b) Entsteht A' aus A durch elementare Zeilenumformungen vom Typ II, so ist $d(A') = d(A)$.

(c) $d(A) = d(E_n) \cdot \sum_{\pi\in\mathcal{S}_n} \operatorname{sign}(\pi) \cdot a_{1\pi(1)} \cdot a_{2\pi(2)} \cdots a_{n\pi(n)}$.

Beweis:

(a) $0 = d(a_1 + a_2, a_1 + a_2, a_3, \ldots, a_n) = d(a_1, a_1, a_3, \ldots, a_n) + d(a_2, a_2, a_3, \ldots, a_n) +$
$+ d(a_1, a_2, a_3, \ldots, a_n) + d(a_2, a_1, a_3, \ldots, a_n) = d(a_1, a_2, a_3, \ldots, a_n) + d(a_2, a_1, a_3, \ldots, a_n)$.

(b) $d(a_1 + \lambda a_j, a_2, \ldots, a_n) = d(a_1, a_2, \ldots, a_n) + \lambda \cdot d(a_j, a_2, \ldots, a_n) = d(a_1, a_2, \ldots, a_n) \quad (j \in \{2, ..., n\})$.

(c) $d(a_1, ..., a_n) = d(\sum_{i_1=1}^n a_{1i_1} e_{i_1}, ..., \sum_{i_n=1}^n a_{ni_n} e_{i_n}) =$
$\sum_{i_1=1}^n \cdots \sum_{i_n=1}^n a_{1i_1} \cdot \ldots \cdot a_{ni_n} \cdot d(e_{i_1}, ..., e_{i_n}) =$
$\sum_{\pi\in F_n} a_{1\pi(1)} \cdot \ldots \cdot a_{n\pi(n)} \cdot d(e_{\pi(1)}, ..., e_{\pi(n)}) \overset{(1)}{=}$
$\sum_{\pi\in\mathcal{S}_n} a_{1\pi(1)} \cdot \ldots \cdot a_{n\pi(n)} \cdot d(e_{\pi(1)}, ..., e_{\pi(n)}) \overset{(2)}{=}$
$\sum_{\pi\in\mathcal{S}_n} a_{1\pi(1)} \cdot \ldots \cdot a_{n\pi(n)} \cdot \operatorname{sign}(\pi) \cdot d(e_1, ..., e_n)$.

(1) Es sei F_n die Menge *aller* Abbildungen $\pi : \{1, ..., n\} \to \{1, ..., n\}$.
Die fragliche Gleichung folgt aus $\mathcal{S}_n = \{\pi \in F_n : \pi \text{ injektiv}\}$ und der Voraussetzung "d alternierend".

(2) Aus (a) folgt durch Induktion nach k: Ist $\pi = \tau_1 \cdots \tau_k$ mit Transpositionen $\tau_1, ..., \tau_k$, so
$d(e_{\pi(1)}, ..., e_{\pi(n)}) = (-1)^k \cdot d(e_1, ..., e_n) \overset{9.4}{=} \operatorname{sign}(\pi) \cdot d(e_1, ..., e_n)$.

Definition.

Für $A = (a_{ij}) \in K^{n\times n}$ sei $\det(A) := \sum_{\pi\in\mathcal{S}_n} \operatorname{sign}(\pi) \cdot a_{1\pi(1)} \cdot a_{2\pi(2)} \cdots a_{n\pi(n)}$. (Leibnizsche Formel)

8.2.2010

Satz 9.6.

Die soeben definierte Funktion $\det : K^{n\times n} \to K$ ist die einzige Determinantenfunktion (zu vorgegebenem $n \geq 1$). Man nennt sie auch kurz *die Determinante*.

Beweis:

1. $\det(a_1, \ldots, a_{k-1}, a_k + \lambda b_k, a_{k+1}, \ldots, a_n) = \sum_{\pi\in\mathcal{S}_n} \operatorname{sign}(\pi) a_{1\pi(1)} \cdots (a_{k\pi(k)} + \lambda b_{k\pi(k)}) \cdots a_{n\pi(n)} =$
$\sum_{\pi\in\mathcal{S}_n} \operatorname{sign}(\pi) a_{1\pi(1)} \cdots a_{k\pi(k)} \cdots a_{n\pi(n)} + \lambda \sum_{\pi\in\mathcal{S}_n} \operatorname{sign}(\pi) a_{1\pi(1)} \cdots b_{k\pi(k)} \cdots a_{n\pi(n)} =$
$\det(a_1, \ldots, a_{k-1}, a_k, a_{k+1}, \ldots, a_n) + \lambda \det(a_1, \ldots, a_{k-1}, b_k, a_{k+1}, \ldots, a_n)$.

2. Sei $a_{1j} = a_{2j}$ für $j = 1, ..., n$. Für $\pi \in \mathcal{S}_n$ sei $\pi' := \pi \circ \tau_{1,2}$. Ferner $\mathcal{S}_n^* := \{\pi \in \mathcal{S}_n : \pi(1) < \pi(2)\}$.
Offenbar gilt $(*)$ $\mathcal{S}_n = \mathcal{S}_n^* \overset{\text{disj}}{\cup} \{\pi' : \pi \in \mathcal{S}_n^*\}$ und folglich
$\det(A) = \sum_{\pi\in\mathcal{S}_n} \operatorname{sign}(\pi) a_{1\pi(1)} \cdot a_{1\pi(2)} \cdots a_{n\pi(n)} \overset{(*)}{=}$
$\sum_{\pi\in\mathcal{S}_n^*} \operatorname{sign}(\pi) a_{1\pi(1)} \cdot a_{1\pi(2)} \cdots a_{n\pi(n)} + \sum_{\pi\in\mathcal{S}_n^*} \operatorname{sign}(\pi') a_{1\pi'(1)} \cdot a_{1\pi'(2)} \cdots a_{n\pi'(n)} =$
$\sum_{\pi\in\mathcal{S}_n^*} \operatorname{sign}(\pi) a_{1\pi(1)} \cdot a_{1\pi(2)} \cdots a_{n\pi(n)} - \sum_{\pi\in\mathcal{S}_n^*} \operatorname{sign}(\pi) a_{1\pi(2)} \cdot a_{1\pi(1)} \cdots a_{n\pi(n)} = 0$.

3. $\det(E) = \sum_{\pi\in\mathcal{S}_n} \operatorname{sign}(\pi) \delta_{1\pi(1)} \cdots \delta_{n\pi(n)} = 1$.

4. Die Eindeutigkeit folgt aus 9.5c.