„Mathematik für Informatiker I" - Prof. Dr. Potts

Dieses Dokument erhebt weder den Anspruch auf Vollständigkeit noch auf Fehlerfreiheit. Die Verwendung der hier vorliegenden Informationen geschieht also auf eigene Gefahr! Korrekturhinweise an tobias.doerffel@informatik.tu-chemnitz.de werden dankbar entgegengenommen.

Inhalt

1. Mengen, Relationen, Funktionen

1.1 Mengen

Die Mengenlehre – ein großes und relativ junges Teilgebiet der Mathematik – nimmt eine zentrale Stellung innerhalb der Mathematik ein. (G.Cantor, 1845-1918)

Definition:

1. Eine Menge ist eine Zusammenfassung von wohl unterschiedenen Objekten unserer Anschauung oder unseres Denkens. Diese Objekte heißen die Elemente der Menge. Für jedes Element ist dabei feststellbar, ob es zur Menge gehört oder nicht.
2. Ist x ein Element der Menge A, so schreibt man $x \in A$, ist x kein Element von A, so schreibt man $x \notin A$.
3. Die Menge, die kein Element enthält, nennt man die leere Menge und bezeichnen sie mit $\emptyset$.

Arten der Mengenangabe:

a) die beschreibende Mengenangabe

A = { x : x hat die Eigenschaft(en) P }

Beispiel: A = { x : x ist ein Student in Chemnitz }

b) die aufzählende Mengenangabe (die Elemente der Menge werden explizit angegeben)

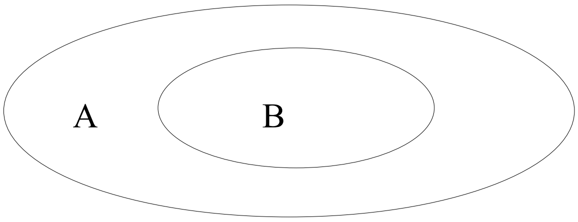
Beispiel: B = { A. Meyer, B. Müller, C.Seidel }

Im Folgenden wollen wir einige spezielle *„Relationen"* betrachten, in denen die Mengen A und B zueinander stehen können, bzw. einige *„Operationen"*, bei denen die Menge A und B einer Menge C zugeordnet sind.

a) Menge B heißt *Teilmenge der Menge A*, symbolisch $B \subseteq A$, wenn jedes Element von B auch Element von A ist.

$x \in B \Rightarrow x \in A$

Beispiel: mit Ven-Diagrammen

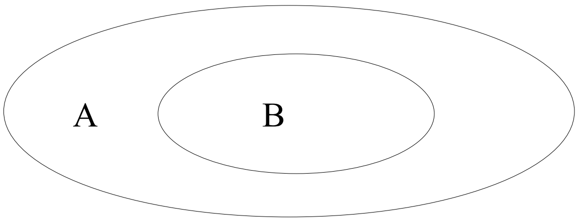


b) Die Mengen A und B heißen gleich, symbolisch $A=B$, wenn jedes Element von A auch Element von B und jedes Element von B auch Element von A ist.

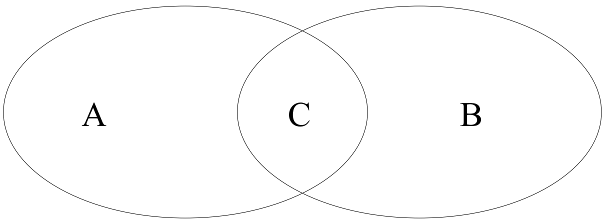
$A=B \Leftrightarrow A \subseteq B \wedge B \subseteq A$

(Das Symbol $R \Leftrightarrow S$ steht dabei als Abkürzung für „R genau dann wenn S“ bzw. „R ist äquivalent mit S“. Das Symbol $R \wedge S$ steht als Abkürzung für „sowohl R als auch S“ bzw. „R und S“. Sind A und B nicht gleich, so schreibt man $A \neq B$)

c) Die Menge B heißt *echte Teilmenge von A,* symbolisch $B \subset A$, wenn B Teilmenge von A ist, aber B ungleich A ist, d.h. $B \subset A \Leftrightarrow (B \subseteq A \wedge B \neq A)$



d) Die Menge C heißt *Durchschnitt der Mengen A und B*, symbolisch $C=A \cap B$ (sprich: C ist A geschnitten mit B), wenn C die Menge aller Elemente ist, die sowohl in A als auch in B liegen, d.h. $C=A \cap B=\{x : x \in A \wedge x \in B\}$



Erweiterung:

$\cap A_i = \{x : x \in A_i ; \forall i \in I\}$

e) Die Mengen A und B heißen *disjunkt*, wenn $A \cap B = \emptyset$

f) Die Menge C heißt V*ereinigungsmenge von A und B*, symbolisch $C = A \cup B$ (sprich: C ist A vereinigt mit B), wenn C die Menge der Elemente ist, die in A oder B liegen, d.h.

$C = A \cup B = \{x : x \in A \vee x \in B\}$

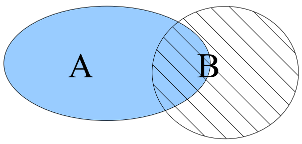
Erweiterung:

$\cup A_i = \{x : \exists i \in I \;\; mit\, x \in A_i\} \;\; i \in I$

g) Die *Differenzmenge* $C = A - B$ (manchmal $C = A \setminus B$) besteht aus allen Elementen von A, die nicht in B liegen, d.h.

$C = A - B = \{x : x \in A \wedge x \notin B\}$

Beispiel:



Ist $A \subseteq B$, so gilt $A - B = \emptyset$.

h) $A \subset M$: Die Differenz $M \setminus A$ heißt *Komplement von A abzüglich M*, symbolisch $C_M(A)$ bzw. A^C

$C_M(A) = \{x : x \notin M \wedge x \notin A\}$

(A ist in M, Menge umfasst M - A)

i) C heißt *symmetrische Differenz der Mengen A und B*. (Alles bis auf die Schnittmenge von A und B)

$A \triangle B = (A - B) \cup (B - A)$

j) C heißt *Cartesisches Produkt der Mengen A und B*, symbolisch $C=A\,x\,B$, wenn C die Menge aller geordneten Paare <x, y> von Elementen $x\in A$ bzw. $y\in B$ ist, d.h.
$AxB=\{<x,y>: x\in A, y\in B\}$

Beispiel:

A = { 0, 1 }
B = { 0, 1, 2 }
AxB = { <0, 0>, <0, 1>, <0, 2>, <1, 0>, <1, 1>, <1, 2> }

k) Die *Potenzmenge der Menge A*, symbolisch P(A), ist diejenige Menge deren Elemente alle Teilmengen der Menge A sind, d.h.

$P(A)=\{U: U\subseteq A\}$

Insbesondere gilt stets: $\emptyset\in P(A), A\in P(A)$
beachte: $P(\emptyset)=\{\emptyset\}$

$P(A)=\{U\subseteq A\}$
$A=\{1,2,3\}$
$U1=\{1\}, U2=\{2\}, U3=\{3\}, U4=\{1,2\}, U5=\{1,3\}, U6=\{2,3\}, U7=\{1,2,3\}, U8=\{\emptyset\}$

Versucht man die Ansammlung aller Mengen selbst wieder als Menge zu betrachten, so ergibt sich folgender Widerspruch:

$M=\{m: m \text{ ist Menge und } m\notin m\}$
M ist also die Menge aller Mengen, die sich nicht selbst enthalten.
- Nehmen wir zunächst an, dass $M\in M$ gilt, so folgt aus der Definition sofort $M\notin M$.
- Nehmen wir an, dass $M\notin M$, so folgt mit M ist Menge auch $M\in M$,

d.h. wir haben gezeigt:
$M\in M \Leftrightarrow M\notin M$
→ ein offensichtlicher Widerspruch

Es gibt verschiedene Ansätze, den Mengenbegriff zu revidieren, so dass oben genannter Widerspruch gelöst wird.

1.2 Relationen

Relationen zwischen Teilmengen sind z.B.

$u \subseteq v, u \subset v, u = v, u \neq v$

Die Beschreibung der Beziehung $u \subseteq v$ für Teilmengen einer vorgegebenen Menge M, d.h. für $u, v \in P(M)$, können wir etwa so vornehmen, dass wir die Teilmenge

$R = \{ <u, v>: u, v \in P(M) \wedge U \subseteq V \}$

des cartesischen Produktes $P(M) x P(M)$ vorgegeben und sagen:
U und V stehen in der Relation $\subseteq$ genau dann, wenn das geordnete Paar $<u, v>$ in R liegt.

M = { 1, 2, 3 }
P(M) = { { 1 }, { 2 }, { 3 }, { 1, 2 }, { 1, 3 }, { 2, 3 }, { 1, 2, 3 }, { Ø } }
P(M)xP(M) = { <{ 1 }, { 1 }>, <{ 1 }, { 2 }>, <{ 1 }, { 3 }>, <{ 1 }, { 1, 2 }>, <{ 1 }, { 1, 3 }>, <{ 1 }, { 2, 3 }>, <{ 1 }, { 1, 2, 3 }>, <{ 2 }, { 1 }>, <{ 2 }, { 2 }>, <{ 2 }, { 3 }>, <{ 2 }, { 1, 2 }>, <{ 2 }, { 1, 3 }>, <{ 2 }, { 2, 3 }>, <{ 2 }, { 1, 2, 3 }>, <{ 3 }, { 1 }>, <{ 3 }, { 2 }>, <{ 3 }, { 3 }>, <{ 3 }, { 1, 2 }>, <{ 3 }, { 1, 3 }>, <{ 3 }, { 2, 3 }>, <{ 3 }, { 1, 2, 3 }> ... }
R=??

Definition: Eine *zweistellige Relation* R auf einer Menge A ist eine *Teilmenge* des *cartesischen Produktes* AxA. Sind $a, b \in A$, so steht a in Relation R zu b genau dann, wenn $<a, b> \in R$ gilt. Anstelle von $<a, b> \in R$ werden die Schreibweisen aRb bzw. R(a, b) verwendet.

Beispiel: Auf jeder Menge A kann die *„Gleichheitsrelation"* (a=b) definiert werden. Wir setzen $R = \{ <a, a>: a \in A \}$, d.h. R besteht aus der Diagonale des cartesischen Produktes AxA.

spezielle Klassen von Relationen:

Definition: Eine Relation R auf der Menge A heißt *Äquivalenzrelation*, wenn sie folgende Eigenschaften hat.

1) Reflexivität: aRa für alle $a \in A$
2) Symmetrie: $aRb \Rightarrow bRa$ für alle $a, b \in A$
3) Transitivität: $(aRb \wedge bRc)$ für alle $a, b, c \in A$

Beispiel: Die *Gleichheitsrelation* ist eine *Äquivalenzrelation*.

Definition: Die Zerlegung einer Menge A in nicht leere paarweise disjunkte Teilmengen $A_i, i \in I$, heißt *Klasseneinteilung oder Partition der Menge A*, d.h. es muss gelten:

i) $\cup A_i = A$
ii) $A_i \cap A_j = \emptyset \quad \forall i, j \in I \, mit \, i \neq j$
iii) $A_i \neq \emptyset \quad \forall i \in I$

Satz: Bilden die Teilmengen $A_i, i \in I$ eine Klasseneinteilung der Menge A_i dann ist die Relation R definiert durch $xRy \, für \, x \in A_j und \, y \in A_k \;\; g.d.w. \, j = k$ eine Äquivalenzrelation.

Beweis:

i) Die Definition ist sinnvoll: Da die Teilmenge $A_i, i \in I$, paarweise disjunkt und ??? gibt es genau ein $j \in I$ mit $x \in A_j$ und ein $k \in I$ mit $y \in A_k$.
ii) R ist reflexiv: xRx, da $x \in A_j, x \in A_k \Rightarrow j = k$
R ist symmetrisch: Sei $x \in A_j, y \in A_k$ und xRy. Dann ist j=k und daher auch yRx.
R ist transitiv: Sei $x \in A_j, y \in A_k, z \in A_l$, gilt xRy und yRz, so ist j=k und k=l, d.h. j=l und damit xRz

Satz: Ist R eine Äquivalenzrelation auf der Menge A, dann bilden die Mengen $K(x) = \{y : yRx\}$ eine Klasseneinteilung von A und es gilt xRy genau dann, wenn x und y in der selben Klasse liegen..

Beweis:

i) $K(x) \neq \emptyset$, da wegen der Reflexivität von R gilt $x \in K(x)$
ii) Die Mengen K(x) sind disjunkt oder gleich: Ist $K(x) \cap K(y) \neq \emptyset$ so gibt es ein z mit $z \in K(x)$ und $z \in K(y)$, d.h. zRx und zRy und damit auch xRz bzw. yRz (Symmetrie R).
Ist nun $a \in K(x)$ beliebig, so folgt aus aRx, xRz und zRy aufgrund der Transitivität auch aRy, d.h. $a \in K(y)$, d.h. $K(x) \subseteq K(y)$.
Analog erhält man $K(y) \subseteq K(x)$, d.h. $K(x) = K(y)$.
iii) $xRy \Leftrightarrow K(x) = K(y)$: gilt xRy, so ist $x \in K(x) \cap K(y)$, d.h. $K(x) \cap K(y) \neq \emptyset$ und daher nach ii) $K(x) = K(y)$. Ist umgekehrt $K(x) = K(y)$ so gilt $x \in K(y)$ und daher xRy.

Zusammenfassung: Jede Äquivalenzrelation R entspricht also „umkehrbar eindeutig“ einer Klasseneinteilung der zugrunde liegenden Menge A. Die entsprechenden Klassen heißem auch die zu R gehörenden Äquivalenzklassen von A.

1.3 Funktionen

Problem: Was bedeutet die Aussage „A hat gleich viele Elemente wie B“ für unendliche Mengen?

Definition:

1) Seien A und B zwei (nicht leere) Mengen. Dann versteht man unter einer Funktion (oder Abbildung) f von A in B eine Vorschrift, die jedem $a \in A$ ein eindeutig bestimmtes $b \in B$ zuordnet. b heißt das Bild von a unter f, symbolisch $b = f(a)$, A heißt Definitionsbereich, B heißt *Zielbereich von f.*
2) Die Funktion $f: A \rightarrow B$ heißt *injektiv (oder eineindeutige) Abbildung von A <u>in</u> B*, wenn jedes Element $b \in B$ höchstens als Bild eines Elementes $a \in A$ unter f auftritt, d.h. $f(a_1) = b, f(a_2) = b \Rightarrow a_1 = a_2 \quad \forall a_1, a_2 \in A, b \in B$ oder äquivalent dazu $a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2) \quad \forall a_1, a_2 \in A$
3) Die Funktion $f: A \rightarrow B$ heißt *surjektiv (oder Abbildung von A auf B)*, wenn jedes $b \in B$ mindestens einmal als Bild eines Elementes $a \in A$ unter f auftritt, d.h. zu jedem $b \in B$ existiert ein $a \in A$ mit $f(a) = b$.
4) Die Funktion $f: A \rightarrow B$ heißt *bijektiv oder eineindeutige Abbildung von A <u>auf</u> B*, wenn f injektiv und surjektiv ist.

Definition: Die Mengen A und B heißen *gleichmächtig*, symbolisch A ~ B, wenn *eineindeutige (injektive)* Zuordnung der Elemente von A auf die Elemente von B existiert.

Definition: (Kardinalzahl einer Menge A, |A|, card A, c(A), #A)

1) Hat die Menge A nur endlich viele Elemente, so bezeichnet $|A|$ die Anzahl der Elemente von A.

Beispiel:
Die Menge $\mathbb{N} = \{1, 2, 3, \ldots\}$ erhält die Kardinalzahl $|\mathbb{N}|$.
Betrachten wir die Menge $\mathbb{Q}^+$ der positiven rationalen Zahlen, so ergibt sich die Frage, ob $\mathbb{Q}^+$ *„mächtiger“* als $\mathbb{N}$ ist. Das „Cantersche Diagonalverfahren“ liefert eine eineindeutig Abbildung von $\mathbb{N}$ auf $\mathbb{Q}^+$, damit ist auch $|\mathbb{Q}^+| = |\mathbb{N}|$. Wir schreiben alle Brüche $\frac{p}{q}$ mit $p, q \in \mathbb{N}$ in ein Rechteckschema wie folgt

$$
\begin{array}{cccccc}
\frac{1}{1} & \frac{2}{1} & \frac{3}{1} & \frac{4}{1} & \frac{5}{1} & \ldots \\[2ex]
\frac{1}{2} & \cancel{\frac{2}{2}} & \frac{3}{2} & \cancel{\frac{4}{2}} & \frac{5}{2} & \ldots \\[2ex]
\frac{1}{3} & \frac{2}{3} & \cancel{\frac{3}{3}} & \frac{4}{3} & \frac{5}{3} & \ldots \\[2ex]
\frac{1}{4} & \cancel{\frac{2}{4}} & \frac{3}{4} & \cancel{\frac{4}{4}} & \frac{5}{4} & \ldots \\
\vdots & & & & &
\end{array}
$$

Die Elemente werden nun wie oben durchnummeriert, wobei Brüche, die eine bereits durchlaufene Zahl aus $\mathbb{Q}^+$ darstellen, übergangen werden.
Eine unendliche Menge, die zur Menge $\mathbb{N}$ gleichmächtig ist, heißt abzählbar.

Die Menge $\mathbb{R}$ der reellen Zahlen ist <u>nicht</u> abzählbar.

Beweis: (indirekter Beweis).

Wir nehmen an, man kann die reellen Zahlen zwischen 0 und 1 abzählen und schreiben eine Abzählung an.

1. 0, d_{11}, d_{12}, d_{13}, d_{14},...
2. 0, d_{21}, d_{22}, d_{23}, d_{24},...
3. 0, d_{31}, d_{32}, d_{33}, d_{34},...

Wir definieren nun die Dezimalstelle $d_i = \{1 \text{ falls } d_{ii} = 2, \text{ sonst } 2\}$
dann ist $x = 0.d_1 d_2 d_3 \ldots$ nicht in obiger Aufzählung enthalten, im Widerspruch zur Annahme der Abzählbarkeit.

2. Zahlen

Die Menge der natürlichen Zahlen $\mathbb{N}=\{1,2,3,\ldots\}$ lässt sich durch ***Peano-Axiome*** kennzeichnen:

1. Eins (1) ist eine natürliche Zahl $1\in\mathbb{N}$
2. Jede natürliche Zahl n hat genau einen Nachfolger $n\in\mathbb{N}\Rightarrow(n+1)\in\mathbb{N}$
3. Eins ist nicht Nachfolger einer natürlichen Zahl $n\in\mathbb{N}\Rightarrow(n+1)\neq 1$
4. Jede natürliche Zahl ist Nachfolger höchstens einer natürlichen Zahl. $n\neq m\Rightarrow(n+1)\neq(m+1)$
5. Ist S eine Menge von natürlichen Zahlen, so dass gilt
   a) $1\in S$
   b) mit jeder Zahl $n\in S$ ist auch ihr Nachfolger $n+1\in S$,
      d.h. $n\in S\Rightarrow n+1\in S$
      dann ist S die Menge der natürlichen Zahlen (d.h. jede natürliche Zahl liegt in S)

Aus Axiom 5 erhalten wir unmittelbar eines der wichtigsten mathematischen Beweisprinzipien.

2.1. Beweisprinzip der vollständigen Induktion

Ist eine Aussage $A(n)$ abhängig von der natürlichen Zahl n und gilt

1) $A(1)$ ist wahr
2) aus der Annahmen „ $A(n)$ ist wahr“ kann hergeleitet werden, dass auch „ $A(n+1)$ ist wahr“ gilt, d.h. für alle $n\in\mathbb{N}$ gilt: $A(n)\Rightarrow A(n+1)$, dann ist $A(n)$ wahr für alle natürlichen Zahlen n.

Eine vollständige Induktion sollte man immer nach dem folgenden Schema durchführen:

Induktionsanfang: Zeige $A(1)$ ist richtig.
Induktionsannahme: Wir nehmen an: $A(n)$ ist richtig für ***ein*** $n\in\mathbb{N}$
Induktionsschluss: Zeige: dann ist auch $A(n+1)$ richtig

Nach dem Beweisprinzip der vollständigen Induktion gilt dann die Aussage für alle $n\in\mathbb{N}$ (oder besser nach Axiom 5, denn sei $M=\{n\in\mathbb{N}: A(n) \textit{ ist richtig für } n\}$, dann ist nach Induktionsanfang $1\in M$ und ist $n\in M$, so auch $n+1$ und damit nach Axiom 5: $m\in\mathbb{N}$)

Beispiel:

Beweise: Die Summe der natürlichen Zahlen von 1 bis n ist $\frac{(n+1)\cdot n}{2}$

Induktionsanfang: A(1): $1=\frac{1\cdot(1+1)}{2}$ → w.A.

Induktionsannahme: Angenommen A(n) stimmt für ein $n\in\mathbb{N}$

z.z. $A(n+1)$ ist richtig

Induktionsschluss: dann gilt,

$$(1+2+3+\ldots+n)+n+1=\frac{n\cdot(n+1)}{2}+(n+1)$$

$$\frac{n\cdot(n+1)}{2}+\frac{2\cdot(n+1)}{2}=\frac{(n+1)\cdot(n+2)}{2}$$

also ist die Aussage für $A(n+1)$ richtig, denn $A(n+1)$ heißt

$$A(n+1)=1+2+3+\ldots+n+1=\frac{(n+1)\cdot(n+2)}{2}$$

Ein weiteres Beispiel:

Die Formel $1^2+2^2+\ldots+n^2=\frac{(n+1)\cdot(2\cdot n+1)}{6}$

soll für alle $n\in\mathbb{N}$ bewiesen werden.

Induktionsanfang: $A(1)$ ist wahr, denn

$$1^2=\frac{(1\cdot(1+1)\cdot(2\cdot 1))}{6}$$ w.A.

Induktionsannahme: Angenommen $A(n)$ stimmt für ein

$$A(n)\colon 1^2+2^2+\ldots+(n+1)^2=\frac{n\cdot(n+1)\cdot(2\text{n}+1)}{6}$$

dann müssen wir

$A(n+1)\colon 1^1+2^1+\ldots+(n+1)^2=\frac{(n+1)\cdot(n+2)\cdot(2n+3)}{6}$

Induktionsschluss:

$$1^1+1^2+\ldots+(n+1)^2=1^2+2^2+\ldots+n^2+(n+1)^2=\frac{(n\cdot(n+1)\cdot(2\cdot n+1))}{6}+(n+1)^2=$$
$$\frac{(n\cdot(n+1)\cdot(2n+1))}{6}+\frac{6\cdot(n+1)^2}{6}=\frac{(n+1)\cdot(n\cdot(2\cdot n+1)+6\cdot(n+1))}{6}=$$
$$\frac{(n+1)\cdot(2\cdot n^2+n+6\cdot n+6)}{6}=\frac{(n+1)\cdot(n+2)\cdot(2\cdot n+3)}{6}$$

Damit haben wir $A(n)\ \forall n\in\mathbb{N}$ gezeigt.

Zur Abkürzung von Summen und Produkten verwendet man folgende Symbole: Es seien $k, l\in\mathbb{N}$

$$\sum_{i=k}^{l} a_i=\begin{Bmatrix} a_k+a_{k+1}+\ldots+a_l \text{ für } k\le l \\ 0 \text{ für } k>l \text{ (leere Summe)}\end{Bmatrix}$$

$$\prod_{i=k}^{l} a_i=\begin{Bmatrix} a_k+a_{k+1}+\ldots+a_l \text{ für } k\le l \\ 0 \text{ für } k>l \text{ (leere Summe)}\end{Bmatrix}$$

2.2 Die ganzen rationalen und reellen Zahlen

Addition und Multiplikation sind im Bereich der natürlichen Zahlen uneingeschränkt ausführbar.

Problem: sind $a, b\in\mathbb{N}$, so braucht die Lösung der Gleichung $x+a=b$ in $\mathbb{N}$ nicht zu existieren.

$\mathbb{Z}=\{\ldots -3,-2,-1,0,1,2,\ldots\}$

Problem: sind $a, b\in\mathbb{Z}$, so braucht die Lösung $bx=a$ in $\mathbb{Z}$ nicht zu existieren.

$\mathbb{Q}=\left\{\frac{m}{n}\colon m\in\mathbb{Z}, n\in\mathbb{Z}\setminus\{0\}\right\}$ rationale Zahlen

<u>Problem:</u> Die Gleichung $x^2=2$ besitzt keine Lösung in $\mathbb{Q}$.
Beweis: Nehmen wir an, es gäbe eine Lösung x der Gleichung $x^2=2$ in $\mathbb{Q}$; da mit x auch -x Lösung der Gleichung ist, können wir annehmen $x>0$.

Dann besitzt $x=\frac{p}{q} \quad p,q \in\mathbb{N}$. Wir können annehmen, dass p und q teilerfremd sind, d.h. der Bruch gekürzt ist.

$\rightarrow\frac{p^2}{q^2}=2$
$\rightarrow p^2=2q^2$
$\rightarrow p^2 \text{ ist eine gerade Zahl}$
$\rightarrow p \text{ ist eine gerade Zahl } \; 2k, k \in\mathbb{N}$
$\rightarrow p^2=4k^2=2q^2$
$\rightarrow 2k^2=q^2$
$\rightarrow q \text{ ist gerade}$

Dies ist ein Widerspruch zur Teilerfremdheit von p und q.
Die rationalen Zahlen lassen Lücken auf der Zahlengerade.

Die exakte Definition der reellen Zahlen kann auf verschiedene Arten vorgenommen werden, verzichten wir hier aber auf eine genauere Darstellung. Insbesondere wollen wir die Addition und Multiplikation reeller Zahlen als bekannt voraussetzen. Für diese Operationen sind die folgenden Eigenschaften erfüllt.

