Skript

Lineare Algebra I

WS

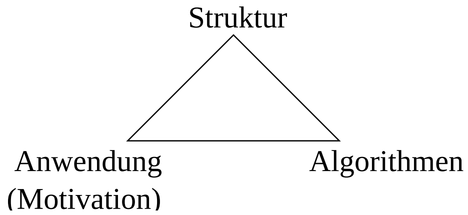
2000/2001

8. Dezember 2000

Inhaltsverzeichnis

1 Mengen/Abbildungen

• Inhalt und Ziel



• Mengentheoretische Sprechweise

Eine Menge besteht aus wohldefinierten (alles muss sich innerhalb einer "Grundmenge" abspielen) Elementen. Man beschreibt sie

1. Alle Elemente der Menge aufzählen
2. oder die Eigenschaften der Elemente aufzählen (wobei man auf Widersprüche achten muß)

1.1 Beispiel

Grundmengen:

- $\mathbb{N}$:= Menge der natürlichen Zahlen $\{1, 2\ldots\}$
- $\mathbb{R}$:= Menge der reellen Zahlen
- $\mathbb{Z}$:= Menge der ganzen Zahlen $\{..., -1, 0, 1...\}$
- $M = \{2, 4, 6\}$ (Aufzählung der Elemente (Bsp. zu 2b s.o.)
- $M = \{n \in \mathbb{N} | 2 \leq n \leq 6, 2|n\}$
- $\mathbb{Q}$:= Menge der rationalen Zahlen $\{\frac{a}{b}|a, b \in, b \neq 0\}$

1.2

1. Ist M eine *Menge* und m ein *Element* von M, so schreiben wir $m \in M$.Wenn m kein *Element* von M ist, so schreiben wir $m \notin M$
2. Zwei Mengen M_1 und M_2 heissen *gleich*, falls sie dieselben Elemente enthalten.Für jedes m (aus der umfassenden Grundmenge) gilt : $m \in M_1 \leftrightarrow m \in M_2$ (Notation : $M_1 = M_2$)
3. M und T seien Mengen. T heisst *Teilmenge* von M, falls jedes $t \in T$ auch Element von M ist. (Notation : $T \subseteq M$) Insbesondere : $\emptyset \subseteq M$ ($\emptyset$: leere Menge also Menge ohne Elemente).
4. Für jede Menge M heisst $\mathrm{Pot}(M) := \{T|T \subseteq M\}$ (also Menge aller Teilmengen von M) die *Potenzmenge* von M

Russel:
($M := \{X|X \notin X\}$ (*ohne* Definition einer Grundmenge wie z.B. $X \in \mathbb{N}$ führt zu einem Widerspruch da :

1. $M \in M \rightarrow M \notin M$
2. $M \notin M \rightarrow M \in M$

1.3 Definition

M Menge, $T_1, T_2 \subseteq M$ (auch: $T_1, T_2 \in Pot(M)$):

1. $T_1 \bigcap T_2 = \{m \in M | m \in T_1$ und $m \in T_2\}$ heißt *Durchschnitt* von T_1 und T_2.
   Für jede Menge U von Teilmengen von M,$U \subseteq Pot(M)$ ist der Durchschnitt definiert als $\bigcap\limits_{T \in U} := \{m \in M | m \in T$ für alle $T \in U\}$.
2. $T_1 \bigcup T_2 := \{m \in M | m \in T_1$ oder $m \in T_2\}$ heißt *Vereinigung* von T_1 und T_2. Für U (wie oben definiert) $\bigcup\limits_{T \in U} := \{m \in M | m \in T$ für mindestens ein $T \in U\}$ (Es existiert ein $T \in U$ mit $m \in T$).
3. $T_1 - T_2 := \{m \in M | m \in T_1$ und $m \notin T_2\}$ heißt die *Differenzmenge* von T_1 und T_2.

1.4 Definition

Seien M und N Mengen:

1. Für $m \in M$ und $n \in N$ bezeichnet $(m,n) := \{\{m\},\{m,n\}\}$ das *geornete Paar* der Elemente.
2. $M \times N := \{(m,n) | m \in M, n \in N\}$ heisst das *kartesische Produkt* von M und N oder auch die *Paarmenge*.

1.5

Für $(m_1,n_1),(m_2,n_2) \in (M \times N)$ gilt :
$(m_1,n_1) = (m_2,n_2) \Leftrightarrow m_1 = m_2$ und $n_1 = n_2$

• Abbildungen

1.6 Definition

M,N Mengen:

1. Vorläufige Definition von *Abbildungen* :
   Eine *Abbildung* oder *Funktion* f von M nach N ist eine Zuordung, die jedem Element $m \in M$ ein eindeutiges Element $n \in N$ zuordnet. Das zugeordnete Element n wird mit $f_{(m)}$ bezeichnet. $f : M \to N$ oder $f : M \to N : m \longmapsto f_{(m)}$
2. Dabei heisst M *Definitionsbereich* und N *Wertebereich*
   Für $T \subseteq M$ heisst $f_{(T)} := \{f_{(m)} | m \in T\}(\subseteq N)$ das *Bild* von T unter f. Im Falle $T = M$ heisst $f_{(M)} =:$ *Bild* von f.
3. Die Menge aller Abbildungen von $M \to N$ wird mit N^M bezeichnet.
   $(f : M \to N \Leftrightarrow f \in N^M)$

1.7 Definition

Sei M eine Menge:

1. Jeder Teilmenge $T \subseteq M$ von M legt eine Abbildung $\chi_T : M \to \{0,1\}$ fest durch :
   $\chi_{T(m)} = 1 \Leftrightarrow m \in T$
   $\chi_{T(m)} = \begin{cases} 1 & m \in T \\ 0 & m \notin T \end{cases}$
   χ_T heisst die charakteristische Funktion von T

2. Jede Abbildung $\chi : M \to \{0,1\}$ legt eine Teilmenge T von M fest :
   $T := \{m \in M | \chi_{(m)} = 1\}$, so dass $\chi = \chi_T$

1.8 Beispiel

1. (Motiv der Bezeichnung N^M)
   Sei $M = \{1,2\} = \underline{2}$ und $N = \{0,1,...,9\} = \underline{9}$
   $f : M \to N$ festgelegt durch f_1 und f_2
   Interpretation : Zahl zwischen $0 = 00$ und 99
   $|N^M| = |N|^{|M|} = 10^2 = 100$ Elemente ($|X| :=$ Anzahl der Elemente von X)
2. (X^n),X Menge,$n \in \mathbb{N}$
   $X^n := X^{\underline{n}} =$ Menge der Abbildungen von $\underline{n} = \{1,2,..,n\}$ nach X $X^n =$ Menge der Folgen der Länge n mit Werten in X
   $\Rightarrow f = (f_{(1)}, f_{(2)}, .., f_{(n)}) = (f_1, f_2, ..., f_n)$ (manchmal ohne die Klammern geschrieben.
   $X = \{0,1\}$
   $(0,0,1) \neq (1,0,0) \in X^3$ (Reihenfolge beachten!)
3. (Matrizen,endliche Doppelfolgen) $X^{n \times m}$
   $m, n \in \mathbb{N}$,X Menge.
   Eine Abbildung $A : \underline{m} \times \underline{n} \to X : (i,j) \longmapsto A_{ij} = A_{(i,j)}$ heisst eine X-wertige Doppelfolge oder $m \times n$*-Matrix*
   Schreibweise: $A = \begin{pmatrix} A_{1,1} & \dots & A_{1,n} \\ \vdots & \ddots & \vdots \\ A_{m,1} & \dots & A_{m,n} \end{pmatrix}$
4. (Unendliche Folgen $X^{\mathbb{N}}$)
   Abbildung $\alpha : \mathbb{N} \to X : i \longmapsto \alpha_i = \alpha_{(i)}$ heissen auch X*-wertige Folgen.*
   Schreibweise : $\alpha = (\alpha_1, ..), \alpha \in X^{\mathbb{N}}$
5. (Polynomfunktion) Eine *reelle Polynomfunktion*
   f ist eine Abbildung $f : \mathbb{R} \to \mathbb{R}$ für die ein $n \in \mathbb{N}$ und reelle Zahlen $a_0, a_1, a_1, \dots, a_n \in \mathbb{R}$ mit
   $f_{(x)} = a_0, a_1x, a_1x_1^2, \dots, a_nx_n^n$ (für alle $x \in \mathbb{R}$)
   z.B.: $f : \mathbb{R} \to \mathbb{R} : x \leftrightarrow x^2$ wobei der Graph zu f die Normalparabel darstellt.