I) *Abgeschlossenheit*:
   1. $a,b\in\mathbb{R}\Rightarrow a+b\in R$
   2. $a,b\in R\Rightarrow a\cdot b\in R$

II) *Assoziativgesetz*:
   1. $a,b,c\in R\Rightarrow(a+b)+c=a+(b+c)$
   2. $a,b,c\in R\Rightarrow(a\cdot b)\cdot c=a\cdot(b\cdot c)$

III) Existenz von „*Einheitselementen*“: Es gibt Elemente $0\in\mathbb{R}, 1\in\mathbb{R}\setminus\{0\}$, so dass
   1. $a\in\mathbb{R}\Rightarrow a+0=0+a=a$
   2. $a\in\mathbb{R}\Rightarrow a*1=1*a=a$

IV) Existenz von „*inversen Elementen*“
   1. $a\in\mathbb{R}\Rightarrow a+(-a)=(-a)+a=0$
   2. $a\in\mathbb{R}\setminus\{0\}\Rightarrow\frac{a\cdot 1}{a}=\frac{1}{a}\cdot a=1$

      (Beachte für a=0 existiert kein Elemente $\frac{1}{a}$ in $\mathbb{R}$)

V) Kommutativgesetz
   1. $a,b\in\mathbb{R}\Rightarrow a+b=b+a$
   2. $a,b\in\mathbb{R}\Rightarrow a\cdot b=b\cdot a$

VI) Distributivgesetz
   1. $a,b,c\in\mathbb{R}\Rightarrow a\cdot(b+c)=a\cdot b+a\cdot c$

VII) *Ordnungseigenschaft*: Es ist eine *Ordnungsrelation* $\leq$ gegeben mit
   1. für beliebige $a,b\in\mathbb{R}$ gilt $a\leq b$ oder $b\leq a$
   2. $a\leq b\Rightarrow a+c\leq b+c$
   3. $a\leq b\wedge c\geq 0\Rightarrow a\cdot c\leq b\cdot c$

(2) und (3) gibt an, dass die Ordnungsrelation mit den algebraischen Operationen verträglich ist

Beachte: Diese Axiome werden auch von den rationalen Zahlen $\mathbb{Q}$ erfüllt. Wir brauchen ein Axiom, welches $\mathbb{Q}$ und $\mathbb{R}$ unterscheidet.

2.2.1 Vollständigkeitsaxiom/Stetigkeitsaxiom

Zerlegt man die Menge $\mathbb{R}$ in zwei Mengen N und M mit der Eigenschaft $\mathbb{R}=N\cup M$, wobei $N\neq\emptyset, M\neq\emptyset$ und für $\forall x\in N, y\in M$ gilt: $x\leq y$. Dann gibt es genau ein Element $s\in\mathbb{R}$ (Schnittzahl) mit $x\leq s\leq y \quad \forall x\in N, y\in M$

Bemerkung: $\mathbb{Q}$ erfüllt nicht das Vollständigkeitsaxiom

$M=\{a\in\mathbb{Q}: a^2\leq 2\}\cup\{a\in\mathbb{Q}: a\leq 0\}$
$M=\{a\in\mathbb{Q}: a^2\geq 2\}\setminus\{a\in\mathbb{Q}: a\geq 0\}$

gibt es keine Schnittzahl in $\mathbb{Q}$. Dies wäre ja $s=\sqrt{(2)}\notin\mathbb{Q}$.

- Eine Menge G mit einer binären Operation „+“ die die Regel I, II, III, IV, V erfüllt, heißt abelsche Gruppe.
- Eine Menge G mit den Operationen $+$ und $*$ heißt Körper.

2.3 Maschinenzahlen

Die reellen Zahlen können nur unvollständig am Computer realisiert werden.
- In exakter Arithmetik wie z.B. maple sind reelle Zahlen durch symbolische Ausdrücke gegeben
- Die in Programmiersprachen üblicherweise als Modell für die reellen Zahlen verwendeten Gleitkommazahlen (floating point numbers) haben feste relative Genauigkeit

Für Maschinenzahlen gelten die Rechenregeln von $\mathbb{R}$.

2.4 Die komplexen Zahlen

Problem: Die Gleichung $x^2+1=0$ besitzt keine Lösung in $\mathbb{R}$ (für $x\in\mathbb{R}$ ist stets $x^2\geq 0$).

Wir bezeichnen die „Lösung“ der Gleichung mit i, so können wir mit Objekten der Form $a+ib, a, b\in\mathbb{R}$ rechnen.

Definition: Unter einer komplexen Zahl z verstehen wir ein geordnetes Paar <a, b> von reellen Zahlen.

$$z=a+ib$$

a heißt Realteil von z: $a=\Re(z)$
b heißt Imaginärteil von z: $b=\Im(z)$
Die Menge aller komplexen Zahlen bezeichnen wir mit $\mathbb{C}$. Seien $a, b, c, d\in\mathbb{R}$. Dann sind Summe und Produkt von komplexen Zahlen definiert durch

$$(a+ib)+(c+id)=(a+c)+i(b+d)$$

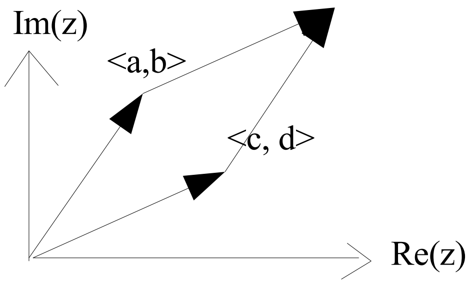
bzw.

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

Die reellen Zahlen werden als Teilmenge aller komplexen Zahlen der Form $(a+i*0) \quad a\in\mathbb{R}$ aufgefasst.

- Das obige Produkt genügt der Forderung
  $i^2=(0+i\cdot 1)\cdot(0+i\cdot 1)=-1+i\cdot 0=-1$
- man sieht leicht, dass die Menge $\mathbb{C}$ mit den Operationen der Addition und Multiplikation die Eigenschaften eines Körpers besitzt.

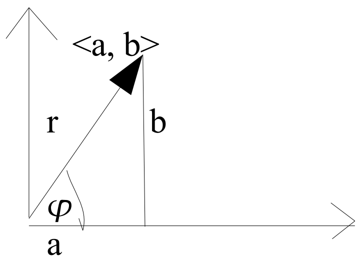
2.4.1 Geometrische Interpretation der Addition



Gaußsche Zahlenebene. Komplexe Zahlenebene.

2.4.2 Geometrische Interpretation der Multiplikation

– Benutzung von „Polarkoordinaten" [r, φ] des Punktes <a, b>



Es gilt:

$$a = r \cdot \cos\varphi$$
$$b = r \cdot \sin\varphi$$

bzw.

$$r = \sqrt{a^2 + b^2}$$
$$\tan\varphi = \frac{b}{a}$$

$$z = r \cdot (\cos\varphi + i \cdot \sin\varphi)$$

r ist Absolutbetrag von z
φ ist Argument von z

$z_1=[r_{1,}\varphi_1]=r_1\cdot(\cos\varphi_1+i\cdot\sin\varphi_1)$
$z_2=[r_{2,}\varphi_2]=r_2\cdot(\cos\varphi_2+i\cdot\sin\varphi_2)$

$z_1\cdot z_2=z_1\cdot z_2\cdot[(\cos\varphi_1\cdot\cos\varphi_2-\sin\varphi_1\cdot\sin\varphi_2)+i\cdot(\cos\varphi_1\cdot\sin\varphi_2-\sin\varphi_1\cdot\cos\varphi_2)]$

$\sin(\alpha+\beta)=\sin\alpha\cdot\cos\beta+\cos\alpha\cdot\sin\beta$
$\cos(\alpha+\beta)=\cos\alpha\cdot\cos\beta+\sin\alpha\cdot\sin\beta$

also

$z_1\cdot z_2=[r_1\cdot r_{2,}\varphi_1+\varphi_2]$

Definition: Sei $z=a+ib\in\mathbb{C}$. Dann heißt $\overline{z}=a-ib\in\mathbb{C}$ die konjugiert komplexe Zahl z.

Es ergeben sich dann die folgenden Beziehungen:

$$z+\frac{\overline{z}}{z}=\Re(z)\ ;\quad z-\frac{\overline{z}}{z_i}=\Im(z)\ ;\quad z\cdot\overline{z}=|z|^2\quad(Norm von z)$$

Mit diesen Beziehungen ergibt sich:

$z=[r,\varphi]$ und $z^{-1}=[\zeta,\vartheta]$

d.h. $[r,\varphi]\cdot[\zeta,\vartheta]=[r\cdot\zeta,\varphi+\vartheta]=1=[1,0]$

$r\cdot\zeta=1\qquad\varphi+\vartheta=0+2k\cdot\pi\qquad k\in\mathbb{Z}$

Definieren wir die Potenzen $z^n(n\in\mathbb{N})$, der Zahl $z\in\mathbb{C}$ wieder rekursiv $z^0=1,z^{n+1}=z^n\cdot z$ für alle $n\in\mathbb{N}$, so erhalten wir $z=[r,\varphi]\Rightarrow[r\cdot n,n\cdot\varphi]$ für alle $n\in\mathbb{N}$.

bzw.

$z=r\cdot(\cos\varphi+i\cdot\sin\varphi)\Rightarrow z^n=r^n\cdot(\cos n\varphi+i\cdot\sin n\varphi)$

2.4.3 Wurzelziehen im Bereich der komplexen Zahlen

Wir nennen jede Lösung w der Gleichung $w^n = z$ eine n-te Wurzel der komplexen Zahl z.

Es sei $z = [r, \varphi] = r \cdot (\cos\varphi + i \cdot \sin\varphi)$ und $w = [\zeta, \vartheta] = \zeta \cdot (\cos\vartheta + i \cdot \sin\vartheta)$ eine Lösung von $w^n = z$, d.h. $[\zeta n, n\vartheta] = [r, \varphi]$.

1. Fall: z=0, d.h. r=0, d.h. r=0 => $\zeta^n=0$ => w=0 ϑ beliebig
2. Fall: z≠0, d.h. $r \neq 0 \Rightarrow \zeta^n = r \Rightarrow \zeta^n = \sqrt[n]{r}$

$$n \cdot \vartheta = \varphi + 2k \cdot \pi \qquad k \in \mathbb{Z}$$
$$\vartheta = \frac{(\varphi + 2k \cdot \pi)}{n} \qquad k \in \mathbb{Z}$$

Definition: Seien $x, y, q \in \mathbb{C}$. Dann heißt x und y kongruent modulo q $x \equiv y\, mod(q)$, wenn eine Zahl $l \in \mathbb{Z}$ existiert, so dass $x + y = lq$.

Sei $z \neq 0$. Dann sind die Wurzeln von $z = r \cdot (\cos\varphi + i \cdot \sin\varphi)$ die Zahlen

$$\sqrt[n]{r} \cdot \cos\frac{\varphi + 2k \cdot \pi}{n} + i \cdot \sin\frac{\varphi + 2k \cdot \pi}{n} \qquad k \in \mathbb{Z}$$

wobei $k_{1,} k_2 \in \mathbb{R}$ genau dann den gleichen Wert liefern, wenn $k_1 = k_2 \cdot mod(n)$ gilt.
Man erhält also alle verschiedenen Werte von $\sqrt[n]{z}$, indem man alle $k \in \{0, 1, 2, \ldots, n-1\}$ verwendet.

Beispiel:

$$z^8 = 1$$
$$\sqrt[n]{1} \cdot \cos(\frac{2k \cdot \pi}{8}) + i \cdot \sin\frac{2k \cdot \pi}{8} \qquad k = 0, 1, 2, \ldots, 7$$

→ 8 Lösungen im Bereich der komplexen Zahlen

Aus obiger Überlegung folgt: Jedes Polynom der Gestalt $w^n = z \quad (z \neq 0)$ besitzt n Wurzeln.

Es gilt sogar mehr: ***(Fundamentalsatz der Algebra)***

Jede algebraische Gleichung $p_n(z) = c_n \cdot z^n + c_{n-1} \cdot z^{n-1} + \ldots + c_0 = 0 \quad (c_i \in \mathbb{C})$ vom Grade $n \geq 1$ besitzt in $\mathbb{C}$ mindestens eine Lösung.
Daraus folgt unmittelbar: Jedes Polynom $p_n(z)$ lässt sich in der Form $p_n(z) = c_n(z - z_1) = c_1 \cdot (z - z_1) \cdot (z - z_2) \cdot \ldots \cdot (z - z_n)$ schreiben. Die komplexen Zahlen $z_{1,} z_{2,} \ldots, z_n$ sind die Nullstellen des Polynoms. Sind unter den $z_{1,} z_{2,} \ldots, z_n$ gleiche Zahlen spricht man von mehrfachen Nullstellen.

3. Algebraische Strukturen

3.1. Gruppoid, Halbgruppe, Monoid, Gruppe

Definition: unter einer algebraischen Struktur verstehen wir eine nicht leere Menge G mit einer oder mehreren „Operationen“.
Im Folgenden betrachten wir zweistellige (oder binäre) Operationen, d.h. eine Vorschrift *, die jedem geordneten Paar <a, b> von Elementen $a,b \in G$ ein Ergebnis $a * b \in G$ zuordnet. $<G, *>$ hat also die Eigenschaft (G1).

(G1) ist *Abgeschlossenheit*: $a,b \in G \Rightarrow a * b \in G$ oder: Eine zweistellige Operationen * ist eine Funktion *: $GxG \rightarrow G$.

Beispiel: M ist eine beliebige Menge.
$G = P(M); \quad Potenzmenge\, P(M) = \{U : U \subseteq M\}$
Offensichtlich erfüllt $<G, U>$ die Eigenschaft (G1). $A, B \in P(M) \Rightarrow A \cup B \in P(M)$

(G2) *Assoziativgesetz*: $(a*b)*c = a*(b*c) \qquad \forall a, b, c \in G$

(G3) Existenz eines *Einheitselementes*: Es existiert ein Element $e \in G$, so dass für alle $a \in G$ gilt: $a*e = e*a$

(G4) Existenz von *„inversen Elementen“*: für jedes $a \in G$ existiert ein $a' \in G$ mit der Eigenschaft $a*a' = a'*a = e$. (wobei e das Einheitselement aus (G3) ist. Statt a' schreiben wir a^{-1} .)

(G5) *„Kommutativgesetz“*: $a*b = b*a \qquad \forall a, b \in G$

Beispiel: $G = \mathbb{R}^{+} = \{x : x \in \mathbb{R} \wedge x > 0\}$
„*“ ist die Zuordnung $<a, b> \rightarrow a^{b}$.

(G1) ist erfüllt, denn $a^{b} \in \mathbb{R}^{+}$
(G2) ist i.a. nicht erfüllt, weil z.B. $(2^{2})^{3} \neq 2^{(2^{3})}$
(G3) e=1 ist ein Rechtseinheitselement, denn $a*e = a, a^{1} = a$
(G4) gilt nicht
(G5) gilt nicht, denn z.B. $2^{3} = 8 \;\; aber \;\; 3^{2} = 9$

Beispiel: G die Menge aller Bewegungen in der Ebene, d.h. alle Abbildungen die sich als Zusammensetzung von Drehung und Translation (Parallelverschiebung) ergeben. „*“ ist die „Zusammensetzung“ (Hintereinanderausführungen von Abbildungen)

(G1) ist erfüllt
(G2) ist erfüllt
(G3) Einheitselement: identische Abbildung, nämlich Drehung um 0° und Translation um 0 in eine beliebige Richtung
(G4) inverses Element: inverse Bewegung (zurückdrehen, zurückverschieben)
(G5) ist nicht erfüllt: z.B. Drehung um 90° und Verschiebung um (1 0)

Satz (Eindeutigkeit des Einheitselements e): $<G,*>$ erfüllt G1. Dann gibt es höchstens ein Element $e \in G$ mit $a*e=e*a=a \quad \forall a \in G$

Beweis: Es gelte

$$a*e_1=e_1*a=a \quad \forall a \in G \quad (1)$$
$$a*e_2=e_2*a=a \quad \forall a \in G \quad (2)$$

Wir setzen in (1) $a=e_2$ so folgt $e_2*e_1=e_2$ setzen wir in (2) $a=e_1$, so folgt $e_2*e_1=e_1$, d.h. $e_1=e_2$.

Satz: $<G,*>$ erfüllt (G1), (G2), (G3). Dann gibt es zu jedem $a \in G$ höchstens ein $a' \in G$ mit $a*a'=a'*a=e$.

Beweis: es gelte
$$a*a_1=a_1*a=e \quad und \quad (1)$$
$$a*a_2=a_2*a=e$$

Dann ist aber $a_1=a_1*e=a_1*(a*a_2)=(a_1*a)*a_2=e*a_2=a_2$

Definition: Eine algebraische Struktur $<G,*>$ mit einer zweistelligen Operation * heißt

- *Gruppoid*, wenn sie (G1) erfüllt
- *Halbgruppe*, wenn sie (G1) und (G2) erfüllt.
- *Monoid*, wenn sie (G1)-(G3) erfüllt.
- *Gruppe*, wenn sie (G1), (G2), (G3) und (G4) erfüllt.
- *Kommutative* oder *Abelsche Gruppe*, wenn sie (G1)-(G5) erfüllt.

Beispiele:

Gruppoid	$<\mathbb{R}^{+}, *>$ mit $a*b=a^{b}$
Halbgruppe	$<\mathbb{R}^{+}, +>$
Gruppoid	$<\mathbb{N}\cup\{0\}, +>$ $(e=0)$
Gruppe	$<Bewegung \in der\, Ebene, *>$ $(s.o.)$
Abelsche Gruppe	$<\mathbb{Z}, +>, <\mathbb{R}, +>, <\mathbb{R}, \cdot>$

Definition: Sei $<G, *>$ eine Gruppe. Eine Teilmenge $H \subseteq G$ für die $<H, *>$ wiederum eine Gruppe ist, heißt *Untergruppe* von $<G, *>$ (insbesondere muss $H \neq \emptyset$ gelten).
Zum Nachweis, dass $<H, *>$ Untergruppe von der Gruppe $<G, *>$ ist. braucht nicht (G1)-(G4) geprüft werden, denn es gilt:
Satz: $<H, *>$ ist genau dann Untergruppe von $<G, *>$, wenn

1) H nicht leere Teilmenge von G ist,
2) für alle $a, b \in H$ gilt: $a*b^{-1} \in H$ (b^{-1} = inverses Element zu b)

Beweis:

i) $<H, *>$ erfüllt (G2), da die Gültigkeit des Assoziativgesetzes beim Übergang von G zu einer Teilmenge erhalten bleibt.
ii) mit $a \in H$ ist wegen 2) auch $a*a^{-1}=a \in H$. Es gilt $a*e=e*a=a \quad \forall a \in H$, da diese Identität sogar für alle $a \in G$ gilt. $<H, *>$ erfüllt also (G3).
iii) Da $e \in H$ ist mit $a \in H$ auch $e*a^{-1}=a^{-1} \in H$ und es gilt $a*a^{-1}=a^{-1}*a=e$, d.h. $<H, *>$ erfüllt (G4).
iv) Seien $a, b \in H$. Damit ist $b^{-1} \in H$ und damit auch $(b^{-1})^{-1} \in H$ und nach 2) $a*(b^{-1})^{-1} \in H$ wegen $b^{-1}*(b^{-1})^{-1}=e=(b^{-1})^{-1}*b^{-1}$ ist aber $(b^{-1})^{-1}=b$ so dass $a*(b-1)^{-1}=a*b$, d.h. $a*b \in H$ und H erfüllt (G1).

Ist die Gruppe $<G, *>$ endlich, so lässt sich die Forderung (2) nochmals abschwächen.

Definition: Sei $<G, *>$ eine Gruppe. Dann sind die *Potenzen* von $a^{n} (n \in \mathbb{N})$ eines Elementes $a \in G$ rekursiv bestimmt durch

$$a^{0}=e, \quad a^{n}=a^{n-1}*a \quad \forall n \in \mathbb{N}$$

Gibt es mindestens ein $n \in \mathbb{N}$, so dass $a^{n}=e$. So heißt die kleinste Zahl $n_{0} \geq 1$ mit dieser Eigenschaft die *Ordnung von a in G*: $n_{0}=O_{o}(a)$. Ist $a^{n} \neq e \quad \forall n \in \mathbb{N}$, so hat *a unendliche Ordnung* in G.

Satz: Ist $<G,*>$ eine Gruppe und hat a endliche Ordnung in G, d.h. $O_G(a)=n\in\mathbb{N}$, so ist $a^{n-1}=a^{-1}$.

Ist G endlich, so hat jedes $a\in G$ endliche Ordnung.

Beweis: es gilt: $a*a^{n-1}=a^n=e,\quad a^{n-1}*a=a^n=e$ und damit $a^{n-1}=a^{-1}$.
Zum Beweis des 2. Teils betrachten wir für festes $a\in G$ die $M(a)=\{a^n: n\in\mathbb{N}\}$. Da $M(a)\subseteq G$, ist auch $M(a)$ endlich → es gibt Zahlen $m,n\in\mathbb{N}$ mit 0<m<n für die gilt:

$$a^n=a^m$$
$$a^{m-1}*e=a^{m-1}*(a*a^{-1})=a^m*a^{-1}=(a^{n-1}*a)*a^{-1}=a^{n-1}*e=a^{n-1}$$

Führt man die Reduktion des Exponenten (n-m) mal durch, so erhält man $e=a^0=a^{n-m}$ mit $n-m\geq 1$ → a hat endliche Ordnung.

Beispiel:

$G=\{0,1,2,3\}$ bildet mit der durch die Verknüpfungstafel

*	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

definierte Operation * einer Gruppe
$M(0)=\{0\}$
$M(1)=\{1,2,3,0\}$
$M(2)=\{2,0\}$
$M(3)=\{3,2,1,0\}$

Beweis:

z.z.: $a,b\in H\Rightarrow a*b^{-1}\in H\quad\forall a,b\in H$ (nach Satz von S. 22)

Da G endlich ist, hat jedes $b\in G$ endliche Ordnung und es gibt $b^{-1}=b^{O_G(b)-1}$, wobei $O_G(b)-1\in\mathbb{N}$ ist. Wegen der Eigenschaft 2) von $<H,*>$ ist mit $b\in H$ auch $b^n\in H\quad\forall b\in H$. Damit ist für $b\in H$ auch $b^{-1}\in H$, wenn $O_G(b)-1\geq 1$, d.h. $O_G(b)\geq 2$ gilt.

noch z.z.: Ist $O_G(b)=1$, d.h. $b^{-1}=b=e$, so ist wegen $e^{-1}=e$ ebenfalls $b^{-1}\in H$. Für jedes $b\in H$ ist auch $b^{-1}\in H$. Wegen 2) ist dann aber für alle $a,b\in H$ auch $a*b^{-1}\in H$ und $<H,*>$ ist Untergruppe von $<G,*>$.

Besitzt das Element $a\in G$ endliche Ordnung n , so bildet insbesondere $<H=\{a^1,a^2,\ldots,a^n=e\},*>$ eine Untergruppe von $<G,*>$. $<H,*>$ heißt die von a erzeugte zyklische Untergruppe von $<G,*>$.

3.2 Ringe, Halbringe, Integritätsbereich, Körper

Jetzt betrachten wir algebraische Strukturen mit zwei zweistelligen Operationen.

Definition: $<H,+,\circ>$ heißt Ring, wenn

1) $<H,+>$ eine abelsche Gruppe (G1-G5) ist
2) $<H,\circ>$ eine Halbgruppe (G1-G2) ist und
3) die *Distributivgesetze* gelten:
$a\circ(b+c)=a\circ b+a\circ c$
$(a+b)\circ c=a\circ c+b\circ c \quad \forall a,b,c\in H$

Beispiele:
- $<\mathbb{Z},+,\circ>,<\mathbb{Q},+,\circ>,<\mathbb{R},+,\circ>,<\mathbb{C},+,\circ>$
- Restklassenring modulo m, Z_m
- sei m fest vorgegeben: $x,y\in Z$ heißt kongruent modulo m, symbolisch $x\equiv y\,(mod\, m)$

Wenn es ein $l\in\mathbb{Z}$ gibt mit $x-y=l\circ m$, d.h. $x\equiv y\,(mod\, m)\Leftrightarrow\exists\, l\in Z\, mit\, x-y=l\circ m.$

Man sieht leicht, dass hierdurch eine Äquivalenzrelation auf Z definiert wird. Die zu x gehörige Äquivalenzklasse hat die Gestalt

$$\bar{x}=\{y:y=x+l\circ m, l\in\mathbb{Z}\}$$

Die Menge aller Äquivalenzklassen wird mit Z_m bezeichnet. Speziell ist

$$Z_m=Z_{-m}, Z_0=Z, Z_1=\bar{0} \quad \bar{0}=\{y:y=0+l\in\mathbb{Z}\}$$

Wir beschränken uns im Folgenden auf $m\in\mathbb{N}$. Auf Z_m kann eine Addition und Multiplikation definiert werden durch

$$\bar{x}+\bar{y}=\overline{x+y}$$
$$\bar{x}\circ\bar{y}=\overline{x\circ y}$$

Man zeigt leicht, dass
$<Z_m, +>$ eine kommutative Gruppe
$<Z_m, \circ>$ ein kommutatives Monoid

und die Distributivgesetze gelten.

Beispiel: Verknüpfungstafel der Multiplikation in $\mathbb{Z}_4$

*	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	0	0	0	0
$\bar{1}$	0	1	2	3
$\bar{2}$	0	2	0	2
$\bar{3}$	0	3	2	1

- Das Einheitselement bezüglich der Operation „+“ in einem Ring heißt auch Nullelement, hier ist es die Restklasse $\bar{0}$.
- Besitzt ein Ring auch ein Einheitselement bezüglich „*“, welches vom Nullelement verschieden ist, so heißt $<H, +, \circ>$ Ring mit Einselement.
- In $\mathbb{Z}$ (wie auch in $\mathbb{Q}, \mathbb{R}, \mathbb{C}$) ist die Gleichung $a \cdot b = 0$ nur dann erfüllt, wenn mindestens eine Zahl a bzw. b gleich Null ist. Dies gilt in $\mathbb{Z}_m$, i.a. nicht.