1.9 Bemerkung

Bemerkung : Ist $f : M \to N$ eine Abbildung, so gilt :

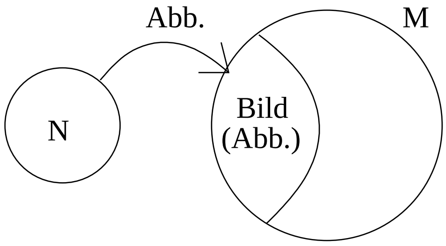
1. $\text{Graph}_{(f)} := \{(m, f_{(m)}) | m \in M\} \subseteq M \times N$
2. Zu jedem $m \in M$ gibt es genau ein $n \in N$ mit
   $(m,n) \in \text{Graph}_{(f)}$,d.h.
   (a) zu jedem $m \in M$ existiert ein $n \in N$ mit $(m,n) \in \text{Graph}_{(f)}$ und
   (b) Sind für $m \in M$ die Paare $(m,n),(m,n') \in \text{Graph}_{(f)}$
   $(n,n' \in \mathbb{N}) \to n = n'$
   umgekehrt klar :
   Teilmenge von $M \times N$ mit 2a und 2b (s.o.) legen eindeutig eine Abbildung $M \to N$ fest

1.10 Definition

Eine Abbildung $f : M \to N$ der Menge M in die Menge N ist eine Teilmenge $f \subseteq M \times N$ mit der Eigenschaft :
Für jedes $m \in M$ existiert ein $n \in N$ mit $(m,n) \in f$.Falls $(m,n) \in f$, schreiben wir $f_{(m)} = n$

1.11 Beispiel

1. Sei S eine Menge. Die sogenannte Diagonale
   $\triangle_{(S)} = \{(s,s)|s \in S\} \subseteq S \times S$ ist eine Abbildung von S in sich. Diese Abbildung wird *Identitä tsabbildung* von S genannt.
   Bezeichnung : $Id_S : S \to S : s \longmapsto s$
   Allgemein : $\emptyset \neq T \subseteq S \Rightarrow \{(s,s)|s \in T\} \subseteq T \times S$ ist eine Abbildung von T nach S und wird als die *Einbettung* von T in S bezeichnet.
   $\iota = \iota_{T,S} : T \to S : t \longmapsto t$



2. M, N Mengen,$n \in N \Rightarrow M \times \{n\} (\subseteq M \times N)$ ist eine Abbildung, die mit bezeichnet wird und heisst *konstante Abbildung*
3. Ist $f : M \to N$ und $\emptyset \neq T \subseteq M$
   $\Rightarrow f_{/T} : f \cap (T \times N)$ ist eine Abbildung von T nach N
   $f_{/T} : T \to N : t \longmapsto f_{(t)}$
   $f_{/T}$ heisst die *Einschränkung* von f auf T

1.12 Lemma

Seien $f_i : S \to T$ und $g : T \to U$ Abbildungen
$\Rightarrow g \circ f := gf := \{(s,u) \in S \times U|$ es existiert ein $t \in T$ mit $(s,t) \in f$ und $(t,u) \in g\}$ ist eine Abbildung von S nach U :
$g \circ f : S \to U$
Beweis: $g \circ f \subseteq S \times U \surd$.
Sei $s \in S \Rightarrow$ es existiert ein $t \in T$ mit $(s,t) \in f$
$(t = f_{(s)})$
g auch eine Abbildung
$\Rightarrow$ es existiert ein $u \in U$ mit $(t,u) \in g$
$(u = g_{(t)})$
$\Rightarrow (s,u) \in g \circ f$ (Nachweis der Existenz $\surd$)
Eindeutigkeit :
$(s,u), (s,u') \in g \circ f \Rightarrow$ es existiert ein $t \in T$ mit
$(s,t) \in f$,
$(t,u) \in g$ und $t' \in T$ mit $(s,t') \in f, (t',u') \in g$
f Abbildung $\Rightarrow t = t' \underbrace{\Rightarrow}_{gAbb} u = u'$ q.e.d

1.13 Definition

Die in 1.12 Definierte Abbildung $g \circ f : S \to U : s \longmapsto g_{(F_{(s)})}$ heisst die *Komposition* (oder Hintereinanderausfürung) von f mit g.

1.14 Beispiel

1. Ist $f : M \to N$ eine Abbildung und $\emptyset \neq T \subseteq M$ mit zugehörender Einbettung ${}^{\iota:T \longrightarrow M}_{\quad t \longmapsto t}$
$\Rightarrow$ Einschränkung $f_{/T} = f \circ \iota$ (ι : Einbettung)
2. Für $n \in \mathbb{N}$ mit $z \in \mathbb{Z}$ bezeichnet "z mod n" (sprich z modulo n) die eindeutige Zahl $r \in \mathbb{Z}$ $0 \leq r < n$ mit $z = \underline{q}n + r$ für ein $q \in \mathbb{Z}$ den kleinsten nicht negativen Rest, der beim dividieren von z durch n bleibt.
$\mu_1 : \mathbb{Z} \to \mathbb{Z} : z \longmapsto z \text{ mod } n$
$\Rightarrow \mu_n \circ \mu_n = \mu_n$
3. Visualisierung : $M\ M \to M := M$
$\alpha : \{0, 1, \ldots, 11\} \to \{0, 1, \ldots, 11\}$:
$x \longmapsto (x^2 + 1) \text{ mod } 12$
$0 \longmapsto 1 \longmapsto 2 \longmapsto 5 \longmapsto 2$ (σ-Allgorithmus) $3 \longmapsto 10 \longmapsto 5 \longmapsto 2$
4. $A = \begin{pmatrix} A_{1,1} & \ldots & A_{1,n} \\ \vdots & \ddots & \vdots \\ A_{m,1} & \ldots & A_{m,n} \end{pmatrix} : \underline{m} \times \underline{n} \to X$ sei eine Matrix
$A_{-i} = \begin{pmatrix} A_{1,i} \\ \vdots \\ A_{m,i} \end{pmatrix}$ " ite-Spalte von A "
Formel :
$\sigma_i : \underline{m} \times \underline{1} \to \underline{m} \times \underline{n} : (\alpha, 1) \longmapsto (a, i)$ Abbildung ite Spalte von $A := A \circ \sigma_i (i \leq i \leq n)$

1.15 Satz

A, B, C, D Mengen, $\alpha : A \to B, \beta : B \to C, \gamma : C \to D$ Abbildung
$\Rightarrow (\gamma \circ \beta) \circ \alpha = \gamma \circ (\beta \circ \alpha)$
Man beachte $\gamma \circ \beta : B \to D, \beta \circ \alpha : A \to C$, so dass beide Seiten wohldefiniert.
Beweis : Sei $a \in A$
Einerseits : $((\gamma \circ \beta) \circ \alpha)(a) = (\gamma \circ \beta)(\alpha_{(a)}) = \gamma(\beta(\alpha_{(a)}))$
Andererseits : $(\gamma \circ (\beta \circ \alpha))(a) = \gamma((\beta \circ \alpha)(a)) = \gamma(\beta(\alpha_{(a)}))$
a beliebig aus $A \Rightarrow$ Behauptung q.e.d.

1.16 Definition

Eine Abbildung $f : M \to N$ heisst *bijektiv*, falls $g := \{(n, m) \in N \times M | (m, n) \in f\}$ eine Abbildung von N nach M ist. In diesem Fall heisst g die zu f inverse Abbildung oder auch die Umkehrabbildung von f und wird mit f^{-1} bezeichnet.
Klar :
$f : M \to N$ ist bijektiv $\Rightarrow f^{-1} : N \to M$ auch bijektiv und
$(f^{-1})^{-1} = f$ und $f^{-1} \circ f = \text{Id}_M$(Identität) und $f \circ f^{-1} = Id_N$

1.17 Beispiel

1. M endliche Menge. Pot(M) (Potenzmenge von M)
1.7 : $\chi : \text{Pot}(M) \to \{0, 1\}^M : T \longmapsto \chi_T$ ist eine Bijektion
2. Eine nicht leere Menge M heisst endlich,falls ein $n \in \mathbb{N}$ existiert und eine Bijektion $\zeta : M \to \{1, \ldots, n\} = \underline{n}$. Man schreibt auch $|M| = n$ und nennt n die Anzahl der Elemente von M oder die *Kardinalität* von M.
$|\emptyset| := 0$ (Herstellen von ζ = Zählen)

3. Eine nicht endliche Menge M heisst abzählbar, falls eine Bijektion $\alpha : M \to \mathbb{N}$ existiert (z.B. Georg Cantor) :
   $\mathbb{N} \times \mathbb{N}$ ist abzählbar. (nach 1. Cantorschen Diagonalverfahren nachweisbar) Pot($\mathbb{N}$)$\in, \mathbb{R}$ nicht abzählbar (nach 2. Cantorschen Prinzip zu beweisen)
4. $\nu\{0, 1, \ldots, 11\} \to \{a, b, \ldots, l\}$ bijektiv
   $0 \longmapsto a$, $1 \longmapsto b$,...
   $\nu \circ \alpha \circ \nu^{-1}$
   Beweis : $(\nu \circ \alpha \circ \nu^{-1}) \circ (\nu_{(i)}) = \nu(\alpha_{(i)})$
   Übergang von α zu $\nu \circ \alpha \circ \nu^{-1}$: Abbilden von Abbildungen
5. Vergleich von $\underset{(m,n)}{M\times M}$ und $\underset{(m,n)}{M^2}$ $m, n \in M$
   $M \times M \to M^2 : \{\{m\}, \{m, n\}\} \longmapsto \{(1, m), (2, n)\}$ ist bijektiv. In Zukunft identifizieren wir $M \times M$ mit M^2,d.h. obige Abbildung wird als Identität angesehen.