Definition: Ein Element $a \neq 0$ eines Ringes $<H, +, \circ>$ heißt *Nullteiler in H*, wenn es ein Element $b \in H, b \neq 0$ gibt, mit $a \cdot b = 0$ oder $b \cdot a = 0$

Beispiel: Falls $m = r \cdot s$ mit $r, s \in \mathbb{N},\quad r, s \geq 2$, so besitzt $\mathbb{Z}_m$ stets Nullteiler, denn da $2 \leq r, s < m$ gilt $\bar{r} \cdot \bar{s} = \bar{0}$.
Falls m eine Primzahl ist, so kann es keine Nullteiler geben, denn sei $\bar{r} \cdot \bar{s} = \bar{0} = \{y : y = l \cdot p, l \in \mathbb{Z}\} \qquad \bar{r}, \bar{s} \neq \bar{0}$ und $r \in \bar{r}, s \in \bar{s}$ mit $1 \leq r, s \leq p-1$ (solche Repräsentanten lassen sich in jeder von $\bar{0}$ verschiedenen Restklasse von $\mathbb{Z}_p$ finden). Wegen $r \cdot s = \in \bar{r} \cdot \bar{s}$ ist $r \cdot s$ durch p teilbar. Da p Primzahl ist, müsste r oder s selbst durch p teilbar sein, ein Widerspruch zu $1 \leq r, s \leq p-1$.

Definition: Ein kommutativer Ring mit Einselement, in dem es keine Nullteiler gibt, heißt Integritätsbereich.

Es gilt also: $<\mathbb{Z}_m, + . \cdot>$ ist genau dann ein Integritätsbereich, wenn m eine Primzahl ist.

weitere Beispiele von Integritätsbereichen: $<\mathbb{Q}, +, \cdot>$, $<\mathbb{R}, +, \cdot>$, $<\mathbb{C}, +, \cdot>$, $<\mathbb{Z}, +, \cdot>$

Definition: Ein Ring $<H,+,\circ>$ mit der Eigenschaft, dass $<H-\{0\},\circ>$ eine abelsche Gruppe bildet, heißt Körper. (0 steht für das Nullelement von $<H,+,\circ>$).
$<\mathbb{Q},+,\cdot>$, $<\mathbb{R},+,\cdot>$, $<\mathbb{C},+,\cdot>$

In einem Körper kann es keine Nullteiler geben:
Wäre $a\cdot b=0, b\neq 0$, so existiert b^{-1} und wir erhalten $a=a\cdot b\cdot b^{-1}=0\cdot b^{-1}$, d.h. $a=0$, da in einem beliebigen Ring $<H,+,\circ>$, wegen $0\cdot c=(0+0)\cdot c=0\cdot c+0\cdot c$ also $0\cdot c=0 \quad \forall c\in H$ gilt: => jeder Körper ist Integritätsbereich. Die Umkehrung stimmt i.a. nicht, vgl. $<\mathbb{Z},+,\circ>$ ($<\mathbb{Z}_0=\mathbb{Z}-\{0\},\circ>$ ist keine abelsche Gruppe, inverse Elemente von 2?).

Satz: Jeder endliche Integritätsbereich $<H,+,\circ>$ ist ein Körper.

Beweis: z.z. zu jedem $a\neq 0$ existiert ein multiplikatives Inverses a^{-1} .
Idee: betrachten die Potenz von a. Da H endlich ist, existiert m, n mit $0<m<n$ und
$a^m=a^n \Rightarrow a^m-a^n=0 \quad bzw. \quad a^m\cdot(a^{n-m}-1)=0$

Wegen der Nullteilerfreiheit von H und wegen $a\neq 0$ muss $a^{n-m}=1$. Damit ist a^{m-n-1} invers zu a bezüglich „*“. (beachte $n-m-1\in\mathbb{N}$).

Satz: Der Restklassenring $<\mathbb{Z}_m,+,\circ>$ ist für $m\geq 1$ genau dann ein Körper, wenn m eine Primzahl ist. Beweis: $<\mathbb{Z}_m,+,\circ>$ ist Integritätsbereich und endlich)

Definition: Es sei $<R_{1,}+_{1,}\cdot_1>$ und $<R_{2,}+_{2,}\cdot_2>$ Ringe. Eine Abbildung $\varphi: R_1\rightarrow R_2$ heißt Homomorphismus, wenn

$$\varphi(x+_1 y)=\varphi(x)+_2\varphi(y) \quad \forall x_{1,} x_2\in R_1$$
$$\varphi(x\cdot y)=\varphi(x)\cdot_2\varphi(y)$$

ist φ zusätzlich umkehrbar eindeutig (d.h. bijektiv), so heißt φ Isomorphismus.
Homomorphismen sind also „strukturverträgliche“ Abbildungen (analog definiert man Abbildungen zwischen Halbgruppen, Gruppen usw.)

Definition: Sind $<G,*_1>$ und $<H,*_2>$ Gruppen und $\varphi: G\rightarrow H$ eine Abbildung mit der Eigenschaft $\varphi(a*_1 b)=\varphi(a)*_2\varphi(b) \quad \forall a,b\in G$ so heißt φ (Gruppen-)Homomorphismus.

Beispiel: $<\mathbb{Z},+,\circ>$ und $<\mathbb{Z}_m,+,\circ>$ und die Abbildung $\varphi:\mathbb{Z}\rightarrow\mathbb{Z}_m \varphi(x)=\overline{x}$, wobei $\overline{x}$ die Restklasse modulo m von x ist.

Die Eigenschaften

$$\varphi(x+y)=\overline{x+y}=\overline{x}+\overline{y}=\varphi(x)+\varphi(y)$$
$$\varphi(x\cdot y)=\overline{x\cdot y}=\overline{x}\cdot\overline{y}=\varphi(x)\cdot\varphi(y)$$

ergeben sich unmittelbar aus der Definition der Addition und Multiplikation von Restklassen. φ ist also ein Homomorphismus, aber (für $m\neq 0$) kein Isomorphismus, da φ zwar surjektiv, aber nicht injektiv ist.

Beispiel:

$\varphi:\mathbb{R}\to\mathbb{C}$
$a\to a+0\mathrm{i}$
$a\to(a,0)$
φ ist ein injektiver Homomorphismus.

- $\varphi: <\mathbb{Z},+>\to<m\cdot\mathbb{Z},+>\quad m\in\mathbb{Z}, m\neq 0\qquad z\to m\cdot z$
- φ ist eine Abbildung (ist $z\in\mathbb{Z}$ so ist immer $\varphi(z)\in m\cdot\mathbb{Z}$)
- φ ist ein Homomorphismus: $\varphi(z_1+z_2)=m\cdot(z_1+z_2)=m\cdot z_1+m\cdot z_2=\varphi(z_1)+\varphi(z_2)$
- surjektiv, das Urbild von $m\cdot z$ ist z
- injektiv, ist $z_1\neq z_2\Rightarrow m\cdot Z_1\neq m\cdot z_2$

und somit ein Isomorphismus. $<\mathbb{Z},+>$ und $<mZ,+>$ sind als Gruppen praktisch nicht zu unterscheiden.
$\varphi: <\mathbb{Z},+,\cdot>\to<m\cdot\mathbb{Z},+,\cdot>\quad m\in\mathbb{Z}$
$\quad z\to m\cdot z$

Es gilt $\varphi(z_{1,}z_2)=m\cdot z_1\cdot z_2\neq m\cdot z_1\cdot z_2=\varphi(z_1)\cdot\varphi(z_2)$ kein Ring-Isomorphismus, als Ring haben $\varphi: <\mathbb{Z},+,\cdot>$ und $<m\cdot\mathbb{Z},+,\cdot>$ unterschiedliche Strukturen.

Satz: Seien $<G,*>$ und $<H,*>$ Gruppen. Für einen Homomorphismus $\varphi:G\to H$ gilt immer

a) $\varphi(e)=e$
b) $\varphi(a^{-1})=(\varphi(a))^{-1}$
c) $\forall\ a,b\in G$ gilt $\varphi(a*b^{-1})=\varphi(a)*(\varphi(b))^{-1}$

Beweis:
$\varphi(e)=\varphi(e*e)=\varphi(e)*\varphi(e)$
$\Rightarrow\varphi(\underbrace{e}_{\text{Einheitsele-ment in G}})=\underbrace{e}_{\text{Einheitselement in H}}$

$\varphi(a)*\varphi(a^{-1})=\varphi(a*a^{-1})=\varphi(e)=e\Rightarrow\varphi(a^{-1})=(\varphi(a))^{-1}$
d) $\varphi(a*b^{-1})=\varphi(a)*\varphi(b^{-1})=\varphi(a)*(\varphi(b))^{-1}$

4. Elementare Kombinatorik

Fragestellungen der Kombinatorik:

Die Kombinatorik beschäftigt sich mit Anzahlenberechnung bestimmter Gruppierungen von Elementen wie z.B.

a) Wie viel Fußballspiele finden in der Bundesliga während einer Saison statt?
b) Der Vorstand eines Vereins von 20 Personen besteht aus dem Vorsitzendem, dem Schriftführer und dem Kassenwart. Wie viele Möglichkeiten gibt es, den Vorstand zu besetzen?
c) Wie groß ist die Wahrscheinlichkeit, beim Lotto (6 aus 49) mit zwei Tippreihen 6 Richtige zu erhalten?
d) Ein Informatiker soll 12 Kontakte eines Schaltbrettes mit 12 Drahtenden verbinden. Leider hat hat er den Plan vergessen. Für das Ausprobieren einer Verkabelung aller 12 Drähte braucht er 10 Sekunden. Wie lange muss er arbeiten, wenn er Pech hat und erst die letzte Kombination richtig ist?

Permutation: Unter einer Permutation der Elemente der endlichen Menge A verstehen wir die lineare Anordnung der Elemente von A.

Beispiel: Sei A = { 1, 2, 3 } dann sind die Permutationen von A die Anordnung

1 2 3
3 1 2
2 3 1
1 3 2
3 2 1
2 1 3

Offensichtlich ist die Anzahl der Permutationen nur von $|A|$ abhängig. Ist $|A|=n$, so wird die gesuchte Anzahl der Permutationen mit P_n bezeichnet. Wie man sofort sieht, ist $P_1=1, P_2=2, P_3=6, \ldots$

Wir wollen die *Folge* $<P_n>$ rekursiv festlegen, indem wir angeben, wie P_n für $n\geq 2$ aus P_{n-1} bestimmt werden kann. Betrachtet man die n Plätze der linearen Anordnung, so gibt es n Möglichkeiten für das erste Element $x\in A$, welches Platz 1 bekommt.

$$P_n=n\cdot P_{n-1} \quad \forall n\geq 2$$
$$P_1=1$$

Wir definieren noch $P_0=1 \Rightarrow P_n=\prod_{j=1}^{n} j \quad \forall n\in\mathbb{N}$

Definition: (n-Fakultät)

$$n! := \prod_{j=1}^{n} j \quad \forall n \in \mathbb{N}$$
$$0! := 1$$

also $n! = 1 \cdot 2 \cdot \ldots \cdot n$, damit $P_n = n!$

Beispiel d) Der Informatiker muss 12! = 479.001.600 Möglichkeiten ausprobieren. Jeder Test dauert 10 sec., somit braucht er insgesamt also etwa 151 Jahre.

Aufgabe: Auf wie viele verschiedene Weisen lassen sich die Elemente

$$\underbrace{a_{1,} a_{1,} \ldots a_{1,}}_{k_1} \underbrace{a_{2,} a_{2,} a_2 \ldots}_{k_2}, \underbrace{a_r, a_r \ldots a_r}_{k_r}$$

anordnen?

a_j trete dabei k_j mal auf $(j = 1, \ldots r)$

$\sum_{i=1}^{r} k_j = n$ (die Anzahl aller Elemente)

Wir nummerieren die Elemente mit zusätzlichen oberen Indizes:

$$a_1^{2,} a_1^2 \ldots a_1^{k_1} m, a_2^{k_1+1} \ldots a_2^{k_1+k_2}, a_r^{k_1+k_2+\ldots} \ldots a_r^n$$

Aus ihnen lassen sich genau $n!$ Permutationen bilden. Wir ersetzen nun die Elemente $a_1^1 \ldots a_1^{k_1}$ durch a_1 so werden alle Permutationen von $a_1^1, a_1^2, \ldots a_1^{k_1}$ gleichgestellt => wir müssen $n!$ durch $k_1!$ dividieren.

$$\frac{n!}{k_1! \cdot k_2! \cdot \ldots \cdot k_r!}$$

Beispiel: Auf wie viel verschiedene Weisen lassen sich k Einsen und m Nullen anordnen?

$$\frac{(k+m)!}{k! \cdot m!} = \frac{n!}{k! \cdot m!} = \frac{n!}{k! \cdot (n-k)!} = \binom{n}{k}$$

Definition: Unter einer Variation von n Elementen zur k-ten Klasse ohne Wiederholung verstehen wir ein geordnetes k-Tupel $<a_{1,} a_{2,} \ldots, a_k>$ von k paarweise verschiedenen Elementen a_i der Menge A mit n Elementen (d.h. $a_i \neq a_j$ für $i \neq j$). Die Anzahl aller derartigen Variationen bezeichnen wir mit V_n^k .

Beispiel:
$n=4, \quad A=\{a_{1,} a_{2,} a_{3,} a_4\}$
$k=2,$
$<a_{1,} a_2> \quad <a_{2,} a_1> \quad <a_{3,} a_1> \quad <a_{4,} a_1>$
$<a_{1,} a_3> \quad <a_{2,} a_3> \quad <a_{3,} a_2> \quad <a_{4,} a_2>$
$<a_{1,} a_4> \quad <a_{2,} a_4> \quad <a_{3,} a_4> \quad <a_{4,} a_3>$
$V_4^2=4 \cdot 3=12$

Bestimmung von V_n^k : Wir gehen aus von allen $n!$ Permutationen $<a_{1,} a_{2,} \ldots, a_n>$ der Menge A und nennen zwei solche Permutationen äquivalent, wenn die aus den ersten k gebildeten Variationen übereinstimen, d.h. wenn $a_i=b_i \quad \forall 1 \leq 1 \leq k$. Man sieht leicht, dass auf diese Weise eine Äquivalenzrelation definiert ist.

$<a_{1,} a_{2,} a_{3,} a_4> R <a_{1,} a_{2,} a_{3,} a_4>$

Klasseneinteilung:
$K(x)=\{y : yRx\}$
$K(<a_{1,} a_{2,} a_{3,} a_4>)=\{ <a_{1,} a_{2,} a_{3,} a_4> , <a_{1,} a_{2,} a_{4,} a_3> \}$

Dabei sind alle zugehörigen Äquivalenzklassen gleich groß.
Für die n-Tupel $<a_{1,} \ldots, a_n>$ einer Klasse ist $<a_{1,} \ldots, a_n>$ fixiert, während die Elemente $<a_{k+1}, a_{k+2}, \ldots, a_n>$ eine beliebige Permutation der verbleibenden $n-k$ Elemente der Menge A darstellen. Jede Äquivalenzklasse besteht aus $P_{n-k}=(n-k)!$ Elementen. Die Anzahl der Äquivalenzklassen, d.h. die gesuchte Anzahl der Variationen zur k-ten Klasse, ergibt sich

$$V_n^k=\frac{Anzahl\,aller\,Permutationen}{Größe\,einer\,Äquivalenzklasse}=n\frac{!}{(n-k)!}=n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot (n-k+1)$$

2. Weg: Analog der Überlegung zur Berechnung der Permutation

- für die erste Position eines k-Tupels der beschriebenen Art haben wir n Möglichkeiten der Besetzung, denn alle $a_{1,} \ldots, a_n$ kommen in Frage

$$\Rightarrow V_n^k=n \cdot V_{n-1}^{k-1} \;\Rightarrow\; V_n^k=n \cdot (n-1) \cdot \ldots (n-k+1)=n \cdot (n-1) \cdot V_{n-k}^0$$

Beispiel aus Frage b) Vorsitzender, Schriftwart und Kassierer bilden ein Tripel. Die Anzahl der Tripel dieser Art ist also bei einer Vereinsstärke von 20 Personen gleich

$20 \cdot 19 \cdot 18 = 6840$

Frage a) 18 Fußballvereine $\Rightarrow V_{18}^{2} = 18 \cdot 17 = 306$

Definition: Unter einer Variation von n Elementen zur k-ten Klasse mit Wiederholung verstehen wir ein geordnetes k-Tupel $< a_{1,} a_{2,} \ldots, a_k >$ von k nicht notwendig verschiedenen Elementen a_i der Menge A mit n Elementen. Die Anzahl aller derartigen Variationen bezeichnen wir mit ${}^{W}V_n^k$.

Es gilt ${}^{W}V_n^k = n^k$, da jedes Element a_i des k-Tupels $< a_{1,} a_{2,} \ldots, a_k >$ ein beliebiges Element der n-elementigen Menge A.

Beispiel: $a_1 \; a_2 \; a_3$

$n=3, k=2$
$a_1 a_1 \;\; a_2 a_1 \;\; a_3 a_1$
$a_1 a_2 \;\; a_2 a_2 \;\; a_3 a_3$
$a_1 a_3 \;\; a_2 a_3 \;\; a_3 a_3$

Beispiel: Wie viele Tupel lassen sich aus den Ziffern 0, 1, 2, ...9 bilden?

Antwort: $10^3 = 1000$, nämlich genau die Zahlen $0, \ldots, 999$

Definition: Unter einer Kombination von n Elementen zur k-ten Klasse ohne Wiederholung verstehen wir ein ungeordnetes k-Tupel $\{a_{1,} a_{2,} \ldots a_k\}$ von k paarweise verschiedenen Elementen a_i der Menge A mit n Elementen, d.h. eine k-elementige Teilmenge. Die Anzahl bezeichnen wir mit C_n^k . Die Elemente von A schreiben wir uns in der durchnummerierten Reihenfolge hin $a_{1,} a_{2,} a_{3,} \ldots, a_n$ und markieren die Elemente a_i , die zu einer bestimmten Teilmenge gehören durch eine darunter geschriebene 1 und alle anderen Elemente durch 0, z.B.

a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
0	1	1	0	1	0	1	1

für $n=8, k=5$. Unsere Teilmenge besteht hier aus den Elementen $a_{2,} a_{3,} a_{5,} a_{7,} a_8$. Auf diese Weise entspricht jede Teilmenge von M genau einem n-Tupel mit k Einsen und m=n-k Nullen.

Nach dem Beispiel (siehe Permutationen) gibt es aber genau $\binom{n}{k}$ solcher n-Tupel, also gibt es auch ebenso viele k-elementige Teilmengen von M

$$C_n^k = \binom{n}{k} = \frac{n!}{k! \cdot (n-k)!}$$

Beispiel c) 6 aus 49

$$\binom{49}{6} = \frac{49 \cdot 48 \cdot 47 \cdot 46 \cdot 45 \cdot 44}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6} = 13.983.816$$

Definition: Unter einer Kombination von n Elementen zur k-ten Klasse mit Wiederholung verstehen wir ein ungeordnetes k-Tupel $\{a_{1,} a_{2,} \ldots a_k\}$ von k nicht notwendig verschiedenen Elementen a_i der Menge A mit n Elementen, d.h. eine k-elementige Teilmenge. Die Anzahl aller derartigen Kombinationen bezeichnen wir mit ${}^W C_n^k$.

Beispiel: $n=5, k=7$
Ein 7-Tupel aus $a_{1,} a_{2,} a_{3,} a_{4,} a_5$ ist z.B. durch $(a_{1,} a_{1,} a_{1,} a_{3,} a_{4,} a_{5,} a_5)$ gegeben. Wir denken uns 5 Kästen von 1 bis 5 durchnummeriert. Die drei Elemente a_1 sollen bedeuten, dass m Kasten 1 drei Kugeln liegen, a_3 bedeutet, dass im Kasten 3 eine Kugel liegt.

ooo		o	o	oo
1	2	3	4	5

Aus diesem Bild lassen wir alles weg, mit Ausnahme der Kugeln und der Zwischenwände.

000 | | 0 | 0 | 00

Dies schaut nach einer Reihenfolge von 7 Nullen und 4 Einsen aus. Davon gib es genau $\binom{7+4}{7}$ Möglichkeiten. Allgemein wegen $k=7, n=5$ ${}^W C_n^k = \binom{k+n-1}{k}$.

Anwendung: Seien x, y Elemente eines kommutativen Rings. Dann ergeben sich beim „Ausmultiplizieren“ des Ausdrucks

$(x+y)^n = (x+y) \cdot (x+y) \cdot \ldots \cdot (x+y) \quad n \in \mathbb{N}$
nach dem Distributivgesetz Summen von Produkten von n-Tipeln von x und y.

z.B.
$n=2 \quad (x+y)\cdot(x+y)=x\cdot x+y\cdot x+x\cdot y+y\cdot y$
$n=3 \quad (x+y)\cdot(x+y)\cdot(x+y)=x\cdot x\cdot x+x\cdot y\cdot x+x\cdot x\cdot y+x\cdot y\cdot y+y\cdot x\cdot x+y\cdot x\cdot y+y\cdot y\cdot y$

Da der Ring kommutativ sein soll, ergeben alle n-Tupel, die k-mal x und $(n-k)$ mal y enthalten, den selben Wert $x^k\cdot y^{n-k}$. Diese Situation tritt $C_n^k=\binom{n}{k}$ mal auf (beachte x: n-Elemente zur k-ten Klasse).

Satz: Seien x, y Elemente eines kommutativen Rings. Dann ist für alle $n\in\mathbb{N}$
$(x+y)^n=\sum_{k=0}^{n}\binom{n}{k}\cdot x^k\cdot y^{n-k}$
Dabei ist $x^0\cdot y^k=y^n$ und $x^n\cdot y^0=x^n$ zu setzen.

Permutationen

Sei $V=\{V_{1,}V_{2,}\dots,V_n\}$ und die Permutation π die Anordnung $w_{1,}w_{2,}\dots w_n$ der Elemente von V.

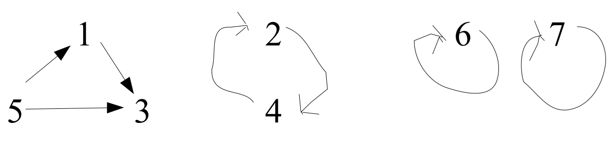
$\Rightarrow \pi: V\rightarrow V \quad bijektiv$
$\pi(V_k)=w_R \quad (k=1\dots\text{n})$

Darstellungsarten:

zweistellige Darstellungen: $\pi=\begin{pmatrix} v_1 & v_2\dots v_n \\ w_1 & w_2\dots w_n\end{pmatrix}$

Beispiel:
$V=\{1,2,3,4,5,6,7\}$
$\pi=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 5 & 2 & 1 & 6 & 7\end{pmatrix}$

Darstellung als Graph



Zyklendarstellung: beginnend mit einem Element v, bildet man die Kette
$V_i, \pi(V_i), \pi(\pi(V_i))$

Da V endlich ist und π injektiv ist, muss nach endlichen Schritten, sagen wir k, wieder V_i erreicht werden. Dieser Zyklus der Länge k wird dann in der Form

$(V_i, \pi(V_i), \pi^2(V_i), \ldots \pi^{k-1}(V_i))$ geschrieben.

Enthält dieser Zyklus noch nicht alle Elemente von V, so beginnt man mit dem nächsten Zyklus mit einem Element V_j der noch nicht im 1. Zyklus enthalten ist.
Jede Permutation kann durch paarweise elementfremde Zyklen dargestellt werden.

Beispiel: $\pi = (1,3,5)(2,4)(6)(7)$

Definition: Seien π, ζ zwei Permutationen der Menge V. Dann ist das Produkt $\delta = \pi \circ \zeta$ die Permutation, die durch die Hintereinanderausführung der Abbildungen π, ζ durch $\delta(V_j) = \pi(\zeta(V_j)) \quad \forall V_j \in V$ definiert ist.

Beachte: i.a. $\pi \circ \zeta \neq \zeta \circ \pi$

Beispiel: $\pi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \qquad \zeta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

$\pi \circ \zeta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \qquad \pi \circ \zeta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

Satz: Sei $S(V)$ die Menge aller Permutationen der Menge V und $\circ$ das Produkt von Permutationen, dann ist $<S(V), \circ>$ eine Gruppe.

Beweis:
- Produkt von Elementen von $S(V)$ ist wieder in $S(V)$
- $\circ$ ist assoziativ
- $S(V)$ besitzt als Einheitselement die „identische" Permutation $id(V_i) = V_i \quad \forall V_i \in V$
- Das inverse Element zu π mit $\pi(v_i) = w_i \quad \forall v_i \in V$ ist die Umkehrabbildung π^{-1} mit $\pi^{-1}(w_i) = v_i \quad \forall w_i \in V$.

Definition: Sei $|V| = n$. Dann heißt $<S(V), \circ>$ symmetrische Gruppe der Ordnung n.

Definition: Sei π eine Permutation der linear geordneten Menge V $V = \{v_1 < v_2 < v_3 < \ldots < v_n\}$. Ein Paar (v_i, v_j) mit $v_i < v_j$, aber $\pi(v_i) > \pi(v_j)$ heißt *Inversion* von π. π heißt gerade, wenn die Anzahl der Inversionen von π gerade ist, symbolisch $sgn(\pi) = 1$. π heißt ungerade, wenn die Anzahl der Inversionen von π ungerade ist, symbolisch $sgn(\pi) = -1$. $sgn(\pi)$ heißt „Vorzeichen" der Permutation.

Beispiel:
$V = \{1,2,3,4,5,6,7\}$

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

→ besitzt 4 Inversionen → $sgn(\pi) = 1$

5. Lineare Algebra

Lineare Algebra ist die Theorie der linearen Räume.

5.1 Vektorräume

Beispiel: Sei $V=\mathbb{R}^3$ die Menge aller Tripel $\vec{a}=\begin{pmatrix}a_1\\a_2\\a_3\end{pmatrix}$ von reellen Zahlen. Jedes Element aus V kann nach Wahl eines kartesischen Koordinatensystems umkehrbar eindeutig einem Punkt des 3-dimensionalen Anschauungsraums zugeordnet werden. Auf V wird eine Addition durch „+“ definiert.

$$\begin{pmatrix}a_1\\a_2\\a_3\end{pmatrix}+\begin{pmatrix}b_1\\b_2\\b_3\end{pmatrix}=\begin{pmatrix}a_1+b_1\\a_2+b_2\\a_3+b_3\end{pmatrix}$$

→ $<V,+>$ ist eine Abelsche Gruppe

Auf V kann für jedes $\lambda\in\mathbb{R}$ ein Produkt „ $\cdot$ “.

$$\lambda\cdot\begin{pmatrix}a_1\\a_2\\a_3\end{pmatrix}=\begin{pmatrix}\lambda\cdot a_1\\\lambda\cdot a_2\\\lambda\cdot a_3\end{pmatrix}$$

→ $<V,+,\cdot>$ ist ein Körper

Man sieht leicht: Für $\vec{a},\vec{b}\in\mathbb{R}^3$ $\lambda,\mu\in\mathbb{R}$

1. $\lambda\cdot(\vec{a}+\vec{b})=\lambda\cdot\vec{a}+\lambda\cdot\vec{b}$
2. $(\lambda+\mu)\cdot\vec{a}=\lambda\cdot\vec{a}$
3. $\lambda\cdot(\mu\cdot\vec{a})=(\lambda\cdot\mu)\cdot\vec{a}$
4. $1\cdot\vec{a}=\vec{a}$

Beispiel B: Sei K ein möglicherweise auch endlicher Körper und K^n die Menge der n-Tupel.

$\begin{pmatrix} x_1 \\ \dots \\ x_n \end{pmatrix}$ von Elementen aus K. Definiert man $\begin{pmatrix} a_1 \\ \dots \\ a_n \end{pmatrix} + \begin{pmatrix} b_1 \\ \dots \\ b_n \end{pmatrix} = \begin{pmatrix} a_1+b_1 \\ \dots \\ a_n+b_n \end{pmatrix}$

bzw. für $\lambda \in K$

$$\lambda \cdot \begin{pmatrix} a_1 \\ \dots \\ a_n \end{pmatrix} = \begin{pmatrix} \lambda \cdot a_1 \\ \dots \\ \lambda \cdot a_n \end{pmatrix}$$

so ist wieder $< K^n, + >$ eine abelsche Gruppe und das Produkt hat die Eigenschaften 1-4.

Beispiel C: Sei V die Menge aller Funktionen $f : [0,1] \to \mathbb{R}$. $f + g \in V$ sei die Funktion h definiert durch

$h(x) = f(x) + g(x) \quad \forall x \in [0,1]$
$\Rightarrow < V, + >$ ist eine abelsche Gruppe.

Für $\lambda \in \mathbb{R}$ definieren wir $h = \lambda \cdot f \Leftrightarrow h(x) = \lambda \cdot f(x) \quad \forall x \in [0,1]$.
$\Rightarrow$ Eigenschaft 1-4 sind erfüllt.

Definition: Sei K ein Körper. Dann heißt $< V, +, K >$ linearer Vektorraum über K, wenn

a) $< V, + >$ eine abelsche Gruppe bildet
b) für jedes $a \in V$ ein Produkt $\lambda \cdot a \in V$ definiert ist, so dass $\forall \lambda, \mu \in K$ und $a, b \in V$ gilt
   1. $\lambda \cdot (a+b) = \lambda \cdot a + \lambda \cdot b$
   2. $(\lambda + \mu) \cdot a = \lambda \cdot a + \mu \cdot a$
   3. $\lambda \cdot (\mu \cdot a) = (\lambda \cdot \mu) \cdot a$
   4. $1 \cdot a = a$

Im Folgenden bezeichnen wir mit $-a$ das inverse Element zu a in der Gruppe $< V, + >$ und mit $-\lambda$ das inverse Element zu λ in $< K, + >$.

Satz: Für $a \in V$ und $\lambda \in K$ gilt

i) $0 \cdot a = 0$
ii) $\lambda \cdot 0 = 0$
iii) $(-\lambda) \cdot a = \lambda \cdot (-a)$
iv) $\lambda \cdot a = 0 \Leftrightarrow \lambda = 0 \vee a = 0$

Beweis:

i) $0 \cdot a = (0+0) \cdot a = 0 \cdot a + 0 \cdot a$
$0 = 0 \cdot a$

ii) $\lambda \cdot 0 = \lambda \cdot (0+0) = \lambda \cdot 0 + \lambda \cdot 0 \quad \vert -(\lambda \cdot 0)$
$0 = \lambda \cdot 0$

iii) Da $a - a = 0$ ist $\lambda \cdot a + \lambda \cdot (-a) = 0$, also
$(-\lambda) \cdot a = -\lambda \cdot a + 0 = -\lambda \cdot a + \lambda \cdot a + \lambda \cdot (-a) = (-\lambda + \lambda) \cdot a + \lambda \cdot (-a) = \lambda \cdot (-a)$

iv) Wegen i) und ii) folgt aus $\lambda = 0 \vee a = 0$ sofort $\lambda \cdot a = 0$ => da K ein Körper ist $\exists\ zu\ \lambda \neq 0$ ein $\lambda^{-1} \in K$ mit $\lambda^{-1} \cdot \lambda = 1 \Rightarrow a = (\lambda^{-1} \cdot \lambda) \cdot a = \lambda^{-1} \cdot 0 = 0$. Falls $\lambda = 0$ ist die Behauptung gezeigt.

Definition: Sei $<V, +, K>$ ein Vektorraum. Ist $U \subseteq V$, so heißt $<U, +, K>$ (linearer) Teilraum oder Unterraum von $<V, +, K>$, wenn $<U, +, K>$ selbst ein Vektorraum ist.

Satz: Sei $<V, +, K>$ ein Vektorraum. Eine nicht leere Teilmenge $U \subseteq V$ ist genau dann ein Teilraum $<U, +, K>$ m wenn Folgendes gilt:

1) $a - b \in U \quad \forall a, b \in U$
2) $\lambda \cdot a \in U \quad \forall \lambda \in K, a \in U$

Beweis: U ist Teilraum von V genau dann, wenn $<U, +>$ Untergruppe von $<V, +>$ ist und Eigenschaft 2 aus dem Satz gilt. Alle weiteren Eigenschaft sind dann sofort erfüllt, da $<V, +, K>$ ein Vektorraum ist. Wir wissen, dass $<U, +>$ genau dann Untergruppe von $<V, +>$ ist, wenn $a + (-b) = a - b \in U \quad \forall a, b \in U$ (siehe Satz S über Untergruppen).

Folgerung: Eine nicht leere Teilmenge $U \subseteq V$ ist genau dann Teilraum von $<V, +, K>$, wenn $a + \mu \cdot b \in U \quad \forall a, b \in U, \mu \in K$ gilt.

Beweis: Ist U ein Teilraum von V, so ist natürlich auch die Bedingung (s.o.) erfüllt. Umgekehrt folgt aus der Bedingung die Eigenschaft 1) und 2) aus dem Satz:

1) setze $\mu = -1$ („-“=inverse bezüglich Addition, „1“=Einselement aus K), so ist wegen $(-1) \cdot b = b \quad a - b \in U$
2) setze $a = 0 \in V$ so folgt $\mu \cdot b \in U \quad \forall \mu \in K, b \in U$

Beispiele: Die Lösungen $x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \in \mathbb{R}^3$ eines homogenen linearen Gleichungssystems.

$$a_{11} \cdot x_1 + a_{12} \cdot x_2 + a_{13} \cdot x3 = 0$$
$$a_{21} \cdot x_1 + a_{22} \cdot x_2 + a_{23} \cdot x3 = 0$$
$$a_{31} \cdot x_1 + a_{32} \cdot x_2 + a_{33} \cdot x3 = 0$$

mit $(a_{ij} \in \mathbb{R})$, bilden einen Teilraum des Vektorraums $<\mathbb{R}^3, +, \mathbb{R}>$ (kurz $\mathbb{R}^3$). Da sicher $\vec{0} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$ eine Lösung ist, ist U nicht leer. Sind $\vec{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$ und $\vec{y} = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}$ Lösungen, so sieht man sofort, dass auch $\vec{x} + \mu \cdot \vec{y}$ eine Lösung ist ($\mu \in \mathbb{R}$).

(erste Zeile nachrechnen:

$$a_{11} \cdot (x_1 + \mu \cdot y_1) + a_{12} \cdot (x_2 + \mu \cdot y_2) + a_{13} \cdot (x_3 + \mu \cdot y_3)$$
$$= a_{11} \cdot x_1 + a_{12} \cdot x_2 + a_{13} \cdot x_3 + \mu (a_{11} \cdot x_1 + a_{12} \cdot x_2 + a_{13} \cdot x_3)$$
$$= 0 + \mu \cdot 0 = 0$$

2) Jede Gerade und jede Ebene durch den Ursprung $\vec{0} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$ bildet einen Teilraum des $\mathbb{R}^3$. Geraden bzw. Ebenen die den Ursprung nicht enthalten (sind keine Teilräume) lassen sich jedoch stets aus Geraden bzw. Ebenen, die durch den Ursprung gehen, durch Translation um einen festen Vektor $\vec{x}_0$ erzeugen.

So ist die Menge

$$g = \{\vec{x} \in \mathbb{R}^3 : \vec{x} = \vec{x}_0 + \lambda \vec{v}, \lambda \in \mathbb{R}, \vec{x}_0, \vec{v} \in \mathbb{R}^3\}$$

die Gerade in Richtung des Vektors $\vec{v}$ durch den Endpunkt des Vektors $\vec{x}_0$.

Die Menge $E = \{\vec{x} \in \mathbb{R}^3 : \vec{x} = \vec{x}_0 + \lambda \cdot \vec{v} + \mu \cdot \vec{w}; \lambda, \mu \in \mathbb{R}, \vec{x}_0, \vec{v}, \vec{w} \in \mathbb{R}^3\}$ stellt die Ebene dar, die durch $\vec{x}_0$ geht und von $\vec{v}$ und $\vec{w}$ aufgespannt wird.

Definition: Seien S, T Teilmengen eines Vektorraums, dann ist die Summe S+T durch
$S + T = \{x : x \, besitzt \, die \, Darstellung \, x = s + t, s \in S, t \in T\}$

Definition: Sei V ein Vektorraum, $x_0 \in V$, U Teilraum von V, dann heißt die Menge $x_0 + V$ affiner Teilraum von V.

Beispiel:

1) Kennen alle Teilräume von $\mathbb{R}^3$: $\{0\}$, Geraden durch 0, Ebenen durch 0, $\mathbb{R}^3$

Damit kennen wir auch die affinen Teilräume des $\mathbb{R}^3$.

2) Betrachten ein lineares Gleichungssystem in $\mathbb{R}^3$ (3 Gleichungen, 3 Unbekannte)

$$\begin{aligned} a_{11}\cdot x_1+a_{12}\cdot xc_2+a_{13}\cdot x_3&=b_1 \\ a_{21}\cdot x_1+a_{22}\cdot xc_2+a_{33}\cdot x_3&=b_2 \qquad (a_{ij}\in\mathbb{R}, b_i\in\mathbb{R}, i,j\in\{1,2,3\}) \qquad (*) \\ a_{31}\cdot x_1+a_{32}\cdot xc_2+a_{33}\cdot x_3&=b_3 \end{aligned}$$

Wissen bereits: Wenn $b_1=b_2=b_3=0$ gilt, dann heißt (*) homogenes Gleichungssystem. Seine Lösungsmenge ist ein Teilraum von $\mathbb{R}^3$. Sei nun $(b_{1,}b_{2,}b_3)\neq(0,0,0)$ (inhomogenes Gleichungssystem) und (*) sei lösbar. Wenn $x=(x_{1,}x_{2,}x_3), x'=(x_1', x_2', x_3')$ zwei Lösungen von (*) sind, dann ist die Differenz $x-x'=(x_1-x_1', x_2-x_2', x_3-x_3')$ eine Lösung des entsprechenden homogenen Systems.

Betrachten 1. Gleichung:

$$\begin{aligned} &a_{11}\cdot(x_1+x_1')+a_{12}\cdot(x_2+x_2')+a_{13}\cdot(x_3-x_3')= \\ &a_{11}\cdot x_1+a_{12}\cdot x_2+a_{13}\cdot x_3-(a_{11}\cdot x_1'+a_{12}\cdot x_2'+a_{13}\cdot x_3')=b_1-b_1=0 \end{aligned}$$

Somit gilt: Besitzt das inhomogene System (*) eine Lösung x_0, so hat jede Lösung x von (*) eine Lösung x_0 die Gestalt $x=x_0+u$ mit $u\in U$ (U Lösungsmenge des homogenen Systems).

Mit anderen Worten: Falls (*) lösbar ist, dann bildet die Lösungsmenge von (*) einen affinen Teilraum in $\mathbb{R}^3$ (nämlich x_0+U).

Satz: Seien $U_{1,}U_2$ Teilräume eines Vektorraums V, dann gilt

a) $U_1\cap U_2$ ist Teilraum von V
b) $U_1\cup U_2$ ist ein Teilraum von V genau dann, wenn $U_1\subseteq U_2$ oder $U_2\subseteq U_1$
c) U_1+U_2 ist Teilraum von V

Beweis:

1) Seien $A,B\in U_1\cap U_2$, d.h. $a,b\in U_1$ und $a,b\in U_2$. Da $U_{1,}U_2$ Teilräume sind, gilt $a+\mu\cdot b\in U_{11}$ und $a+\mu\cdot b\in U_2 \quad \forall\,\mu\in K$. Somit gilt $a+\mu\cdot b\in U_1\cap U_2 \quad \forall\,\mu\in K$
2) $\Leftarrow$: Wenn $U_1\subseteq U_2$ gilt, dann ist $U_1\cup U_2=U_2$ also Teilraum. Wenn $U_2\subseteq U_1$ gilt, dann ist $U_1\cup U_2=U_1$, also Teilraum $\Rightarrow$: Sei nun $U_1\cup U_2$ Teilraum, aber es gelte weder $U_1\subseteq U_2$ noch $U_2\subseteq U_1$. Dann gibt es Vektoren $a\in U_1$ mit $a\notin U_2$ und $b\in U_2$ und $b\notin U_1$. Betrachten $c=a+b\in U_1\cup U_2$, d.h. $c\in U_1$ oder $c\in U_2$.
Wäre $c\in U_1$, dann wäre auch $c+(-a)=b\in U_1$ → Widerspruch zu $b\notin U_1$
Wäre $c\in U_2$, dann wäre auch $c+(-b)=a\in U_2$ → Widerspruch zu $a\notin U_2$

3) Seien $a,b \in U_1+U_2$ beliebig, d.h. $a=a_1+a_2, b=b_1+b_2$ mit $a_1, b_1 \in U_1, a_2, b_2 \in U_2$.
   Betrachten $a+\mu\cdot b=a_1+a_2+\mu\cdot b_1+\mu\cdot b_2=\underbrace{a_1+\mu\cdot b_1}_{\in U_1}+\underbrace{a_2+\mu\cdot b_2}_{\in U_2} \quad \forall \mu\in K$

Bemerkung: Für 2 Teiräume U_1, U_2 aus V gelten folgende Inklusionen
$\{0\}\subseteq U_1\cup U_2 \begin{matrix}\subseteq U_1 \subseteq \\ \subseteq U_2 \subseteq\end{matrix} U_1+U_2\subseteq V$

Def.: Sei $<V,+,K>$ ein Vektorraum, $S\subseteq V$ eine nichtleere Teilmenge. Die Menge $L(S)=\{x\in V: x=\sum_{i=1}^{n}\lambda_i\cdot a_i \;\; mit \;\; a_i\in S, \lambda_i\in K, n\in\mathbb{N}\}$ aller endlichen Linearkombinationen von Vektoren aus S heißt *lineare Hülle von S* in V.

Wenn , dann $L\{\emptyset\}=\{0\}$ $S=\emptyset$. Offenbar gilt $S\subseteq L(S)$.

Satz: Sei S beliebige Teilmenge von V. Die lineare Hülle $L(S)$ ist ein Teilraum von V.

Beweis: Für $S=\emptyset$ gilt $L(S)=\{0\}$, dies ist ein Teilraum von V. Sei nun $S\neq\emptyset$ und
$a_1, a_2 \ldots a_m, \;\; b_1, b_2, \ldots, b_n \in S, \;\; a=\sum_{i=1}^{m}\lambda_i\cdot a_i\in L(S), \;\; b=\sum_{i=1}^{n}\mu_i\cdot b_i\in L(S) (\lambda_i, \mu_i\in K)$

Betrachten wir für $\mu\in K$ beliebig: $a+\mu\cdot b=\sum_{i=1}^{m}\lambda_i\cdot a_i+\sum_{i=1}^{n}\mu\cdot\mu_i\cdot b_i$ → endliche Linearkombination von $a_1,\ldots,a_m, b_1,\ldots,b_n\in S$.

Beispiel: $V=\mathbb{R}^3$

$$S=S_1=\left\{\begin{pmatrix}1\\0\\0\end{pmatrix},\begin{pmatrix}0\\1\\0\end{pmatrix}\right\}\Rightarrow L(S)=\left\{\begin{pmatrix}x_1\\x_2\\0\end{pmatrix} mit\, x_1, x_2\in\mathbb{R}\right\}=\left\{\begin{pmatrix}x_1\\x_2\\x_3\end{pmatrix}\in\mathbb{R}^3 mit\, x_3=0\right\}$$

$$S=S_2=\left\{\begin{pmatrix}1\\0\\0\end{pmatrix},\begin{pmatrix}1\\1\\0\end{pmatrix}\right\}=---''---$$

$$S=S_3=\left\{\begin{pmatrix}1\\0\\0\end{pmatrix},\begin{pmatrix}1\\1\\0\end{pmatrix},\begin{pmatrix}0\\1\\0\end{pmatrix}\right\}=---''---$$

Satz:
1) Ist S Teilraum von V, dann gilt $L(S)=S.$
2) Für jede Teilmenge S von V gilt: $L(L(S))=L(S)$
3) $L(S)$ ist der kleinste Teilraum von V, der S enthält, d.h. ist $S\subseteq U$ und U Teilraum, so

gilt $L(S)\subseteq U$.

Beweis:

1) Ist S Teilraum von V, dann enthält S auch alle endlichen Linearkombinationen von Elementen aus S, d.h. $L(S)=S$
2) Da $L(S)$ Teilraum ist, folgt diese Behauptung aus 1)
3) Wir wissen, dass $L(S)$ Teilraum ist, der S enthält, $S\subseteq L(S)$. Sei nun U Teilraum mit $S\subseteq U$. Dann gilt $L(S)\subseteq L(U)=U$

Satz: Seien $U_{1,}U_2$ Teilräume von V. Dann besitzt jeder Vektor x des Teilraumes U_1+U_2 eine Darstellung $x=x_1+x_2$ mit eindeutig bestimmten Vektoren $x_1\in U_1$ und $x_2\in U_2$, wenn $U_1\cup U_2=\{0\}$.

Beweis: $\Rightarrow$: Sei $x\in U_1+U_2$ beliebig und die Darstellung $x=x_1+x_2$ mit $x_1\in U_{1,}x_2\in U_2$ eindeutig, aber $U_1\cap U_2>\{0\}$, d.h. $\exists y(\neq 0)\in U_1\cap U_2$. Dann gilt $x=x_1+y+x_2-y$, was der Eindeutigkeit der Darstellung widerspricht.

$\Leftarrow$: Sei nun $U_1\cap U_2=\{0\}$. Wir nehmen an, wir haben 2 Darstellungen
$x=x_1+x_2=x_1'+x_2' \quad x_{1,}x_1'\in U_1 \quad x_{2,}x_2'\in U_2$. Dann gilt
$\begin{matrix} x_1-x_1'+x_2=x_2' \\ U_1\in x_1-x_1'=x_2'-x_2\in U_2 \end{matrix}$, d.h. $x_1-x_1'=x_2'-x_2\in U_1\cap U_2=\{0\}$

$x_1-x_1'=0 \quad x_2'-x_2=0 \quad x_1=x_1'$ und $x_2=x_2'$, d.h. die Darstellung ist eindeutig.

Definition: Sind $U_{1,}U_2$ Teilräume von V mit $U_1\cap U_2=\{0\}$, so heißt der Teilraum U_1+U_2 die direkte Summe, symbolisch $U_1\oplus U_2$. Ist $U_1\oplus U_2=V$ so heißt U_2 Komplementärraum zu U_1 in V.

Beispiel: Sei $V=R^{1,}U_1=\left\{\begin{pmatrix}\lambda\\0\end{pmatrix}:\lambda\in K\right\}$. Dann ist $U_2=\left\{\begin{pmatrix}0\\\lambda\end{pmatrix}:\lambda\in K\right\}$ ein Komplementärraum.

Dies gilt auch für $U_2=\left\{\begin{pmatrix}\lambda\\\lambda\end{pmatrix}:\lambda\in K\right\}$. $\forall\vec{x}\in\begin{pmatrix}x_1\\x_2\end{pmatrix}\in V$ gilt $\begin{pmatrix}x_1\\x_2\end{pmatrix}=\begin{pmatrix}x_1-x_2\\0\end{pmatrix}+\begin{pmatrix}x_2\\x_2\end{pmatrix}$, d.h.

$U_1+U_2'=V$. Da $U_1\cap U_2'=\left\{\begin{pmatrix}0\\0\end{pmatrix}\right\}$. ist $U_1\oplus U_2'=V$ und wegen $\begin{pmatrix}1\\1\end{pmatrix}\in U_2',\begin{pmatrix}1\\1\end{pmatrix}\notin U_2$ ist $U_2\neq U_2'$, d.h. Komplementärrume sind i.a. nicht eindeutig bestimmt.

5.2 Lineare Unabhängigkeit, Basis, Dimension

Lemma: Seien $x_{1,}\dots,x_p$ Vektoren des Vektorraums V. Dann sind die folgenden Aussagen äquivalent.

1) Die Darstellung eines beliebigen Vektors $x \in L(x_{1,}\dots,x_p)$ in der Form $x=\sum_{i=1}^{p}\lambda_i\cdot x_i \quad \lambda_i\in K$ ist eindeutig.
2) Der Nullvektor besitzt nur die triviale Darstellung, d.h. $\sum_{i=0}^{p}\lambda_i\cdot x_i=0\Rightarrow\lambda_i=0 \quad \forall i=1,\dots,p$

Beweis:

1) => 2) Der Nullvektor besitzt die eindeutige Darstellung $0=\sum_{i=0}^{p}0\cdot x_i$
2) => 1) Angenommen es gäbe 2 verschiedene Darstellungen $x=\sum_{i=1}^{p}\lambda_i\cdot x_i=\sum_{i=1}^{p}\mu_i\cdot x_i$ des Vektors x
$\Rightarrow x-x=0=\sum_{i=1}^{p}(\lambda_i-\mu_i)\cdot x_i$
Da die Darstellungen verschieden sind, existiert ein i_0 mit $\lambda_{i_0}\neq\mu_{i_0}$. Dann ist aber die Darstellung (*) eine nichttriviale Darstellung des Nullvektors → Widerspruch zu 2)

Definition: Seien $x_{1,}\dots,x_p$ Vektoren des Vektorraums V über K.

- Die Vektoren $x_{1,}\dots,x_p$ heißen linear abhängig, wenn es eine nichttriviale Darstellung des Nullvektors 0 als Linearkombination von $x_{1,}\dots,x_p$ gibt, d.h. wenn es ein p-Tupel $(\lambda_{1,}\dots,\lambda_p)\neq(0,\dots,0)$ von $\lambda_i\in K(i=1,\dots,p)$ gibt, so dass $\sum_{i=1}^{p}\lambda_i\cdot x_i\neq 0$.
- Die Vektoren $x_{1,}\dots,x_p$ heißen lineaer unabhängig, wenn der Nullvektor nur die triviale Darstellung als Linearkombination von $x_{1,}\dots,x_p$ besitzt: $\sum_{i=1}^{p}\lambda_i\cdot x_i=0\Rightarrow\lambda_i=0 \quad i=1,\dots,p$, d.h. wenn $x_{1,}\dots,x_p$ nicht linear abhängig ist.

Folgerung aus obigem Lemma:

$x\in L(x_{1,}\dots,x_p)$ hat genau dann eine eindeutige Darstellung $x=\sum_{i=1}^{p}\lambda_i\cdot x_i$, wenn $x_{1,}\dots,x_p$ linear unabhängig.

Bemerkung: Der Nullvektor ist in jedem Vektorraum linear abhängig, denn der Körper K muss mindestens die beiden Elemente 0 und 1 enthalten. Dann ist aber $1 \cdot 0 = 0$ eine nichttriviale Darstellung von 0.

Beispiele:

1) Die Vektoren $\vec{e}_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ und $\vec{e}_2 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ des $\mathbb{R}^3$ sind linear unabhängig, denn aus

   $$\lambda_i \cdot \vec{e}_1 + \lambda_2 \cdot \vec{e}_2 = 0 \quad \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \Rightarrow \lambda_1 = \lambda_2 = 0$$

2) Das System $\{\vec{x}, \vec{x}\}$ $\vec{x} \in \mathbb{R}^k$ ist linear abhängig, denn $1 \cdot \vec{x} + (-1) \cdot \vec{x} = 0$.
3) Sei V der Vektorraum der Funktionen $f : [0,1] \rightarrow \mathbb{R}$. Seien $x_{1,} \ldots, x_n$ verschiedene Elemente von $[0,1]$ und die Funktionen $f_{1,} \ldots f_n$ definiert durch

   $$f_i(x) = \begin{cases} 1 & für\ x = x_i \\ 0 & für\ x \neq x_i \end{cases}$$

   Dann sind die Vektoren $f_i \quad , i = 1, \ldots, n$ linear unabhängig, denn ist

   $\sum_{i=1}^{n} \lambda_i \cdot f_i = 0 \quad (Nullfunktion\, 0(x) = 0 \,\forall\, x \in [0,1])$ so ist auch

   $$\sum_{i=1}^{n} \lambda_i \cdot f_i(x) = 0(x) \quad \forall\, x \in [0,1]$$

   Setzt man speziell $x = x_j (1 \leq j \leq n)$ ein, so ist $f_i(x_j) = \begin{cases} 1\, für\ j = i \\ 0\, für\ j \neq i \end{cases}$ also

   $\sum_{i=1}^{n} \lambda_i \cdot f_i(x_j) = \lambda_j = 0$, d.h. die Vektoren sind linear unabhängig.

Definition: Die maximale Kardinalzahl einer linear unabhängigen Teilmenge des Vektorraums von V, symbolisch dim V, heißt die Dimension von V, d.h.

1) $dim\{0\} = 0$
2) Gibt es ein $n \in \mathbb{N}, n \geq 1, x_{1,} \ldots, x_n \in V$, die linear unabhängig sind, jedoch je $(n+1)$ Vektoren linear abhängig, so ist dim V=n
3) Gibt es zu jedem $n \in \mathbb{N}, n \geq 1$ eine linear unabhängige Menge $\{x_{1,} \ldots x_p\}$ von n Vektoren, so heißt V unendlich-dimensional.

Beispiel 1: Sei V der Vektorraum der Funktionen $f : [0,1] \rightarrow \mathbb{R}$. Seien $x_{1,} x_{2,} x_{3,} \ldots$ paarweise verschiedene Elemente und die Funktionen $f_{1,} f_{2,} \ldots$ wie oben definiert. Wir haben gezeigt, dass für jedes $n \in \mathbb{N}$ ein System $f_{1,} f_{2,} \ldots, f_n$ von linear unabhängigen Funktionen gibt. V ist also unendlich-dimensional, $dim\, V = \infty$

Beispiel 2) Sei $V=\mathbb{R}^1$. Dann ist jedes $x\in\mathbb{R}^{1,} x\neq 0$ linear unabhängig. Aber 2 Vektoren $y, z\in\mathbb{R}^1$ sind linear abhängig. Ist $y=0$ oder $z=0$ so ist dies trivial, da 0 der Nullvektor in $\mathbb{R}^1$ ist und dieser stets linear abhängig ist. Sei nun $y\neq 0$ und $z\neq 0$. Dann gibt es Zahlen $\lambda, \mu=0$, so dass $y=\lambda\cdot x, z=\mu\cdot x\Rightarrow \mu\cdot y-\lambda\cdot z=\mu\cdot\lambda\cdot x=0$, d.h. y, z sind linear abhängig $\Rightarrow dim\,\mathbb{R}^1=1$.

Definition: Sei U ein Teilraum von V mit $dim U=k$. Dann heißt $x_0+U=\{x_0+u : u\in U\}$ ein k-dimensionaler affiner Teilraum.

weitere Beispiele: 1) Sei $V=\mathbb{R}^3$. Die Vektoren $\begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix}$ sind linear unabhängig, denn

$\lambda_1\cdot e_1+\lambda_2\cdot e_2+\lambda_3\cdot e_3=\begin{pmatrix}\lambda_1\\\lambda_2\\\lambda_3\end{pmatrix}=\begin{pmatrix}0\\0\\0\end{pmatrix}$.

2) $V=\mathbb{R}^3$. Sind die Vektoren $\begin{pmatrix}0\\1\\2\end{pmatrix}, \begin{pmatrix}-1\\2\\1\end{pmatrix}, \begin{pmatrix}3\\1\\1\end{pmatrix}$ linear abhängig oder linear unabhängig? Dazu machen wir den Ansatz $\lambda_1\cdot\begin{pmatrix}0\\1\\2\end{pmatrix}+\lambda_2\cdot\begin{pmatrix}-1\\2\\1\end{pmatrix}+\lambda_3\cdot\begin{pmatrix}3\\1\\1\end{pmatrix}=\begin{pmatrix}0\\0\\0\end{pmatrix}$. Dies entspricht dem linearen Gleichungssystem

$-\lambda_2+3\cdot\lambda_3=0$ I
$\lambda_1+2\cdot\lambda_2+\lambda_3=0$ II
$2\cdot\lambda_1+\lambda_2+\lambda_3=0$ III

$\lambda_1+2\cdot\lambda_2+\lambda_3=0$ II
$-\lambda_2+3\cdot\lambda_3=0$ I
$0-3\cdot\lambda_2-\lambda_3=0$ III – 2 II

$0+0-10\cdot\lambda_3=0 \Rightarrow\lambda_3=0 \quad \Rightarrow\lambda_1=0 \quad \Rightarrow\lambda_2=0$

=> die Vektoren sind linear unabhängig

Definition: Eine Teilmenge B des Vektorraums V heißt Basis von V, wenn
1) B linear unabhängig
2) L(B)=V

d.h. eine Basis ist linear unabhängiges Erzeugendensystem für V.

=> Folgerung: Ist $B=\{x_{1,}\ldots,x_n\}$ Basis von V, so lässt sich jeder Vektor $x\in V$ eindeutig als Linearkombination $x=\sum_{i=1}^{n}\lambda_i\cdot x_i$ darstellen.

Beispiel: $\vec{e}_k\in\mathbb{R}^n$ mit $\vec{e}_k=\begin{pmatrix}0\\ \vdots\\ 0\\ 1\\ 0\\ \vdots\\ 0\end{pmatrix}$. $B=\{\vec{e}_{1,}\vec{e}_{2,}\ldots,\vec{e}_n\}$ ist eine Basis des Vektorraums $\mathbb{R}^3$. B heißt die kanonische Basis von $\mathbb{R}^n$.

Satz: Sei V ein Vektorraum mit $dim V=n\in\mathbb{N}, n\geq 1$. Dann ist $B\subseteq V$ genau dann eine Basis, wenn sie aus n linear unabhängigen Vektoren besteht. Insbesondere ist also $dim V=|B|$ für jede Basis von V.

Beweis: Sei $B=\{x_{1,}\ldots,x_n\}$ linear unabhängig in V mit $dim V=n$. Dann ist $L(B)=V$, denn sonst wäre nämlich für ein $x\in V, x\notin L(B)$ und $\lambda\cdot x+\sum_{i=1}^{n}\lambda_i\cdot x_i=0$ (*) so wäre $\lambda=0$ (da sonst $\lambda\cdot x=-\sum_{i=1}^{n}\lambda_i\cdot x_i$, d.h. $x=\sum_{i=1}^{n}-\lambda^{-1}\cdot\lambda_i\cdot x_i$, also $x\in L(B)$), d.h. $\sum_{i=1}^{n}\lambda_i\cdot x_i=0$ und da $x_i(i=1\ldots\text{n})$ linear unabhängig sind auch $\lambda_i=0(i=1\ldots\text{n})$. Damit folgt aus (*), dass $\lambda=0,\lambda_i=0,i=1,\ldots,n\Rightarrow x,x_{1,}\ldots,x_n$ sind linear unabhängig in V im Widerspruch zu $dim V=n$. Jede Menge von n linear unabhängig Vektoren in V mit $dim V=n$ ist also eine Basis.

Umkehrung: Sei $dim V=n$. Zu zeigen: n linear unabhängige Vektoren bilden eine Basis.

Aus $dim V=n$ folgt, dass es eine Menge von n linear unabhängigen Vektoren in V gibt. Es bleibt zu zeigen, dass je 2 Basen eines Vektorraums gleich viele Elemente enthalten. Dazu benötigen wir die folgenden zwei Sätze:

Satz: (Austauschlemma) Sei $B=\{x_{1,}\ldots,x_n\}$ eine Basis VR V und $a\in V, a\neq 0$. Dann existiert eine Vektor x_i in der Basis, der gegen a ausgetauscht wieder eine Basis ergibt, d.h. $B'=\{x_{1,}\ldots,x_{i-1},a,x_{i+1},\ldots,x_n\}$.

Beweis: Da $L(x_{1,}\ldots,x_n)=V$, existiert eine Darstellung $a=\sum_{j=1}^{n}\lambda_j\cdot x_j$ und da $a\neq 0$, ist mindestens ein $\lambda_j\neq 0$. Sei $\lambda_i\neq 0$. Wir behaupten $B'=\{x_{1,}\ldots,x_{i-1},a,x_{i+n},x_n\}$ ist Basis.

1) B' ist linear unabhängig.
   Sei $\sum_{j=1}^{n}\lambda_j\cdot x_j+\mu\cdot a=0$, d.h. $\sum_{j=1,j\neq i}^{n}\lambda_i\cdot x_j+\sum_{j=1}^{n}\mu\cdot\lambda_j\cdot x_j=\sum_{j=1,i\neq j}^{n}(\lambda_j+\mu\cdot\lambda_j)\cdot x_j+\mu\cdot\lambda_i\cdot x_i=0$

Da $x_{1,} \ldots, x_n$ linear unabhängig sind, folgt
$\mu_j + \mu \cdot \lambda_j = 0 \quad j = 1 \ldots n \quad j \neq i \quad \mu \cdot \lambda_i = 0 \Rightarrow \mu = 0 \Rightarrow \lambda_j = 0 \quad j = 1 \ldots n, j \neq i$, also ist B' linear unabhängig.

2) $L(B') = V$. Aus der Darstellung $\vec{a} = \sum_{j=1}^{n} \lambda_j \cdot x_j$ folgt $\lambda_i \cdot x_i = a - \sum_{j=1, j \neq i}^{n} \lambda_j \cdot x_j$ und wegen $\lambda_i \neq 0$ folgt $x_i = \lambda_i^{-1} \cdot a - \sum_{j=1}^{n} \lambda_i^{-1} \cdot \lambda_j \cdot x_j$. Sei nun $x \in V$. Da $L(B) = V$, existiert eine Darstellung $x = \sum_{j=1}^{n} \mu_j \cdot x_j = \mu_i \cdot x_i + \sum_{j=1, j \neq i}^{n} \mu_j \cdot x_j \Rightarrow x = \mu_i \cdot \lambda_i^{-1} \cdot a + \sum_{j=1, j \neq i}^{n} (\mu_j - \mu_i \cdot \lambda_i^{-1} \cdot \lambda_j) \cdot x_j$, also $x \in L(B')$.

Bemerkung: a ist also gegen jeden Vektor $x_i \in B$ austauschbar, für den in der eindeutigen Darstellung $a = \sum_{j=1}^{n} \lambda_j \cdot x_j \quad (\lambda_j \neq 0)$ ist.

<u>Austauschsatz von Steinitz:</u>

Sei $B = \{x_{1,} \ldots, x_n\}$ eine Basis des Vektorraums V und seien $a_{1,} \ldots, a_p$ linear unabhängige Vektoren aus $V, p \leq n$. Dann existieren p Elemente $x_{i_1}, x_{i_2}, \ldots, x_{i_p}$ aus B so dass $B' = \{a_a, \ldots, a_p\} \cup \{x_j : j = 1 \ldots n, j \neq i_k, k = 1 \ldots p\}$ wieder eine Basis von V ist.

Beweis: Vollständige Induktion über p ($1 \leq p \leq n$)

Induktionsanfang: Für p=1 klar, weil dies das Austauschlemma ist.
Induktionsvoraussetzung: Der Satz ist für p-1 linear unabhängige Vektoren richtig.
Induktionsschritt: Seien nun $a_{1,} \ldots, a_p$ linear unabhängig. Nach der Induktionsvoraussetzung kann man dann $a_{1,} \ldots, a_{p-1}$ gegen $x_{i_1}, x_{i_2}, \ldots, x_{i_{p-1}}$ austauschen und erhält eine Basis B". a_p besitzt die Darstellung $a_p = \sum_{i=1}^{p-1} \mu_i \cdot a_i + \sum_{j=1, j \neq i_{1,} i_{2,} \ldots, i_{p-1}}^{n} \mu_i \cdot x_j$.
(Idee analog zum Austauschlemma)

Wir behaupten, dass mindestens eine der Zahlen $\lambda_i \neq 0$ ist. Wären nämlich alle $\lambda_j = 0$, so wäre $a_p + \sum_{i=1}^{p-1} (-\mu_i) \cdot a_i = 0$ eine nicht-triviale Darstellung des Nullvektors, ein Widerspruch zur linearen Unabhängigkeit von $a_{1,} \ldots, a_p$.
Da mindestens eine Zahl $\lambda_j \neq 0$, lässt sich a_p nach der Bemerkung zum Austauschlemma gegen das entsprechende x_j austauschen => Behauptung.

Folgerung 1: (und damit der Beweis vor dem Austauschlemma). Je 2 Basen eines Vektorraums V enthalten gleich viele Elemente.

Beweis: (indirekt)

Seien $B_1=\{x_{1,}\ldots,x_k\}$ und $B_2=\{\eta_{1,}\ldots,\eta_k\}$. 2 Basen von V und $k<n$ (o.B.d.A.)
Nach dem Austauschlemma lassen sich k Vektoren $\eta_{i_1},\eta_{i_2},\ldots\eta_{i_k}$ von B_2 austauschen, so dass $B_2{}'=B_1\cup\{\eta_j: j=1,\ldots,n\wedge j\neq i_{1,}i_{2,}\ldots i_k\}$ wieder eine Basis bildet.
Da B_1 eine Basis war, ist aber $\eta_j\in L(B_1)$, d.h. die Vektoren aus B_2 sind linear abhängig → Widerspruch.

Folgerung 2: Jede Menge $\{a_{1,}\ldots,a_p\}$ von linear unabhängigen Vektoren in einem Vektorraum V kann zu einer Basis von V erweitert werden.

Beweis: Sei $\dim V=n\in\mathbb{N}$. Sann besitzt V eine Basis $\{x_{1,}\ldots,x_n\}$. Nach dem Austauschsatz gibt es dann $i_{1,}\ldots,i_p$ so dass $\{a_{1,}\ldots,a_p\}\cup\{x_j: j=1,\ldots,n\ \ j\neq i_k\ \ k=1\ldots\mathrm{p}\}$ wieder eine Basis ist.

Folgerung 3: Zu jedem Teilraum U eines Vektorraums V gibt es einen Komplementärraum W in V.

Beweis: Sei $\dim U=p$ und $\{a_{1,}\ldots,a_p\}$ eine Basis von U. Ist $p=\dim V$, so setzen wir $W=\{0\}$. Ist $p<n$, so lässt sich $\{a_{1,}\ldots,a_p\}$ durch $b_{1,}\ldots,b_{n-p}$ zu einer Basis in V erweitern.
Sei $W=L(b_{1,\ldots,},b_{n-p})$. Da $U=L(a_{1,}\ldots,a_p), V=L(a_{1,\ldots,},a_p,b_{1,}\ldots,b_{n-p})$ ist V=U+W. Da außerdem $a_{1,}\ldots,a_p,b_{1,}\ldots,b_{n-p}$ linear unabhängig sind, ist $U\cap V=\{0\}$, denn wäre $x\neq 0\ \ x\in U\cap V$, so wäre

$$x=\sum_{i=1}^{p}\lambda_i\cdot a_i\quad(\lambda_i,\ldots,\lambda_p)\neq(0,\ldots,0)$$
$$x=\sum_{j=1}^{n-p}\mu_i\cdot b_i\quad(\mu_i,\ldots,\mu_p)\neq(0,\ldots,0)$$
$$0=x-x=\sum_{i=1}^{p}\lambda_i\cdot a_i+\sum_{j=1}^{n-p}(-\mu_i)\cdot b_j$$

eine nicht-triviale Darstellung des Nullvektors.

Satz: Seien U, W Teilräume des Vektorraums V. Dann gilt $\dim(U+W)=\dim U+\dim W-\dim(U\cap W)$.

Beweis: Sei $B_1=\{x_1,\ldots,x_p\}$ eine Basis von $U\cap W$, d.h. $\dim(U\cap W)=p$.
($B_1=\{0\},\dim(U\cap W)=0$ erlaubt).

Sei $\dim U = p + r$ und $\dim W = p + s$. Dann erweitern wir B_1 zu einer Basis.

$B_2 = \{x_1, \ldots, x_p, y_1, \ldots y_r\}$ von U
$B_3 = \{x_1, \ldots, x_p, z_1, \ldots z_s\}$ von W

Sei $U_1 = L(y_1, \ldots, y_r), W_1 = L(z_1, \ldots, z_s)$, dann können die Teilräume dargestellt werden durch

$$U = (U \cap W) \oplus U_1$$
$$W = (U \cap W) \oplus W_1$$

und $U + W = (U \cap W) \oplus U_1 \oplus W_1$, d.h.

$$\begin{aligned} \dim(U+W) &= \dim(U \cap W) + \dim U_1 + \dim W_1 \\ &= p + r + s \\ &= p + r + p + s + - p \\ &= \dim U + \dim W - \dim(U \cap W) \end{aligned}$$

5.3 Lineare Abbildungen

Definition: Seien U, V Vektorräume über den Körper K. Eine Abbildung $A: U \to V$ heißt lineare Abbildung, wenn folgendes gilt:

$$A(\lambda x+\mu y)=\lambda A(x)+\mu A(y) \quad x, y \in U \quad \lambda, \mu \in K$$

(Vektorraumhomomorphismus)

Beispiele: Sei $U=\mathbb{R}^{3,} V=\mathbb{R}^2$

$A\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}=\begin{pmatrix} x_1+2x_2 \\ -3x_3 \end{pmatrix}$ ist linear.

für $\vec{x}=\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}\in\mathbb{R}^3$ und $\vec{y}=\begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}\in\mathbb{R}^3$ und $\lambda, \mu \in K$.

$$A(\lambda\vec{x}+\mu\vec{y})=A\begin{pmatrix} \lambda x_1+\mu y_1 \\ \lambda x_2+\mu y_2 \\ \lambda x_3+\mu y_3 \end{pmatrix}=\begin{pmatrix} \lambda x_1+\mu y_1+2(\lambda x_2+\mu y_2) \\ -3(\lambda x_3+\mu y_3) \end{pmatrix}=\begin{pmatrix} \lambda(x_1+2x_2)+\mu(y_1+2y_2) \\ \lambda(-3x_3)+\mu(-3y_3) \end{pmatrix}$$

$$\lambda\begin{pmatrix} x_1+2x_2 \\ -3x_3 \end{pmatrix}+\mu\begin{pmatrix} y_1+2y_2 \\ -3y_3 \end{pmatrix}$$

$$\lambda A(x)+\mu A(y)$$

2) Sei $\vec{u}, \vec{v}\in\mathbb{R}^3$ und $A: \mathbb{R}^2\to\mathbb{R}^3 \quad A\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}=x_1\vec{u}+x_2\vec{v}$.

$$A(\lambda\vec{x}+\mu ec\, y)=A\left(\lambda\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}+\mu\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}\right)$$

A ist linear, denn $=A\begin{pmatrix} \lambda x_1+\mu y_1 \\ \lambda x_2+\mu y_1 \end{pmatrix}$

$$=(\lambda x_1+\mu y_1)\vec{u}+(\lambda x_2+\mu y_1)\vec{v}$$
$$=\lambda x_1\vec{u}+\lambda x_2\vec{v}+\mu x_1\vec{u}+\mu x_2\vec{v}$$
$$=\lambda A(x)+\mu A(y)$$

3) Die Menge $\mathbb{R}_n[x]$ alle Polynome vom Grade <= n über R, d.h. alle Ausdrücke der Form $\sum_{i=0}^{n} a_i \cdot x^i \quad (a_i \in \mathbb{R})$ bilden mit den Operationen

$$\sum_{i=0}^{n} a_i \cdot x^i + \sum_{i=0}^{n} b_i \cdot x^i = \sum_{i=0}^{n} (a_i + b_i) \cdot x^i$$
$$\lambda \sum_{i=0}^{n} a_i \cdot x^i = \sum_{i=0}^{n} \lambda \cdot a_i \cdot x^i$$

einen Vektorraum über $\mathbb{R}$. Die Abbildung $D: \mathbb{R}_n[x] \to \mathbb{R}_n[x]$

$$D\left(\sum_{i=0}^{n} a_i \cdot x^i\right) = \sum_{i=1}^{n} (i\, a_i)\, x^{i-1} + 0 \cdot x^n$$

n=3
$D(a_0 + a_1 x + a_2 x^2 + a_3 x_3) = a_1 + 2 a_2 x + 3 a_3 x^2 + 0 x^3$
(Differenzationsoperator) ist linear. (HA)

4) $A: \mathbb{R} \to R \qquad A(x) = x + 1$ ist nicht linear, denn z.B. $1 = A(0+0) \neq A(0) + A(0) = 1 + 1$

5) $A: \mathbb{R}^2 \to \mathbb{R}^2 \quad A\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 \\ (x_1 + x_2)^2 \end{pmatrix}$ ist nicht linear, denn

$$A\left(2\begin{pmatrix} 1 \\ 1 \end{pmatrix}\right) = A\begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 \\ 16 \end{pmatrix} \quad \neq \quad A\begin{pmatrix} 1 \\ 1 \end{pmatrix} + A\begin{pmatrix} 1 \\ 1 \end{pmatrix} = 2\, A\begin{pmatrix} 1 \\ 1 \end{pmatrix} = 2\begin{pmatrix} 1 \\ 4 \end{pmatrix} = \begin{pmatrix} 2 \\ 8 \end{pmatrix}$$

6) Sei $U = V = \mathbb{R}^3$ und

$$A(\vec{x}) = A\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} a_{11} \cdot x_1 + a_{12} \cdot x_2 + a_{13} + x_3 \\ a_{21} \cdot x_1 + a_{22} \cdot x_2 + a_{23} + x_3 \\ a_{31} \cdot x_1 + a_{32} \cdot x_2 + a_{33} + x_3 \end{pmatrix}$$

wobei $a_{ij} \in \mathbb{R}$ vorgegeben sind, ist linear.

Satz: Seien U,V Vektorräume über K. Die Abbildung $A: U \to V$ sei linear, dann gilt:

1) $A(0) = 0$
2) Sind $x_{1,} \dots, x_n$ linear abhängig in U, so sind auch $A(x_1), A(x_2), \dots, A(x_n)$ linear abhängig in V.
   Dies gilt nicht für linear unabhängige Vektoren, $x_{1,} \dots, x_n$ linear unabhängig $\neq > A(x_1), A(x_2), \dots, A(x_n)$ linear unabhängig

3) Ist $\{x_{1,} \ldots, x_n\}$ eine Basis von U, so ist A durch die Angabe von $A(x_1), A(x_2), \ldots, A(x_n)$ eindeutig festgelegt.

Beweis:

1. $A(0) = A(0 \cdot 0) = 0 \cdot A(0) = 0 \quad da\, 0 \cdot x = 0 \quad \forall x \in V$

2. $x_{1,} \ldots, x_n$ linear abhängig $\Rightarrow \exists \lambda_{1,} \ldots, \lambda_n \neq (0,0,\ldots,0)$ mit . Dann ist auch $A(\sum_{i=0}^{n} \lambda_i \cdot x_i) = \sum_{i=1}^{n} \lambda_i \cdot A(x_i)$ und damit sind auch $A(x_i)$ $i=1\ldots n$ linear abhängig
   Aber: wählen wir z.B. die Abbildung $A: U \rightarrow V$ mit $A(x)=0 \quad \forall x \in U$ so ist A linear, führt aber linear unabhängige Mengen von Vektoren in den Nullvektor der linear abhängige.

   oder Beispiel: $\begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix}$ sind linear unabhängig, aber $A\begin{pmatrix}1\\0\\0\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix}, A\begin{pmatrix}1\\0\\0\end{pmatrix} = \begin{pmatrix}2\\0\end{pmatrix}$ sind linear abhängig.

3. Ist $\{x_{1,} \ldots, x_n\}$ Basis von U und $x = \sum_{j=1}^{n} \lambda_j \cdot x_j$ so ist
   $A(x) = A(\sum_{j=1}^{n} \lambda_j \cdot x_j) = \sum_{j=1}^{n} \lambda_i \cdot A(x_i)$, d.h. A(x) ist durch $A(x_j)$ $(j=1,\ldots,n)$ festgelegt.

Definition: Sei $A: U \rightarrow V$ eine lineare Abbildung. Dann heißt

1) Kern $A = \{x : x \in U, A(x) = 0\}$ der Kern von A
2) Im $A = \{y : y \in V \;\; und \;\; \exists x \in U \;\; mit \;\; A(x) = y\}$ - das Bild von U unter der Abbildung A.

Satz: Ist $A: U \rightarrow V$ linear, dann ist Kern A ein Teilraum von U. Im A ist V.

Beweis:

1) Seien $x_{1,} x_2 \in Kern\, A$. Dann ist für
   $A(x_1 + \lambda \cdot x_2) = A(x_1) + \lambda \cdot A(x_2) = 0 + \lambda \cdot 0 = 0 \;\Rightarrow\; x_1 + \lambda \cdot x_2 \in Kern\, A$
2) Sei $y_{1,} y_2 \in \Im A, d.h. \exists x_{1,} x_2 \in U \;\; mit \;\; y_1 = A(x_1), y_2 = A(x_2)$. Dann ist
   $y_1 + \lambda \cdot y_2 = A(x_1) + \lambda \cdot A(x_2) = A(x_1 + x_2)$ mit $x_1 + \lambda \cdot x_2 \in U, d.h.\, y_1 + \lambda x_2 \in \Im A$

Beispiele:

1) $A: \mathbb{R}^2 \to \mathbb{R}^2$
$A\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 - 2\cdot x_2 \\ 0 \end{pmatrix}$
Der Kern „Kern A" besteht aus allen $x_{1,} x_2$ mit der Eigenschaft $x_1 = 2\cdot x_2$. Das Bild Im A besteht aus allen $x_{1,} x_2$ mit $x_2 = 0$.
2) Sei $U = V = \mathbb{R}_n[x]$ und $D: \mathbb{R}_n[x] \to \mathbb{R}_n[x]$ wie im Beispiel 3 (oben)
Der Nullvektor in $\mathbb{R}_n[x]$ ist das Nullpolynom $\sum_{j=1}^{n} 0\cdot x^j = 0$
$p(x) = \sum_{j=0}^{n} a_j \cdot x^j \quad \in Kern D \Leftrightarrow D(p) = \sum_{j=1}^{n} top\, n(j\cdot a_j)\cdot x^{j-1} = \sum_{j=0}^{n} 0\cdot x^j \Leftrightarrow a_j = 0, \ \ j = 1 \ldots \mathrm{n}$
$\Rightarrow Kern D = \{p(x) \in \mathbb{R}_n[x] : p(x) = a_0 \cdot x^0 + 0\cdot x^1 + \ldots + 0\cdot x^n, a_0 \in \mathbb{R}\} = \{a_0 \cdot x^{0,} a \in \mathbb{R}\}$
$\Im D = \{p(x) \in \mathbb{R}_n[x] : p(x) = \sum_{j=1}^{n-1} a_j \cdot x^j, a_j \in \mathbb{R}\} = \mathbb{R}_{n-1}[x]$

Definition: Sei $A: U \to V$ linear, d.h. ein Vektorraumhomomorphismus. Ist A injektiv, so heißt A Monomorphismus, ist A surjektiv, so heißt A Epimorphismus, ist A bijektiv, so heißt A Isomorphismus,

Gibt es einen Isomorphismus $A: U \to V$, so heißen U und V isomorph, symbolisch $U \simeq V$.

Beispiel: Ist $B = \{x_{1,} \ldots, x_n\}$ eine geordnete Basis von V über dem Körper K und $x = \sum_{i=1}^{n} \lambda_i \cdot x_i$

so ist die Abbildung $F_B: V \to K^n$ $F_B(x) = \begin{pmatrix} \lambda_1 \\ \ldots \\ \lambda_n \end{pmatrix}$ eine bijektive Abbildung (die Darstellung von x ist eindeutig). Die Abbildung ist linear, denn seien

$x = \sum_{i=1}^{n} \lambda_i \cdot x_i, \ \ y = \sum_{i=1}^{n} \mu_i \cdot x_i \quad \in V, \ \ \lambda_i, \mu_i \in K$ dann ist

$$F_B(\lambda y + \mu y) = F_B\left(\sum_{i=1}^{n} (\lambda \lambda_i + \mu \mu_i) x_i\right) = \begin{pmatrix} \lambda\lambda_1 + \mu\mu_1 \\ \lambda\lambda_2 + \mu\mu_2 \\ \ldots \\ \lambda\lambda_n + \mu\mu_n \end{pmatrix} = \lambda \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \ldots \\ \lambda_n \end{pmatrix} + \mu \begin{pmatrix} \mu_1 \\ \mu_2 \\ \ldots \\ \mu_n \end{pmatrix}$$

$$= \lambda \cdot F_B(x) + \mu \cdot F_B(y)$$

F_B heißt kanonischer Isomorphismus.

Satz:

1) Seien $A:U\to V, B:V\to W$ linear, dann ist die Hintereinanderausführung $C=B\circ A:U\to W$ linear. Sind A und B Isomorphismen, so ist auch C ein Isomorphismus.
2) Sei A ein Isomorphismus. Dann ist auch die Umkehrabbildung $A^{-1}:V\to U$ ein Isomorphismus.

Beweis:

1) Seien $x,y\in U, \lambda,\mu\in K$
$(B\circ A)(\lambda x+\mu y)=B(A(\lambda x+\mu y))=B(\lambda A(x)+\mu A(y))=$
$\lambda B(A(x))+\mu B(A(y))=\lambda(B\circ A)(x)+\mu(B\circ A)(y)$
$\Rightarrow B\circ A$ ist linear. Sind A und B bijektiv, so ist auch $B\circ A$ bijektiv → C ist ein Isomorphismus
2) Mit A ist auch A^{-1} bijektiv.
z.z.: $A-1$ ist linear
Seien $y_{1,}y_{2in}V, \lambda\in K$. Da A bijektiv ist, gibt es $x_{1,}x_2\in U$ mit
$A(x_1)=y_{1,}\ A(x_2)=y_2\Rightarrow A^{-1}(\lambda y_1+\mu y_2)=A^{-1}(\lambda A(x_1)+\mu A(x_2))=$
$A^{-1}(A(\lambda x_1+\mu x_2))=\lambda_1+\mu x_2=\lambda A^{-1}(y_1)+\mu A^{-1}(y_2)$

Satz: Eine lineare Abbildung $A:U\to V$ ist genau dann injektiv, wenn $kern A=\{0\}$ gilt.

Beweis: Sei A injektiv, d.h. aus $A(x)=A(y)$ folgt x=y. Dann gilt $A(x)-A(y)=A(x-y)=0\Leftrightarrow x-y=0$, d.h. $Kern A=\{0\}$.

Sei $A(x)=A(y)\ \Rightarrow 0=A(x)-A(y)=A(x-y)\ \Rightarrow x-y\in Kern A\ \Rightarrow x-y=0\ \Rightarrow x=y$

Satz: Sei $A:U\to V$ linear mit $dim U=n<\infty$. Dann ist $dim Kern A+dim\Im A=dim U$.

Beweis: Offenbar ist Kern A als Teilraum von U mit $dim U=n$ ebenfalls endlichdimensional. Nun sei $B=\{e_{1,}\dots,e_k\}$ eine Basis von Kern A. Diese kann durch $\{e_{k+1},\dots,e_n\}$ zu einer Basis in U ergänzt werden.
Jedes Element von Im A besitzt folgende Gestalt

$$A\left(\sum_{i=1}^n\lambda_i e_i\right)=\sum_{i=1}^n\lambda_i A(e_i)=\underbrace{\sum_{i=1}^k\lambda_i A(e_i)}_{0\,denn\,A(e_i)=0\ i=1,\dots,k}+\sum_{i=k+1}^n\lambda_i A(e_i)$$

Das Bild von A wird somit durch die Vektoren $A(e_i)(i=k+1,\dots,n)$ aufgespannt. Diese Vektoren sind linear unabhängig, denn aus

$$0=\sum_{i=k+1}^n\lambda_i A(e_i)=A\left(\sum_{i=k+1}^n\lambda_i e_i\right)$$

$$\Rightarrow x := \sum_{i=k+1}^{n} \lambda_i e_i \in Kern\, A$$

Jedes Element $x \in Kern\, A$ kann in der Form

$$x = \sum_{i=1}^{k} \mu_i e_i$$

dargestellt werden, d.h.

$$0 = x - x = \sum_{i=1}^{k} \mu_i e_i \cdot \sum_{i=k+1}^{n} (-\lambda_i) e_i$$

und da e_i $(i = 1, \ldots, n)$ linear unabhängig sind, folgt $\mu_i = 0$ $i = 1, \ldots, k$ und $\lambda_i = 0$ $i = k+1, \ldots, n$ $\Rightarrow A_{ei}$ $i = k+1 \ldots n$ sind linear unabhängig und damit $dim \Im A = n - k$

Satz: Es seien U und V Vektorräume über K. $b_1, \ldots, b_n$ sei eine Basis von U und $v_i \in V$ $i = 1 \ldots n$. Dann gibt es genau eine lineare Abbildung $A: U \rightarrow V$ mit der Eigenschaft $A(b_i) = v_i$ $\forall i = 1 \ldots n$

Beweis: Die Abbildung ist durch $A(b_i) = v_i$ $(i = 1 \ldots n)$ eindeutig festgelegt.

für $u = \sum_{i=1}^{n} \lambda_i b_i$ definieren wir deshalb die Abbildung $A(u)$

Die Abbildung ist linear.

Eindeutigkeit: Sei B eine weitere Abbildung mit dieser Eigenschaft, dann ist $B(u) = \sum_{i=1}^{n} \lambda_i B\underbrace{(e_i)}_{v_i} = A(i)$, d.h. A und B sind eindeutig.

Satz: Es seien U und V endlichdimensionale Vektorräume über K. Dann sind U und V genau dann isomorph, wenn sie die gleiche Dimension haben.

$$U \simeq V \Leftrightarrow dim\, U = dim\, V$$

Beachte: jeder K-Vektorraum der Dimension n ist isomorph zu K^n, d.h. insbesondere jeder endlich dimensionale Vektorraum ist isomorph zu $\mathbb{R}^n$

Beweis:

<=

Sei $A:U \to V$ ein Isomorphismus und $u_1 \dots u_n$ eine Basis von U. Wir zeigen $A(u_1), A(u_2) \dots A(u_n)$ bilden eine Basis von V.
$A(u_i)\ \ i=1\dots n$ sind linear unabhängig, denn aus

$0=\sum_{i=1}^{n} \lambda_i A(u_i)=A\left(\sum_{i=1}^{n} \lambda_i u_i\right)$ folgt wegen der Injektivität (Satz $Kern\,A=\{0\}$)
$\sum_{i=1}^{n} \lambda_i u_i=0 \Rightarrow \lambda_i=0 \quad i=1\dots n$ da u_i linear unabhängig $\Rightarrow A(u_i) \quad i=1\dots n$ sind linear unabhängig. Die Vektoren $A(u_i)$ erzeugen V. Da A surjektiv ist, gibt es zu jedem $v \in V$ ein $u \in U$ mit $A(U)=V$, also ist $v=A(u)=A\left(\sum_{i=1}^{n} \lambda_i u_i\right)=\sum_{i=1}^{n} \lambda_i A(u_i)$.

=>

Sei $dim\,U=dim\,V$ und sei $u_{1,} u_{2,} \dots, u_n$ eine Basis von U und $v_1 \dots v_n$ eine Basis von V. Nach dem obigen Satz gibt es dann zwei lineare Abbildungen mit $A:U \to V \quad A(u_i)=v_i$ $B:V \to U \quad B(v_i)=u_i$. Diese Abbildungen sind invers zueinander und somit sind sie bijktive lineare Abbildungen, d.h. ein Isomorphismus zwischen U und V.

5.4 Matrizen

Situation:

$F_B: U \to K^n$ $(K = \mathbb{R}$ *oder* $\mathbb{C}, n = \dim U$, *Isomorphismus*$)$
$B = \{u_1, \dots, u_n\}$ Basis von U
$F_{B'}: V \to \mathbb{R}^m$ $(m = \dim V$, *Isomorphismus*$)$
$B' = \{v_1, v_2, \dots, v_m\}$ Basis von V

$$\begin{array}{ccc} U & \to & V \\ F_B\downarrow & & \downarrow \\ \mathbb{R}^n & \dots & \mathbb{R}^m \end{array}$$

Problem: Wie können die Abbildungen $A: \mathbb{R}^n \to \mathbb{R}^m$ aussehen?

5.4.1 Matrizen und lineare Abbildungen in $\mathbb{R}^2$

Eine lineare Abbildung $A: \mathbb{R}^2 \Rightarrow \mathbb{R}^2$ kann durch die Angabe der Bilder von den Basisvektoren $\begin{pmatrix}1\\0\end{pmatrix}$ und $\begin{pmatrix}0\\1\end{pmatrix}$ angegeben werden.

Sind diese $A\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}a_{11}\\a_{21}\end{pmatrix}, A\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}a_{12}\\a_{22}\end{pmatrix}$ so gilt für jeden Vektor $\vec{x} \in \mathbb{R}^2$

$$A(\vec{x}) = A\begin{pmatrix}x_1\\x_2\end{pmatrix} = A\left(x_1\begin{pmatrix}x_1\\x_2\end{pmatrix} + x_2\begin{pmatrix}x_1\\x_2\end{pmatrix}\right) = x_1 A\begin{pmatrix}1\\0\end{pmatrix} + x_2 A\begin{pmatrix}0\\1\end{pmatrix} = x_1\begin{pmatrix}a_{11}\\a_{21}\end{pmatrix} + x_2\begin{pmatrix}a_{12}\\a_{22}\end{pmatrix} = \begin{pmatrix}a_{11}x_1 + a_{12}x_2\\a_{21}x_1 + a_{22}x_2\end{pmatrix}$$

Dabei ist $\vec{x} = \begin{pmatrix}x_1\\x_2\end{pmatrix}$ ein Vektor und $A = \begin{pmatrix}a_{11} & a_{12}\\a_{21} & a_{22}\end{pmatrix}$ nennen wir Matrix.

Definition: Ein Quadrupel reeller Zahlen $\begin{pmatrix}a_{11} & a_{12}\\a_{21} & a_{22}\end{pmatrix}$ heißt 2x2-Matrix. Die Menge aller 2x2 Matrizen bezeichnen wir mit $\mathbb{R}^{2x2}$. $\begin{pmatrix}a_{11}\\a_{21}\end{pmatrix}$ und $\begin{pmatrix}a_{12}\\a_{22}\end{pmatrix}$ heißen Spalten oder Spaltenvektoren und $(a_{11} \quad a_{12})$ und $(a_{21} \quad a_{22})$ heißen Zeilen oder Zeilenvektoren. a_{ij} ist das Element in der i-ten Zeile und in der j-ten Spalte.

Damit folgt: Zu jeder linearen Abbildung $A: \mathbb{R}^2 \to \mathbb{R}^2$ gibt es genau eine Matrix $A \in \mathbb{R}^{2x2}$ mit der Eigenschaft $A(\vec{x})=A\vec{x}$. Umgekehrt definiert jede Matrix $A\in\mathbb{R}^2\to\mathbb{R}^2$ durch die Vorschrift $A\in\mathbb{R}^2\to\mathbb{R}^2: A(\vec{x})=A\vec{x}$.

Beispiele:

1) $A\begin{pmatrix}\lambda & 0\\ 0 & \lambda\end{pmatrix}$ für $\vec{x}\in\mathbb{R}^2$ ist $A\vec{x}=\begin{pmatrix}\lambda & 0\\ 0 & \lambda\end{pmatrix}\begin{pmatrix}x_1\\ x_2\end{pmatrix}=\begin{pmatrix}\lambda x_1\\ \lambda x_2\end{pmatrix}=\lambda\begin{pmatrix}x_1\\ x_2\end{pmatrix}$. Jeder Vektor wird um den Faktor λ gedehnt.
2) Die Matrix der Drehung um den Winkel α soll bestimmt werden. Der Vektor $\begin{pmatrix}1\\ 0\end{pmatrix}$ wird in dem Vektor $\begin{pmatrix}\cos\alpha\\ \sin\alpha\end{pmatrix}$ gedreht. Der Vektor $\begin{pmatrix}0\\ 1\end{pmatrix}$ wird in dem Vektor $\begin{pmatrix}-\sin\alpha\\ \cos\alpha\end{pmatrix}$.
   Die Matrix der Drehung um den Winkel α lautet $D_a=\begin{pmatrix}\cos\alpha & -\sin\alpha\\ \sin\alpha & \cos\alpha\end{pmatrix}$.

Sind A, B zwei lineare Abbildungen, $A, B\in\mathbb{R}^{2x2}$ so ist die Hintereinanderausführung möglich und $B\circ A$ ist wieder eine lineare Abbildung. Welche Matrix C gehört dazu? Sei

$$A=\begin{pmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix}, B=\begin{pmatrix}b_{11} & b_{12}\\ b_{21} & b_{22}\end{pmatrix}, C=\begin{pmatrix}c_{11} & c_{12}\\ c_{21} & c_{22}\end{pmatrix}.$$

$$\begin{pmatrix}c_{11}\\ c_{21}\end{pmatrix}=(B\circ A)\begin{pmatrix}1\\ 0\end{pmatrix}=B\left(A\begin{pmatrix}1\\ 0\end{pmatrix}\right)=B\begin{pmatrix}a_{11}\\ a_{21}\end{pmatrix}=\begin{pmatrix}b_{11}a_{11}+b_{12}a_{21}\\ b_{21}a_{11}+b_{22}a_{21}\end{pmatrix}$$

$$\begin{pmatrix}c_{12}\\ c_{22}\end{pmatrix}=(B\circ A)\begin{pmatrix}0\\ 1\end{pmatrix}=B\left(A\begin{pmatrix}0\\ 1\end{pmatrix}\right)=B\begin{pmatrix}a_{12}\\ a_{22}\end{pmatrix}=\begin{pmatrix}b_{11}a_{12}+b_{12}a_{22}\\ b_{21}a_{12}+b_{22}a_{22}\end{pmatrix} \Rightarrow c_{ij}=\sum_{k=1}^{2} b_{ik}a_{kj}$$

Beispiel:

$$A\begin{pmatrix}4 & 3\\ 2 & 1\end{pmatrix}$$

$$B=\begin{pmatrix}1 & 2\\ 2 & 4\end{pmatrix}\begin{pmatrix}8 & 5\\ 16 & 10\end{pmatrix}=C=B\circ A$$ oder kurz $C=BA$.

$$A=\begin{pmatrix}4 & 3\\ 2 & 1\end{pmatrix}\begin{pmatrix}10 & 20\\ 4 & 8\end{pmatrix}=C=A\circ B$$

i.a. $AB\neq BA$

5.4.2 Matrizen und lineare Abbildungen von $K^n \to K^m$

K steht wie üblich für irgendeinen Körper, z.B. Körper der reellen Zahlen.

Definition: Das rechteckige Schema von Elementen des Körpers K

$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & \dots \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$ heißt mxn Matrix. Die Menge aller mxn Matrizen mit Elementen aus K bezeichnen wir mit K^{mxn}. Dabei ist m die Anzahl der Zeilen und n die Anzahl der Spalten der Matrix. Der erste Index heißt Zeilenindex, der zweite Index heißt Spaltenindex.

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

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & \dots \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \dots \\ x_m \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \dots \\ b_m \end{pmatrix}$$, also $A\vec{x}=\vec{b}$.

Die Schreibweise $A\vec{x}=\vec{b}$ steht also abkürzend für ein lineares Gleichungssystem mit m linearen Gleichungen

$a_{i1}x_1+a_{i2}x_2+\dots+a_{¿}x_n=b_n \quad (i=1\dots n)$ mit den n Unbekannten $x_{1,}x_{2,}\dots,x_n$.

Satz: Zu jeder linearen Abbildung $f:K^n \to K^m$ gibt es genau Matrix $A \in K^{mxn}$ mit der Eigenschaft $f(\vec{x})=A\vec{x} \quad \forall \vec{x} \in K^n$. Umgekehrt definiert jede Matrix $A \in K^{mxn}$ eine lineare Abbildung $f:K^n \to K^m$ durch die Vorschrift $f:K^n \to K^m: \vec{x} \to A\vec{x} \;\; f(\vec{x})=A\vec{x}$.

Beweis: In den Spalten der Matrix stehen die Bilder der Basisvektoren durch diese wird doe Abbildung vollständig bestimmt, z.B. ist

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & \dots \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \begin{pmatrix} 1 \\ \dots \\ \dots \\ 0 \end{pmatrix} = \begin{pmatrix} a_{11} \\ \dots \\ \dots \\ a_{mn} \end{pmatrix}$$

Beachte: Für eine Abbildung von $K^n \to K^m$ braucht man eine Matrix aus K^{mxn}.

Beispiel: ges.: Matrix zu der Abbildung $f: \mathbb{R}^3 \to \mathbb{R}^2$

$$f\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_1 + \frac{1}{3} x_3 \\ x_2 + \frac{1}{3} x_3 \end{pmatrix}$$

$$f\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad f\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad f\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{3} \\ \frac{1}{3} \end{pmatrix}$$

$$A \begin{pmatrix} 1 & 0 & \frac{1}{3} \\ 0 & 1 & \frac{1}{3} \end{pmatrix} \in \mathbb{R}^{2x3}$$

Matrixmultiplikation und Hintereinanderausführung linearer Abbildungen

Sind $A: K^n \to K^m$ und $B: K^m \to K^r$ lineare Abbildungen, so ist die Hintereinanderausführung möglich und auch $B \circ A: K^n \to K^r$ ist linear. Die Matrix C heißt Produkt der Matrizen B und A. $C = B A$.

$$\begin{pmatrix} a_{11} & a_{1j} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{mj} & \dots & a_{mn} \end{pmatrix} \begin{pmatrix} b_{11} & b_{1j} & \dots & b_{1n} \\ \dots & \dots & \dots & \dots \\ b_{m1} & b_{mj} & \dots & b_{mn} \end{pmatrix} = \begin{pmatrix} \dots & \dots & \dots & \dots \\ \dots & b_{i1} a_{1j} + \dots + b_{im} a_{ni} & \dots & \dots \\ \dots & \dots & \dots & \dots \end{pmatrix}$$

also gilt $C = (c_{ij})_{i=1, j=1}^{r, n} \quad c_{ij} = \sum_{k=1}^{m} b_{ik} a_{kj}$

Beispiele:
1)

$$B = \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix} \quad A = \begin{pmatrix} 1 \\ 3 \end{pmatrix}$$

$$\begin{matrix} & \begin{pmatrix} 1 \\ 3 \end{pmatrix} \\ \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix} & \begin{pmatrix} 7 \\ 15 \\ 23 \end{pmatrix} \end{matrix}$$

bzw. $BA = \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \end{pmatrix} = 1 \begin{pmatrix} 1 \\ 3 \\ 5 \end{pmatrix} + 3 \begin{pmatrix} 2 \\ 4 \\ 6 \end{pmatrix} = \begin{pmatrix} 7 \\ 15 \\ 23 \end{pmatrix}$

2)

$$\vec{x}=\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}\in\mathbb{R}^{3x1} \qquad \vec{y}=\begin{pmatrix} y_1 & y_2 & x_3 \end{pmatrix}\in\mathbb{R}^{1x3}$$

$$\vec{x}\cdot\vec{y}=\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}\begin{pmatrix} y_1 & y_2 & x_3 \end{pmatrix}=\begin{pmatrix} x_1 y_1+x_1 y_2+x_1 y_3 \\ x_2 y_1+x_2 y_2+x_2 y_3 \\ x_3 y_1+x_3 y_2+x_3 y_3 \end{pmatrix}$$

$$\vec{y}\cdot\vec{x}=\begin{pmatrix} y_1 & y_2 & x_3 \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}=x_1 y_1+x_2 y_2+x_3 y_3\in\mathbb{R}$$

3)

$$A=\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}\in\mathbb{R}^{3x3}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}A=\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}=A$$

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

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}A=\begin{pmatrix} 4 & 5 & 6 \\ 1 & 2 & 3 \\ 7 & 8 & 9 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & 1 \end{pmatrix}A=\begin{pmatrix} 1 & 2 & 3 \\ 4\lambda & 5\lambda & 6\lambda \\ 7 & 8 & 9 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & \lambda & 1 \end{pmatrix}A=\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7+4\lambda & 8+5\lambda & 9+6\lambda \end{pmatrix}$$

Definition:

Für zwei Matrizen $A=(a_{ij})_{i=1,j=1}^{m,n}\in K^{mxn}$ und $B=(b_{ij})_{i=1,j=1}^{m,n}\in K^{mxn}$ und $\lambda\in K$ sei

$$A+B=\begin{pmatrix} a_{11}+b_{11} & \dots & a_{1n}+b_{1n} \\ \dots & \dots & \dots \\ a_{m1}+b_{m1} & \dots & a_{mn}+b_{mn} \end{pmatrix}$$ komponentenweise Addition

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

Rechenregeln für Matrizen

Satz: A, B, C seien gegebene Matrizen. Dann gilt

$(A+B)C=AC+BC$ \
| Distributivgesetze
$A(B+C)=AB+AC$ /

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

sofern die Matrizensummen und Matrizenprodukte auf einer Seite diese Gleichung ausführbar sind.

Satz: (Existenz einer inversen Matrix)

Es sei $A\in K^{nxn}$ die Matrix einer linearen Abbildung. Dann sind die folgenden Bedingungen äquivalent.

1) Es gibt eine Matrix $A^{-1}\in K^{nxn}$ mit der Eigenschaft
$$A^{-1}A=AA^{-1}=E=\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & \dots & \dots & \dots \\ 0 & \dots & \dots & 1 \end{pmatrix}$$
2) Die Abbildung $A:K^n\rightarrow K^n$ ist bijektiv
3) Die Spalten der Matrix A bilden eine Basis des K^n
4) Die Spalten der Matrix A sind linear unabhängig

Beweis:

1) $\Leftrightarrow$ 2)

1) besagt, dass es zu A eine inverse Abbildung gibt. Damit ist A bijektiv. Jede bijektive Abbildung f einer Menge auf sich selbst besitzt eine Umkehrabbildung g, für die gilt: $f \circ g = g \circ f = id$

2) $\Rightarrow$ 3)
Nach einem Satz aus Abschnitt 5.3 ist bekannt, dass bijektive lineare Abbildungen eine Basis auf eine Basis abbilden. Die Spalten der Matrix A sind aber gerade die Bilder der Basis. Bilden umgekehrt die Spalten eine Basis, so heißt dies, dass A eine Basis in eine Basis abbildet und damit ist A ein Isomorphismus (siehe Abschnitt 5.3) also bijektiv.

4) $\Rightarrow$ 3) klar

3) $\Rightarrow$ 4) n linear unabhängige Vektoren in einem n-dimensionalen Vektorraum bilden immer eine Basis (siehe Abschnitt 5.3)

Satz: Die Menge der invertierbaren Matrizen in K^{nxn} bilden bezüglich der Multiplikation eine Gruppe.

Beweis:
(G2) Assoziativgesetz: $(AB)C = A(BC)$ gilt

(G3) Existenz eines Einheitselementes: $E = \begin{pmatrix} 1 & \dots & 0 \\ \dots & 1 & \dots \\ 0 & \dots & 1 \end{pmatrix}$ $AE = EA$

(G4) Existenz von inversen Elementen gilt

(G1) Abgeschlossenheit: ist das Produkt zweier invertierbarer Matrizen wieder invertierbar?

Ja, denn $(AB)^{-1} = B^{-1} A^{-1}$

$B^{-1}(A^{-1} A) B = B^{-1} E B = B^{-1} B = E$

Beispiel: Berechnung der inversen Matrix von $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Falls die inverse Matrix $A^{-1} = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$ existiert, so muss gelten

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} +$$

d.h. 4 Gleichungen für die 4 Unbekannten e, f, g, h.

$ae+bg=1$
$af+bh=0$
$ce+dg=0$
$cf+dh=1$

$ade+bdg-bce-bdg=d \Rightarrow (ad-bc)e=d$
$adf+bdh-bcd-bdh=-b \Rightarrow (ad-bc)f=-b$
$-ace-bcg+ace+adg=-c \Rightarrow (ad-bc)g=-c$
$-acf-bch+acf+adh=a \Rightarrow (ad-bc)h=a$

→ falls $ad \neq bc$ ist gilt

$$\begin{pmatrix} e & f \\ g & h \end{pmatrix} = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Definition: Der Rang einer Matrix $A \in K^{mxn}$ ist die maximale Anzahl linear unabhängiger Spaltenvektoren in der Matrix.

1) $A=\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ rang A=3
2) $A=\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 2 & 0 & 2 \end{pmatrix}$ rang A=2 $(\vec{s}_1+\vec{s}_2=\vec{s}_3)$
3) $A=\begin{pmatrix} 1 & 2 & 4 \\ 2 & 4 & 8 \\ 3 & 6 & 12 \end{pmatrix}$ rang A=1
4) $A=\begin{pmatrix} 1 & 3 & 0 & 4 \\ 2 & 5 & 1 & 0 \\ 3 & 8 & 1 & 4 \end{pmatrix}$ Zeilenrang=2

Satz: Ist $f: K^n \rightarrow K^m$ eine lineare Abbildung mit zugehöriger Matrix $A \in K^{mxn}$ mit der Spalten ($s_{1,} s_{2,} \ldots, s_n$) so gilt:

i) Im f= $L(s_{1,} s_{2,} \ldots, s_n)$
ii) Ker f= $\{\vec{x} : A\vec{x}=\vec{0}\}$ ist die Menge der Lösungen des Gleichungssystems $A\vec{x}=\vec{0}$
iii) dim Im f=rang A
iv) dim Ker f=n-rang A

Beweis:

i) Da die s_i alle im Bild liegen und das Bild ein Vektorraum ist, gilt natürlich $\Im f \supseteq L(s_1, s_2, \ldots, s_n)$
Andererseits gilt:
$$f(\vec{x}) = A\vec{x} = \begin{pmatrix} a_{11}x_1 + \ldots a_{1n}x_n \\ \ldots \\ a_{m1}x_1 + \ldots + a_{mn}x_n \end{pmatrix} = x_1\vec{s}_1 + x_2\vec{s}_2 + \ldots + x_n\vec{s}_n$$
also lässt sich jedes Bildelement $f(\vec{x})$ als Linearkombination der Spaltenvektoren schreiben und somit $\Im f \subseteq L(\vec{s}_1, \ldots, \vec{s}_n)$

ii) ist die Def. des Kerns

iii) ist eine Folgerung von i)

iv) Es gilt $dim \Im f + dim Ker f = n$ (siehe Abschnitt 5.3)

Satz: „Spaltenrang=Zeilenrang“
für jede m x n Matrix ist der Rang gleich der Maximalzahl linear unabhängiger Zeilen der Matrix.

Beweis:

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

$\vec{z}_1, \vec{z}_2, \ldots, \vec{z}_m$ seien die Zeilen von $A(\vec{z}_1 = (a_{11}, a_{12}, \ldots, a_{1n}))$.

$\vec{s}_1, \vec{s}_2, \ldots, \vec{s}_m$ seien die Zeilen von $A(\vec{s}_1 = \begin{pmatrix} a_{11} \\ \ldots \\ a_{1n} \end{pmatrix})$. Der Zeilenrang sei r und es sei

$\vec{b}_1 = (b_{11}, b_{12}, \ldots, b_{1n})$
$\vec{b}_2 = (b_{21}, b_{22}, \ldots, b_{2n})$
...
$\vec{b}_r = (b_{r1}, b_{r2}, \ldots, b_{rn})$

eine Basis des von den Zeilen aufgespannten Vektorraums, d.h. die Zeilenvektoren können aus den Vektoren $\vec{b}_1, \ldots, \vec{b}_r$ linear kombiniert werden.

$\vec{z}_1 = k_{11}\vec{b}_1 + k_{12}\vec{b}_2 + \ldots + k_{1r}\vec{b}_r$
$\vec{z}_2 = k_{21}\vec{b}_1 + k_{22}\vec{b}_2 + \ldots + k_{2r}\vec{b}_r$
...
$\vec{z}_m = k_{m1}\vec{b}_1 + k_{m2}\vec{b}_2 + \ldots + k_{mr}\vec{b}_r$

Diese m Gleichungen können auch koordinatenweise aufgeschrieben werden.

z.B. erste Zeile

$$\underbrace{\begin{pmatrix} a_{11} \\ a_{12} \\ \dots \\ a_{11} \end{pmatrix}}_{\vec{z}_1} = k_{11} \underbrace{\begin{pmatrix} b_{11} \\ b_{12} \\ \dots \\ b_{1n} \end{pmatrix}}_{\vec{b}_1} + k_{12} \underbrace{\begin{pmatrix} b_{21} \\ b_{22} \\ \dots \\ b_{2n} \end{pmatrix}}_{\vec{b}_2} + \dots + k_{1r} \underbrace{\begin{pmatrix} b_{r1} \\ b_{r2} \\ \dots \\ b_{rn} \end{pmatrix}}_{\vec{b}_r}$$

Wir erhalten einen neuen Satz von m Gleichungen indem wir die (i-te) Zeile für jede der n Gleichungen aufschreiben.

$$a_{1i} = k_{1i} + b_{1i} + k_{12} b_{2i} + \dots + k_{1r} b_{ri}$$
$$a_{2i} = k_{2i} + b_{2i} + k_{22} b_{2i} + \dots + k_{2r} b_{ri}$$
...
$$a_{mi} = k_{mi} + b_{¿} + k_{m2} b_{mi} + \dots + k_{mr} b_{ri} \#$$

d.h.

$$s_i = \underbrace{\begin{pmatrix} k_{11} \\ \dots \\ k_{m1} \end{pmatrix}}_{\vec{k}_1} b_{1i} + \underbrace{\begin{pmatrix} k_{12} \\ \dots \\ k_{m2} \end{pmatrix}}_{\vec{k}_2} b_{2i} + \dots + \underbrace{\begin{pmatrix} k_{1r} \\ \dots \\ k_{mr} \end{pmatrix}}_{\vec{k}_r} b_{ri}$$

d.h. wir haben den i-ten Spaltenvektor $\vec{s}_i$ aus den Vektoren $\vec{k}_{1,} \vec{k}_{2,} \dots, \vec{k}_r$ linear kombiniert.

Dies gilt für alle $i = 1 \dots n$. Damit ist die Dimension des Spaltenraums jedenfalls <= r (der Spaltenraum kann durch $\vec{k}_{1,} \vec{k}_{2,} \dots, \vec{k}_r$ erzeugt werden) → Spaltenrang <= Zeilenrang

Jetzt vertauschen wir in dem Beweis jeweils Spalten und Zeilen und erhalten Zeilenrang <= Spaltenrang. => Spaltenrang=Zeilenrang und ab sofort gibt es nur noch den Rang einer Matrix.

Satz: Eine Matrix $A \in K^{nxn}$ ist genau dann invertierbar wenn Rang A=n.

Beweis:

- ist Rang A=n so bilden die Spalten eine Basis. Nach dem Satz zur Existenz einer inversen Matrix ist A invertierbar.
- wenn a eine Inverse besitzt, so bilden die Spalten eine Basis, also ist Rang A=n.

5.4.3 Spezielle Matrizen und Manipulation mit Elementarmatrizen

Definition: Sei $A=(a_{j,k})^{(n,n)} \in K^{nxn}$ eine quadratische Matrix.

1) gilt $a_{j,k}=0 \ \ \forall j>k$, dann heißt dieMatrix A obere Dreiecksmatrix
2) gilt $a_{j,k}=0 \ \ \forall j<k$, dann heißt die Matrix A untere Dreiecksmatrrix
3) gilt $a_{j,k}=0 \ \ \forall j\neq k$, dann heißt die Matrix A eine Diagonalmatrix
4) Die Einträge $a_{11,}a_{22,}\dots,a_{nn}$ heißen Diagonaleinträge der Matrix.

Beispiel:

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ 0 & a_{22} & a_{23} \\ 0 & 0 & a_{33} \end{pmatrix} \qquad \begin{pmatrix} c_{11} & 0 & 0 \\ 0 & c_{22} & 0 \\ 0 & 0 & c_{33} \end{pmatrix}$$

obere Dreiecksmatrix Diagonalmatrix

Definition:

1) Die quadratische Matrix $E=\begin{pmatrix} 1 & 0 & 0 \\ 0 & \dots & 0 \\ 0 & 0 & 1 \end{pmatrix} \in K^{nxn}$ heißt die n-te Einheitsmatrix
2) Folgende Elementarmatrizen sind leichte Modifikationen der Einheitsmatrix:

$E_{n,[\vec{z}_p\rightarrow\lambda\vec{z}_p]}$ Der Diagonaleintrag e_{pp} wird durch λ ersetzt.
$E_{n,[\vec{z}_q\rightarrow\lambda\vec{z}_p]}$ Der Eintrag e_{qp} wird durch λ ersetzt.
$E_{n,[\vec{z}_p <=> \vec{z}_q]}$ die Diagonaleinträge e_{pp} und e_{qq} werden durch Null ersetzt, die Einträge e_{pq} und e_{qp} werden durch Eins ersetzt.

Beispiel: für $\lambda\in K$ gilt

$$E_{3,[\vec{z}_3\rightarrow\lambda\vec{z}_2]}=\begin{pmatrix} 1 & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & 1 \end{pmatrix}, E_{3,[\vec{z}_2 <=> \lambda\vec{z}_3]}=\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, E_{3,[\vec{z}_3\rightarrow\vec{z}_3+\lambda\vec{z}_2]}=\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \lambda & 0 & 1 \end{pmatrix}$$

Beispiel: Wir zeigen, dass durch Multiplikation mit Elementarmatrizen eine Matrix in eine obere Dreiecksmatrix überführt werden kann.

Sei $A=\begin{pmatrix}1 & 3 & 2\\ 1 & 3 & 1\\ 2 & 5 & 5\end{pmatrix}\in\mathbb{R}^{3x3}$

$$A^{(1)}=E_{3,[z_1\to z_2-z_1]}A=\begin{pmatrix}1 & 0 & 0\\ -1 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}\begin{pmatrix}1 & 3 & 2\\ 1 & 3 & 1\\ 2 & 5 & 5\end{pmatrix}=\begin{pmatrix}1 & 3 & 2\\ 0 & 0 & -1\\ 2 & 5 & 5\end{pmatrix}$$

$$A^{(2)}=E_{3,[z_3\to z_3-\lambda z_1]}A^{(1)}=\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ -2 & 0 & 1\end{pmatrix}\begin{pmatrix}1 & 3 & 2\\ 0 & 0 & -1\\ 2 & 5 & 5\end{pmatrix}=\begin{pmatrix}1 & 3 & 2\\ 0 & 0 & -1\\ 0 & -1 & 1\end{pmatrix}$$

$$A^{(3)}=E_{3,[z_2<=>z_3]}A^{(2)}=\begin{pmatrix}1 & 0 & 0\\ 0 & 0 & 1\\ 0 & 1 & 0\end{pmatrix}\begin{pmatrix}1 & 3 & 2\\ 0 & 0 & -1\\ 0 & -1 & 1\end{pmatrix}=\begin{pmatrix}1 & 3 & 2\\ 0 & -1 & 0\\ 0 & 0 & -1\end{pmatrix}$$

und daher

$$\begin{pmatrix}1 & 3 & 2\\ 0 & -1 & 1\\ 0 & 0 & -1\end{pmatrix}=E_{3,[\vec{z}_3<=>\vec{z}_3]}\cdot E_{3,[\vec{z}_3-2\vec{z}_1]}\cdot E_{3,[\vec{z}_2\to\vec{z}_2-1\vec{z}_1]}\cdot A$$

Satz: Es sei $\vec{z}_j = A(j,:)\ \ j=1,\dots,m$ die Zeilen einer Matrix $A \in K^{mxn}$. Das Ergebnis der Multiplikation einer Elementarmatrix mit der Matrix A ist:

$E_{m,[\vec{z}_p \to \lambda \vec{z}_p]}$ Multiplikation der Zeile p mit λ. Die Matrix $E_{m,[\vec{z}_p \to \lambda \vec{z}_p]} \cdot A$ besitzt die Zeilen $A(j,:)$ für $j \neq p$.

$E_{m,[z_q \to \vec{z}_q + \lambda \vec{z}_q]}$ Addition des λ -fachen der p-ten Zeile zur q-ten Zeile

Die Matrix $E_{m,[z_q \to \vec{z}_q + \lambda \vec{z}_q]}$ besitzt die Zeilen $A(j,:)$ für $j \neq q$ und $A(q,:) + \lambda A(p,:)$ für j=q.

$E_{m,[z_q <=> \vec{z}_p]}$ Tausch der Zeilen p und q.

Beweis: Zur Abkürzung setzen wir $B := E_{m,[z_q \to \vec{z}_q + \lambda \vec{z}_p]} \in K^{mxm}$ und berechnen C=BA (die anderen Fälle bleiben zur Übung).

z.Z.:

$C(j,:) = A(k,:)$ für $j \neq q$
$C(q,:) = A(q,:) + \lambda A(p,:)$

Für die Zeile $j \neq q$ der Matrix B gilt $B(j,:) = (0,\dots \underbrace{,1}_{j-te\,Spalte} ,0\dots 0)$.

d.h. $b_{j,k} = 0$ für $j \neq k$ und daher mit der Definition des Matrixproduktes (siehe Abschnitt 5.4.2)

$C_{j,k} = \sum_{l=1}^{m} b_{j,l} a_{l,k} = b_{jj} a_{jk} = a_{jk}$ für $k = 1 \dots \mathrm{n}$, d.h. $C(j,:) = A(j,:)$ für alle $j \neq q$.

Für die q-te Zeile gilt:

$$B(j,0) = (0,\dots, \underbrace{\lambda}_{p-te\,Spalte} ,\dots \underbrace{,1}_{q-te\,Spalte} ,\dots,0)$$

und daher

$$C_{q,k} = \sum_{l=1}^{m} b_{ql} a_{lk} = \lambda a_{pk} + a_{qk} \quad k = 1 \dots \mathrm{n}$$

d.h.
$C(q,:) = A(q,:) + \lambda A(p,:)$

Die Inverse der Elementarmatrizen lassen sich explizit angeben.

Satz: Seien $p,q \in \{1,\ldots,n\}, \lambda \in K$

1) $\left(E_{n,[\vec{z}_p \to \lambda \vec{z}_p]}\right)^{-1} = E_{n,[\vec{z}_p \to \lambda^{-1} \vec{z}_p]} \quad \lambda \neq 0$
2) $\left(E_{n,[\vec{z}_p \to \vec{z}_p + \lambda \vec{z}_q]}\right)^{-1} = E_{n,[\vec{z}_p \to \vec{z}_p - \lambda^{-1} \vec{z}_q]}$
3) $\left(E_{n,[\vec{z}_p <=> \lambda \vec{z}_p]}\right)^{-1} = E_{n,[\vec{z}_p <=> \vec{z}_q]}$

Definition: Sei K ein Körper, $A = (a_{j,k})_{j=1,k=1}^{m,n} \in K^{mxn}$

1) Die Matrix $A^T := (a_{k,j})_{k=1,j=1}^{m,n} = ¿$
2) Gilt $A = A^T$, dann heißt die Matrix A symmetrisch.
3) Ist insbesondere $K = \mathbb{C}$ heißt
   $A^H := \overline{A^T} := (\overline{a}_{k,j})_{k=1,j=1}^{n,m} \in \mathbb{C}^{nxm}$
   die zur Matrix a konjugiert komplexe Matrix.
4) gilt $A = A^H$, dann heißt A hermitisch.

Beispiel:

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix}^T = \begin{pmatrix} 1 & 3 & 5 \\ 2 & 4 & 6 \end{pmatrix}$$

$$\begin{pmatrix} i & 1 \\ 2 & 3+2i \end{pmatrix}^H = \begin{pmatrix} -i & 2 \\ 1 & 3-2i \end{pmatrix}$$

Lemma: Seien $A,B \in K^{lxm}, C \in K^{mxn}$ und $\lambda \in K$. Dann gilt:

1) $(A+B)^T = A^T + B^T \qquad (A+B)^H = A^H + B^H$
2) $(\lambda A)^T = \lambda A^T \qquad (\lambda A)^H = \vec{\lambda} A^H$
3) $(A^T)^T = A \qquad (A^H)^H = A$
4) $(A \cdot C)^T = C^T A^T \qquad (AC)^H = C^H A^H$

$(A^T)^{-1} = (A^{-1})^T$

5.5 Lineare Gleichungen

Ein lineares Gleichungssystem $A\vec{x}=\vec{b}$ ist ein System von $m\in\mathbb{N}$ Gleichungen und $n\in\mathbb{N}$ Unbekannten $\vec{x}=(x_k)_{k=1}^{n}\in K^n$, wobei die Matrix

$$A=\begin{pmatrix} a_{11} & \dots & a_{1n} \\ . & . & . \\ a_{m1} & \dots & a_{mn} \end{pmatrix}\in K^{mxn} \quad a_{j,k}\in K$$
$$=(a_{j,k})_{j=1,k=1}^{m,n}$$

und der Vektor $\vec{b}=(b_j)_{j=1}^{n}\in K^m$ gegeben wird.

Beispiel: Gesucht sind die Punkte $\vec{x}=\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}\in\mathbb{R}^2$ mit

$$2x_1-x_2=6$$

mit $m=1, n=2, A=(2x-1)\in\mathbb{R}^{1x2} \quad \vec{b}=6\in\mathbb{R}^1$

lässt sich die Gleichung in der Form $A\vec{x}=\vec{b}$.

Definition: Sei $A\in K^{mxn}, \vec{b}\in K^m$. Die Menge aller Lösungen eines LGS $A\vec{x}=\vec{b}$ heißt Lösungsmenge des LGS

$$Lös(A,b):=\{\vec{x}\in K^n: A\vec{x}=\vec{b}\}$$

Ist $\vec{b}=\vec{0}$ dann heißt die Lösungsmenge auch Kern der Matrix A.

$$Ker(A):=Lös(A,\vec{0})=\{\vec{x}\in K^n: A\vec{x}=\vec{0}\}$$

Das lineare Gleichungssystem $A\vec{x}=\vec{b}$ heißt homogen falls $\vec{b}=\vec{0}$ ist andernfalls inhomogenes LGS.

obiges Beispiel:

$$2x_1-x_2=6 \Leftrightarrow x_2=2x_1-6$$
$$Lös(A,\vec{b})=\{\vec{x}\in\mathbb{R}^2: x_1\in\mathbb{R}\wedge x_2=2x_1-6\}=$$
$$\left\{\begin{pmatrix} 0 \\ -6 \end{pmatrix}+t\begin{pmatrix} 1 \\ 2 \end{pmatrix}: t\in\mathbb{R}\right\}$$

$Ker(A)=\{\vec{x}\in\mathbb{R}^2 : x_1\in\mathbb{R}\wedge x_2=2x_1\}$
$=\left\{t\begin{pmatrix}1\\2\end{pmatrix} : t\in\mathbb{R}\right\}$

Beispiel: $m=1, n=1$, d.h. $a_{11}x_1=b_1$ wobei $a_{11}b_1\in K$. Folgende Fälle sind möglich:

$a_{11}\neq 0 : Lös(a_{11,}b_1)=\{a_{11}^{-1}b_1\}$
$a_{11}=0\wedge b_1\neq 0 \quad Lös(a_{11,}b_1)=0$

Sei nun m=1, n=2, also $a_{11}x_1 a_{12}x_2=b_1$ wobei $a_{11,}a_{12,}b\in K$.

Eine Diskussion aller denkbaren Fälle ist nicht mehr in 3 Zeilen möglich.

=> Charakterisierung der Lösungsmenge

Satz: Sei $A\in K^{mxn}, b\in K^m$ und $\vec{s}_{1,}\vec{s}_{2,}\dots,\vec{s}_n$ die Spalten der Matrix A. Dann heißt das LGS $A\vec{x}=\vec{b}$

i) keine Lösung, falls $\vec{b}\notin L(\vec{s}_{1,}\vec{s}_{2,}\dots,\vec{s}_n)$
ii) genau eine Lösung, falls $\vec{b}\in L(\vec{s}_{1,}\vec{s}_{2,}\dots,\vec{s}_n)$ und die Spalten $\vec{s}_{1,}\vec{s}_{2,}\dots,\vec{s}_n$ sind linear unabhängig
iii) keine eindeutige Lösung falls $b\in L(\vec{s}_{1,}\vec{s}_{2,}\dots,\vec{s}_n)$ und die Spalten $\vec{s}_{1,}\vec{s}_{2,}\dots,\vec{s}_n$ sind linear abhängig

Beweis:

5.6 Gaußsches Eliminationsverfahren

Ziel: Herleitung eines Verfahrens, welches die Lösungsmenge eines beliebigen LGS berechnet werden kann.

Definition: Sei $A\in(a_{j,k})\in K^{mxn}, \vec{b}\in K^m$ und $A\vec{x}=\vec{b}$ ein LGS.

i) Der Vektor $\vec{b}$ heißt rechte Seite des LGS.
ii) Die Matrix $(A||b)\in K^{mx(n+1)}$ heißt heißt die um die rechte Seite erweiterte Matrix.
iii) Folgende Form einer erweiterten Matrix heißt Zeilenstufenform:

$$(A||b)=\begin{pmatrix} A_1 & A_2 & ||b_1 \\ 0 & 0 & ||b_2 \end{pmatrix}=\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1s} & ||a_{1,s+1} & \dots & a_{1n} & ||b_1 \\ 0 & a_{22} & \dots & a_{2s} & ||\dots & \dots & \dots & ||\dots \\ 0 & . & . & a_{ss} & ||a_{s,s+1} & \dots & a_{sn} & ||b_s \\ 0 & \dots & \dots & 0 & ||0 & \dots & 0 & ||b_{s+1} \\ \dots & \dots & \dots & \dots & ||0 & \dots & 0 & ||\dots \\ 0 & \dots & \dots & 0 & ||0 & \dots & 0 & ||b_m \end{pmatrix}$$

wobei $a_{11,}\dots,a_{ss}\neq 0$. Hierbei ist $A_1\in K^{s*s}$ eine obere Dreiecksmatrix, $A_2\in K^{s*(n-s)},\vec{b}_1\in K^s,\vec{b}_2\in K^{n-s}$

Die Bestimmung der Lösungsmenge eines beliebigen LGS erfolgt nun in zwei Phasen.

Phase I: Die Überführung des Gleichungssystems in Zeilenstufenform ohne Veränderung der Lösungsmenge.
Phase II: Die Bestimmung der Lösungsmenge der Zeilenstufenform.

Die Phase I: Der nächste Satz zeigt, u.a. dass gewisse Manipulationen mit Elementarmatrizen die Lösungsmenge des zugehörigen Gleichungssystems nicht ändern.

Satz: Sei $A\in K^{mxn},\vec{b}\in K^m,B\in K^{mxn}\dots C\in K^{nxn}\dots$

Dann gilt:

i) $Lös(A,b)=Lös(BA,B\vec{b})$
$Lös(A,b)=C\,Lös(AC,\vec{b})$

Beweis: es gilt: $\vec{x}\in Lös(A,b)\Leftrightarrow A\vec{x}=\vec{b}\Leftrightarrow BA\vec{x}=B\vec{b}\Leftrightarrow \vec{x}\in Lös(BA,B\vec{b})$

iii) Die Behauptung folgt aus $\vec{b}=A\vec{x}=AC\vec{y}$ wobei $x=C\vec{y}$

Bemerkung:
- Elementare Zeilenumformungen mit invertierbaren Elementarmatrizen ändern die Lösungsmenge eines LGS nicht (siehe Abschnitt 5.4.3)
- wegen ii) dürfen Spaltenvertauschungen (Multiplikation von rechts mit $E_{m,[\vec{z}_p\Leftrightarrow\vec{z}_q]}$ vorgenommen werden. Dies bewirkt jedoch eine entsprechende Vertauschung der Komponenten des Lösungsvektors

Satz: Sei $A \in K^{mxn}, \vec{b} \in K^m$. Es gibt eine invertierbare Matrix $B \in K^{mxm}$ und eine invertierbare Matrix $C \in K^{nxn}$, so dass die erweiterte Matrix $(BAC || B\vec{b})$ Zeilenstufenform besitzt.

Beweis: Der Beweis ist konstruktiv. Wir geben hier einen beliebigen Schnitt s des Verfahrens an. Die erweiterte Matrix möge die Gestalt

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1s} & \| a_{1,s+1} & \dots & a_{1n} & \| b_1 \\ 0 & a_{22} & \dots & a_{2s} & \| \dots & \dots & \dots & \| \dots \\ 0 & . & . & a_{ss} & \| a_{s,s+1} & \dots & a_{sn} & \| b_s \\ 0 & \dots & \dots & 0 & \| 0 & \dots & 0 & \| b_{s+1} \\ \dots & \dots & \dots & \dots & \| 0 & \dots & 0 & \| \dots \\ 0 & \dots & \dots & 0 & \| 0 & \dots & 0 & \| b_m \end{pmatrix}$$

mit $a_{11,} \dots, a_{ss} \neq 0$. Wir werden dieMatrix so modifizieren, dass die Zeilen 1...s und die Spalten 1...s im wesentlichen unverändert bleiben, zum anderen der verbleibende Teil in die folgende Gestalt überführt wird.

...

Dies kann formal durch Multiplikation mit invertierbaren Matrizen erreicht werden.

- Bestimmung eines Pivotelementes – wir müssen erreichen, dass $a'_{s+1,s+1} \neq 0$ ist. Sind alle Einträge $a_{j,k} = 0$ für $j = s+1 \dots m$ und $k = s+1 \dots n$, dann ist die Matrix bereits in der Zeilenstufenform. Andernfalls gilt es eine erste Spalte $p \geq s+1$ (i.a. die $s+1$ te) in welcher ein von Null verschiedener Eintrag zu finden ist. Gegebenenfalls bewirkt die Multiplikation mit einer Elementarmatrix von rechts ein Vertauschen der Spalten, so dass wir davon ausgehen, dass sich in der (s+1)ten Spalte ein von Null verschiedenes Element befindet. Bezeichne $q \geq s+1$ die erste Spalte mit $a_{k,s+1} \neq 0$ multiplizieren wir gegebenenfalls die erweiterte Matrix von links mit $E_{m,[\vec{z_{s+1}} \Leftrightarrow \vec{z_q}]}$.
- der Eliminierungsschritt: für das Pivotelement gilt $a_{s+1,s+1} \neq 0$. Für die Zeilen

  $j = s+2, \dots, m$ setzen wir $P_j = \dfrac{a_{j,s+1}}{a_{s+1,s+1}}$

  $A'(j,:) := A(j,:) - P_j A(s+1,:)$

  $b'_j := b_j - p_j b_{s+1}$

  Die Lösungsmengen der zugehörigen Gleichungssysteme stimmen überein, da wir nun mit invertierbaren Elementarmatrizen gearbeitet haben.

5.7 Berechnung der Inversen einer Matrix un Dreieckszerlegung

Eine quadratische nxn Matrix kann nur dann invertierbar sein, wenn sie Rang n hat. Die Zeilen-Stufen-Form hat also die Gestalt einer oberen Dreiecksmatrix, wobei die Diagonalelemente von Null verschieden sind.

$$\begin{pmatrix} a_1 & x & x \\ 0 & \dots & x \\ \dots & \dots & \dots \\ 0 & \dots & a_{nn} \end{pmatrix}$$

- Multipliziert man jeweils die i-te Zeile mit $\frac{1}{a_{ii}}$ so steht in der Diagonalen überall die 1.
- von rechts anfangend können wir jetzt wie im Gaußschen Algorithmus die Elemente in der rechten oberen Hälfte zu 0 machen.

Satz: Wandelt man eine invertierbare nxn Matrix mit elementaren Zeilenumformungen in eine Einheitsmatrix um, so entsteht die zu A inverse Matrix A^{-1} wenn man diese Umformung in der gleichen Reihenfolge auf die Einheitsmatrix andwendet.

Beweis: Bezeichnen wir mit $D_{1,}\dots,D_k$ die Matrizen die den an A durchgeführten Zeilenumformungen entspricht, so gilt

$E=D_k D_{k-1}\dots A=(D_k\dots D_1)A$ also

$A^{-1}=D_k\dots D_1$

Beispiel:

A

1 0 2	1 0 0	
2 -1 3	0 1 0	II-2I
4 1 8	0 0 1	
1 0 2	1 0 0	
0 -1 -1	-2 1 0	
0 1 0	-4 0 1	III+II
1 0 2	1 0 0	
0 -1 -1	-1 2 0	II*(-1)
0 0 -1	-6 1 1	III*(-1)

1 0 2	1 0 0	I-2III	
0 1 1	2 -1 0	II-III	
0 0 1	6 -1 -1		

1 0 0	-11 2 2	\	
0 1 0	-4 0 1			A^{-1}
0 0 1	6 -1 -1	/	

Dreieckszerlegung

Die Dreieckszerlegung oder LR-Zerlegung einer Matrix folgt sofort aus dem Gauß-Algorithmus.

Ziel: gesucht ist eine untere Dreiecksmatrix L (mit Einsen auf der Hauptdiagonalen) und eine obere Dreiecksmatrix R R, so dass A=L*R.

nochmals obiges Beispiel zur Phase I

Es gilt

$$\begin{pmatrix}1 & 1 & 1\\ 0 & -3 & -1\\ 0 & 0 & \frac{-1}{3}\end{pmatrix}=B\begin{pmatrix}1 & 1 & 1\\ 2 & -1 & 1\\ 3 & -2 & 1\end{pmatrix}$$

mit der invertierbaren Matrix B

$$B=E_{3,[\vec{z}_3\rightarrow\vec{z}_3-\frac{5}{3}\vec{z}_2]}E_{3,[\vec{z}_3\rightarrow\vec{z}_3-3\vec{z}_1]}E_{3,[\vec{z}_2\rightarrow\vec{z}_2-2\vec{z}_1]}$$

also

$$B^{-1}R=A$$

B^{-1} kann nach einem Satz aus Abschnitt 5.4.3 einfach invertiert werden

$$B^{-1}=(E_{3,[\vec{z}_2\rightarrow\vec{z}_2-2\vec{z}_1]})^{-1}(E_{3,[\vec{z}_3\rightarrow\vec{z}_3-3\vec{z}_1]})^{-1}(E_{3,[\vec{z}_3\rightarrow\vec{z}_3-\frac{5}{3}\vec{z}_2]})^{-1}$$

$$=E_{3,[\vec{z}_2\rightarrow\vec{z}_2+2\vec{z}_1]}¿^{-1}(E_{3,[\vec{z}_3\rightarrow\vec{z}_3+3\vec{z}_1]})^{-1}(E_{3,[\vec{z}_3\rightarrow\vec{z}_3+\frac{5}{3}\vec{z}_2]})^{-1}$$

$$=\begin{pmatrix}1&0&0\\2&1&0\\0&0&0\end{pmatrix}\begin{pmatrix}1&0&0\\0&1&0\\3&0&1\end{pmatrix}\begin{pmatrix}1&0&0\\0&1&0\\0&\frac{5}{3}&1\end{pmatrix}$$

$$=\begin{pmatrix}1&0&0\\2&1&0\\3&0&1\end{pmatrix}\begin{pmatrix}1&0&0\\0&1&0\\0&\frac{5}{3}&1\end{pmatrix}=\begin{pmatrix}1&0&0\\2&1&0\\3&\frac{5}{3}&1\end{pmatrix}=L$$

Probe: L*R=A

5.8 Determinanten

Definition: Sei U ein Vektorraum über K mit $\dim U=n>0$. Eine Funktion $D: U^n \to K$ heißt Determinantenfunktion, wenn sie folgende Eigenschaften hat.

1) D ist multilinear, d.h. linear in allen Argumenten für alle
   $1 \le i \le n, \lambda, \mu \in K, x_{1,} x_{2,} \dots, x_n, \tilde{x}_i \in U$
   $D(\vec{x}_{1,} \vec{x}_{2,} \dots, \lambda x_i + \mu \tilde{x}_i, \dots, x_n) = \lambda D(\vec{x}_{1,} \dots, x_i, \dots, x_n) + \mu D(\vec{x}_{1,} \dots, \tilde{x}_i, \dots, x_n)$
2) Sind mindestens zwei der Vektoren $\vec{x}_{1,} \dots, x_n$ gleich, d.h. $\vec{x}_i = \vec{x}_j = \vec{a}$ für ein Paar i ≠ j, so ist

   $D(\dots, \vec{a}, \dots, \vec{a}, \dots) = 0$
3) Es gibt eine Basis $\{\vec{x}_{1,} \dots, \vec{x}_n\}$ von U, so dass $D(\vec{x}_{1,} \dots, \vec{x}_n) \neq 0$

Eigenschaften einer Determinantenfunktion

1) Bei Vertauschung zweier Argumente ändert sich das Vorzeichen.
   Beweis: $0 = D(\dots, \vec{a}+\vec{b}, \dots, \vec{a}+\vec{b}, \dots)$
2) Sei $\{\vec{a}_{1,} \dots, a_n\}$ eine Basis von U und $\vec{b}_{1,} \dots, b_n \in U$. Dann gibt es eine Darstellung

   $$\vec{b}_i = \sum_{j_i=1}^{n} a_{j_i i} \vec{a}_{j_i} \quad \forall\, 1 \le i \le n$$

   und wir erhalten wegen der Multilinearität

   $$D(\vec{b}_{1,} \dots, \vec{b}_n) = \sum_{j_1=1}^{n} ¿$$

Wegen der Eigenschaft II) ist $D(a_{j_1}, \dots, a_{j_n})$ stets Null, wenn mindestens zwei Argumente gleich sind, d.h. $D(a_{j_1},\dots,a_{j_n})$ kann nur dann einen Beitrag liefern, wenn $<j_{1,}\dots,j_n>$ eine Permutation von $V_n=\{1,\dots,n\}$ ist. Wir können daher auch einfach schreiben

$$D=(\vec{b}_{1,}\dots,\vec{b}_n)=\sum \alpha_{\pi(1),1},\dots,alpha_{\pi(n),n} \quad D(a_{\pi(1)},\dots,a_{\pi(n)})$$

(Wdh. Abschnitt 4 $<S(V_n),\circ>$ asymmetrischr Gruppe der Ordnung n, $|V|=n$)

Durch sukzessives Vertauschen von jeweils 2 Elementen gelangt man von $(\vec{a}_{1,}\dots,\vec{a}_n)$ in endlich vielen Schritten zu der Permutation $(a_{\pi(1)},\dots,a_{\pi(n)})$. Bei jeder Vertauschung ändert sich das Vorzeichen von D

$$\Rightarrow D(\vec{a}_{\pi(1)},\dots,\vec{a}_{\pi(n)})=sgn(\pi)D(\vec{a}_{1,}\dots,\vec{a}_n)$$
$$\Rightarrow D(\vec{b}_{1,}\dots,\vec{b}_n)=\sum_{\pi\in S_n} sgn(\pi)\alpha_{\pi(1),1}\dots\alpha_{\pi(n),n} \quad D(\vec{a}_{1,}\dots,\vec{a}_n)$$

Satz: Sei $\{\vec{a}_{11,}\dots,\vec{a}_n\}$ eine Basis von $U,\vec{b}_{1,}\dots,\vec{b}_n\in U$ mit $\vec{b}_i=\sum_{j=1}^{n}\alpha_{ji}\vec{a}_j \quad 1\le i\le n$. Dann ist jede Determinantenfunktion $D:U^n\rightarrow K$ von der Gestalt

(*) $D(\vec{b}_{1,}\dots,\vec{b}_n)=c\cdot\sum_{\pi\in S(V_n)} sgn(\pi)\alpha_{\pi(1),1},\alpha_{\pi(2),2}\dots\alpha_{\pi(n),n}$

mit $c\in K,c\neq 0$ und umgekehrt jede durch (*) definierte Funktion ist eine Determinantenfunktion:

Beweis: Wir müssen nur noch zeigen, dass (*) eine Determinantenfunktion definiert. Dazu müssen wir die Eigenschaften i), ii) und iii) nachrechnen.

3) Ist $\{\vec{x}_{1,}\dots,\vec{x}_n\}$ linear unabhängig, so ist $D(\vec{x}_{1,}\dots,\vec{x}_n)\neq 0$. Wähle in ii) $\{\vec{a}_{1,}\dots,\vec{a}_n\}=\{\vec{x}_{1,}\dots,\vec{x}_n\}$

4) Ist $\{\vec{x}_{1,}\dots,\vec{x}_n\}$ linear abhängig, so ist $D(\vec{x}_{1,}\dots,\vec{x}_n)=0$ o.B.d.A $\vec{x}_n=\sum_{i=1}^{n-1}\lambda_i\vec{x}_i$, also

$$D(\vec{x}_{1,}\vec{x}_{2,}\dots,\sum_{i=1}^{n-1}\lambda_i\vec{x}_i)=\sum_{i=1}^{n}\lambda_i D(\vec{x}_{1,}\vec{x}_{2,}\dots,\vec{x}_i)=0$$

Die Determinantenfunktion liefert also ein Kriterium zur Untersuchung der Frage, ob $\vec{x}_{1,}\dots,\vec{x}_n$ linear unabhängig in U mit $dim U=n$ ist.

Definition: Sei $A=(\alpha_{i,j})_{i=1,j=1}^{n,n}\in K^{nxn}$. Dann ist die Determinante von A, symbolisch det A, definiert durch

$$det\,A = \sum_{\pi \in S_n} sgn(\pi)\alpha_{\pi(1),1}, \alpha_{\pi(2),2} \dots \alpha_{\pi(n),n}$$

Man verwendet auch die Schreibweise

$$det\begin{pmatrix} a_1 & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} \text{ bzw. } \begin{vmatrix} a_1 & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{vmatrix}$$

Bezeichnen wir mit $\vec{s}_{1,} \dots, \vec{s}_n$ die Spaltenvektoren von A, so ist $det(A) = D(\vec{s}_{1,} \dots, \vec{s}_n)$ mit der Festlegung $D(\vec{e}_{1,} \dots, \vec{e}_n) = 1$.

Beispiele:

n=1: $det(\alpha_{11}) = \alpha_{11}$

n=2: $det\begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix}$: $V = \{1,2\}, \pi = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \pi = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \rightarrow det\begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix} = \alpha_{1,1}\alpha_{2,2} - \alpha_{2,1}\alpha_{1,2}$

n=3: $det\begin{pmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} \\ \alpha_{21} & \alpha_{22} & \alpha_{23} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} \end{pmatrix}$:

$V = \{1,2,3\}, \pi = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \pi = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \pi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \pi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},$

$\pi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \pi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

$$det\begin{pmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} \\ \alpha_{21} & \alpha_{22} & \alpha_{23} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} \end{pmatrix} = \alpha_{11}\alpha_{22}\alpha_{33} - \alpha_{11}\alpha_{32}\alpha_{23} - \alpha_{21}\alpha_{12}\alpha_{33} + \alpha_{21}\alpha_{32}\alpha_{13} + \alpha_{31}\alpha_{12}\alpha_{23} - \alpha_{31}\alpha_{22}\alpha_{13}$$

- $A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ $det\,A = 0$, d.h. die Spalten von A sind linear abhängig, d.h. A ist nicht invertierbar
- $A = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} det\,A = 2 \cdot 2 - 1 \cdot 1 = 3$, d.h. A ist inverbar

Satz: Der Einfluss von elementaren Zeilenumformungen auf Matrizen

i) Das Vertauschen zweier Zeilen kehrt das Vorzeichen der Determinante um.
ii) Die Addition des λ -fachen einer Zeile zu einer anderen ändert sich die Determinante nicht.
iii) Multipliziert man eine Zeile mit einem Faktor $\lambda \in K$, so gilt

$$det(\vec{x}_1, \dots, \lambda \vec{x}_i, \dots, \vec{x}_n) = det(\vec{x}_1, \dots, \vec{x}_i, \dots, \vec{x}_n)$$

Beweis:

i) und iii) folgen sofort aus der Definition und den Eigenschaften der Determinantenfunktion.
zu ii): $det(\vec{z}_1, \dots, \vec{z}_i + \lambda \vec{z}_j, \dots, \vec{z}_n) = det(\vec{z}_1, \dots, \vec{z}_i, \dots, \vec{z}_n) + \underbrace{det(\vec{z}_1, \dots, \lambda \vec{z}_j, \dots, \vec{z}_n)}_{0}$

Jetzt können wir auf eine Matrix wieder den Gaußschen Algorithmus anwenden. Bei den meisten Operationen ändert sich die Determinante nicht. Das Verfahren endet sofort, wenn wir bei unseren Umwandlungen auf eine ohne Pivotelement ≠ 0 stoßen. Denn das kann in einer n x n Matrix nur der Fall sein, wenn der Rang kleiner als n ist, d.h. die Zeilen sind linear abhängig und damit ist die Determinante gleich Null.

Ist der Rang von A gleich n, so erhalten wir unter Verwendung der elementaren Zeilenumformungen

$$det\, A = \pm det\, A \begin{pmatrix} a_{11} & . & . & . \\ 0 & . & . & . \\ 0 & . & . & a_{nn} \end{pmatrix}$$

durch weitere Zeilenumformungen erhalten wir $det\, A = \pm \alpha_{11} \alpha_{22} \dots \alpha_{nn} \cdot \underbrace{det \begin{pmatrix} 1 & . & 0 \\ . & . & . \\ 0 & . & 1 \end{pmatrix}}_{1}$

Satz: (Multiplikationssatz für Determinanten)

Für Matrizen $A, B \in K^{nxn}$ gilt $det(A \cdot B) = det(A) det(B)$

Beweis: Sind $\vec{a}_1, \dots, \vec{a}_n$ die Spaltenvektoren der Matrix, so sind $B\vec{a}_1, B\vec{a}_2, \dots, B\vec{a}_n$ die Spaltenvektoren des Matrizenproduktes BA. Bei festgehaltener Matrix B ist daher

$$det(BA) = det(B\vec{a}_1, B\vec{a}_2, \dots, B\vec{a}_n) = \sum_{\pi \in S_n} b_{\pi(1),1} \dots b_{\pi(n),b} \cdot det(\vec{a}_1, \dots, \vec{a}_n) = det(B) det(A)$$

Folgerung: Da $det(E) = 1$, gilt mit $A^{-1} A = E$
$1 = det(A^{-1} A) = det(A^{-1}) det(A)$ $det(A^{-1}) = (det\, A)^{-1}$

Satz: für $A \in K^{nxn}$ gilt $det(A) = det(A^T)$
Beweis: Es gilt für $A = (a_{ij})_{i=1,j=1}^{n,n}$ und $A^T (a_{ji})_{i=1,j=1}^{n,n}$.
$det(A) = \sum_{\pi \in S_n} sgn(\pi) a_{\pi(1),1} a_{\pi(2),2} \dots a_{\pi(n),n} = \sum_{n \in S_n} sgn(\pi) \prod_{i=1}^{n} a_{\pi(i),i}$. Sei π^{-1} die inverse

Permutation von π . Wir haben dann

$$\prod_{i=1}^{n} a_{\pi(i),i} = \prod_{i=1}^{n} a_{\pi^{-1}(\pi(i)),\pi^{-1}(i)} = \prod_{i=1}^{n} a_{i,\pi^{-1}(i)}$$

weiter ist wegen $sgn(\pi)\cdot sgn(\pi^{-1}) = sgn(\pi\circ\pi^{-1}) = 1$, d.h. $sgn(\pi) = sgn(\pi^{-1})$ und wir erhalten

$$det(A) = \sum_{\pi\in S_n} sgn(\pi^{-1}) \prod_{i=1}^{n} a_{i,\pi^{-1}(i)} = \sum_{\pi\in S_n} sgn(\pi) \prod_{i=1}^{n} a_{i,\pi(i)} = det(A^T)$$

Satz: (Entscheidungssatz von Laplace)

Für $A\in K^{nxn}$ bezeichne $A_{jk}\in K^{(n-1)x(n-1)}$

$$A_{j,k} = \begin{pmatrix} a_{11} & \dots & a_{1k} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{i1} & \dots & a_{ik} & \dots & a_{\text{¿}} \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & \dots & a_{nk} & \dots & a_{nn} \end{pmatrix}$$

die aus A durch Streichung der i-ten Zeile und k-ten Spalte entsteht. Dan gilt (Entwicklung nach der ersten Zeile)

$$det(A) = \sum_{k=1}^{n} (-1)^{1+k} a_{1,k} \cdot det A_{1,k}$$

Beweis:

$$det(A) = \sum_{\pi\in S_n} sgn(\pi) a_{\pi(1),1} a_{\pi(2),2} \dots a_{\pi(n),n}$$

$$= \sum_{k=1}^{n} a_{1,k} \sum_{\pi} (2)\dots\pi(n) sgn(k,\pi(2),\pi(3)\dots\pi(n)) a_{\pi(2),2}\dots a_{\pi(n),n}$$

Nun gilt:

$$sgn(k,\pi(2),\dots,\pi(n)) = (-1)^{k-1} sgn(\pi(2),\pi(3)\dots\pi(k-1),k,\pi(k+1)\dots\pi(n))$$

$$= (-1)^{k-1} sgn(\pi(2),\pi(3),\dots,pi(k-1),\pi(k+1),\dots\pi(n))$$

und damit

$$det(A) = \sum_{k=1}^{n} a_{1,k} (-1)^{k-1} det(A_{1,k})$$

Bemerkung: Analog erhält man für die Entwicklung nach der i-ten Zeile bzw. k-ten Spalte

$$det(A)=\sum_{k=1}^{n}(-1)^{i+k}a_{i,k}det(A_{ik})=\sum_{i=1}^{n}(-1)^{i+k}a_{i,k}det(A_{ik})$$

Beispiel:

n=2

$$A=\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

$$det(A)=a_{11}a_{22}-a_{12}a_{21}$$
$$det(A)=a_{21}a_{12}+a_{22}a_{11}$$
$$det(A)=a_{22}a_{11}+a_{21}a_{12}$$

n=3

Entwicklung nach der 1. Zeile:

$$\begin{vmatrix} 1 & 0 & 2 \\ 2 & -2 & 3 \\ 4 & 1 & 8 \end{vmatrix}=1\cdot\begin{vmatrix} -2 & 3 \\ 1 & 8 \end{vmatrix}+2\begin{vmatrix} 2 & -2 \\ 4 & 1 \end{vmatrix}=(1)(-19)+2\cdot 10=1$$

Entwicklung nach der 2. Spalte

$$\begin{vmatrix} 1 & 0 & 2 \\ 2 & -2 & 3 \\ 4 & 1 & 8 \end{vmatrix}=(-2)\cdot\begin{vmatrix} 1 & 2 \\ 4 & 8 \end{vmatrix}+(-1)\begin{vmatrix} 1 & 2 \\ 2 & 3 \end{vmatrix}=(-2)(0)+(-1)(-1)=1$$

Satz: (Cramersche Regel)

Ist $A=(\vec{a_1},\dots,\vec{a_n})\in K^{nxn}$ eine invertierbare Matrix mit den Spaltenvektoren $\vec{a_k}$, so lässt sich die (eindeutige bestimmte) Lösung einer linearen Gleichungssystems $A\vec{x}=\vec{b}$ $\vec{b}\leftarrow K^n$ angegeben durch

$$x_k=\frac{det(\vec{a_1},\dots,\vec{a_{k-1}},\vec{b},\vec{a_{k+1}},\dots,a_n)}{det(\vec{a_1},\dots,\vec{a_{k-1}},\vec{a_k},\vec{a_{k+1}},\dots,a_n)}$$

Beweis:

$$A\vec{x}=\vec{b}\Leftrightarrow\vec{b}=\sum_{k=1}^{n}x_k\vec{a}_k$$

$$det(\vec{a}_{1,} \ldots, \vec{a}_{k-1}, \vec{b}, \vec{a}_{k+1}, \ldots, a_n) = det(\vec{a}_{1,} \ldots, \vec{a}_{k-1}, \sum_{k=1}^{n} x_k \vec{a}_k, a_{k+1}, \ldots, a_n)$$

$$= \sum_{j=1}^{n} x_j \underbrace{det(a_{1,} \ldots, a_{k-1}, a_j, a_{k+1}, \ldots, a_n)}$$

Bemwerkung: Die Cramersche Regel ist vor allem für theoretische Untersuchungen brauchbar. Für numerische Auswertung ist sie i.a. zu aufwändig.

Beispiel:

$$\begin{array}{l} x_1 + 2x_2 = 2 \\ 2x_1 - x_2 + x_3 = 1 \\ 3x_1 + 2x_2 + x_3 = 0 \end{array} \qquad A = \begin{pmatrix} 1 & 2 & 0 \\ 2 & -1 & 1 \\ 3 & 2 & 1 \end{pmatrix} \quad \vec{b} = \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix}$$

$$det(A) = 1 \cdot \begin{vmatrix} -1 & 1 \\ 2 & 1 \end{vmatrix} - (2) \begin{vmatrix} 2 & 1 \\ 3 & 1 \end{vmatrix} = 1 \cdot (-3) + (-2) \cdot (-1) = -1$$

$$x_1 = \frac{1}{-1} \begin{vmatrix} 2 & 2 & 0 \\ 1 & -1 & 1 \\ 0 & 2 & 1 \end{vmatrix} = (-1) \left((-1) \begin{vmatrix} -1 & 1 \\ 2 & 1 \end{vmatrix} + (-2) \begin{vmatrix} 1 & 1 \\ 0 & 1 \end{vmatrix} \right) = 8$$

$$x_2 = \frac{1}{-1} \begin{vmatrix} 1 & 2 & 0 \\ 2 & 1 & 1 \\ 3 & 0 & 1 \end{vmatrix} = (-1) \left((+1) \begin{vmatrix} 1 & 1 \\ 0 & 1 \end{vmatrix} + (-2) \begin{vmatrix} 2 & 1 \\ 3 & 1 \end{vmatrix} \right) = 3$$

$$x_3 = \frac{1}{-1} \begin{vmatrix} 1 & 2 & 2 \\ 2 & -1 & 1 \\ 3 & 2 & 0 \end{vmatrix} = (-1) \left((+3) \begin{vmatrix} 2 & 2 \\ -1 & 1 \end{vmatrix} + (-2) \begin{vmatrix} 1 & 2 \\ 2 & 1 \end{vmatrix} \right) = -18$$