1.18 Definition

Sei $f : M \to N$ eine Abbildung:

1. Für $n \in N$ heisst $f^{-1}_{(\{n\})} := \{m \in M | f_{(m)} = n\}$ die *Faser* von f über n oder das volle Urbild von n in M
   (<u>VORSICHT</u> : dieses $f^{-1}_{(\{\})}$ nicht mit Umkehrabbildung verwechseln!)
2. f heisst *injektiv* oder*eineindeutig*,falls jede Faser von F aus höchstens einem Element besteht.D.h. zu jedem $n \in N$ existiert höchstens ein $m \in M$ mit $f_{(m)} = n$
3. f heisst *surjektiv* oder eine Abbildung *auf* N, falls keine Faser von f leer ist, d.h. zu jedem $n \in N$ existiert $m \in M$ mit $f_{(m)} = n$

1.19 Beispiel

1. Sei $T \subseteq M \Rightarrow$ Einbettung
   $\iota_T : T \to M : t \longmapsto t$ ist injektiv

2. Sei M endlich , $M \neq \emptyset \Rightarrow$
   $|| :$ Pot $(M) \to \underline{|M|} \bigcup \{0\} = \{0, 1, \ldots, \mathbb{N}\}$
   $T \longmapsto |T|$
   Ist eine surjektive Abbildung (Fasern von n =Pot$_n(M) = \{T \subseteq M | |T| = n\}$)

1.20 Lemma

Sei $\alpha : M \to N$ Abbildung. Es gilt

1. Ist α injektiv $\Rightarrow$ es existiert eine Abbildung $\beta : N \to M$ mit $\beta \circ \alpha = \mathrm{Id}_M$. Jedes derartige β heisst *Linksinverses* von α.
2. Ist α surjektiv $\Rightarrow$ es existiert eine Abbildung $\gamma : N \to M$ mit $\alpha \circ \gamma = \mathrm{Id}_N$. Jedes derartige γ heisst *Rechtsinverses* von α.

Beweis:

1. $\alpha : \mathbb{R} \to \mathbb{R} : x \longmapsto x^2$
   $\alpha_{(3)} = \alpha_{(-3)} \Rightarrow$ nicht injektiv $-1 \notin \text{Bild}_{(\alpha)} \to$ nicht surjektiv
2. $\alpha 1 \mathbb{R} \to \mathbb{R}_{\geq 0} : x \longmapsto x^2$ nicht injektiv aber surjektiv
3. $\gamma : \mathbb{R}_{\geq 0} \to \mathbb{R} : x \longmapsto \sqrt{x}$
4. $\epsilon : \mathbb{R} \to \mathbb{R} : x \to x^3$ ist bijektiv
5. $\nu : \mathbb{R} \to \mathbb{R} : x \to 3x + 7$ ist bijektiv
6. $\text{Pot}_{(M)} \to \{0,1\}^M : T \to \chi_T$ bijektiv
   Beweis :
   (a) injektiv : $T = T' \Rightarrow \chi_T = \chi_{T'}$
   (b) surjektiv : $\chi : M \to \{0,1\}$ existiert ein T mit $T \subseteq M$ und $\chi_T = \chi$?
   Ja : $T = \{m \in M | X_{(m)} = 1\} \Rightarrow \chi_T = \chi$(volles Urbild) $(X_{(m)} := \chi^{-1}(\{1\}))$
   $\{0,1\}^M \to \text{Pot}_{(M)}$
   $\chi \longmapsto \chi^{-1}_{(\{1\})}$

Abbildung 1: Zusatz Beispiele zu Surjektiv/Injektiv

1. Für $n \in N$ mit $n \in \alpha_{(M)}$ existiert genau ein $m \in M$ mit
   $\alpha_{(m)} = n$
   Definiere $\beta_{(n)} = m$
   Für $n \in N - \text{Bild}_{(\alpha)} = m$
   $m \in M \Rightarrow \beta_{(\alpha_{(m)})} = m$ d.h. $\beta \circ \alpha = \text{Id}_M$ Da id_M surjektiv $\Rightarrow \beta$ surjektiv q.e.d.
2. Übung

1.21 Beispiel

$\_ : \mathbb{N} \to \text{Pot}_{endlich}(\mathbb{N}) - \{\emptyset\} : n \longmapsto \underline{n} = \{1, 2, \ldots, n\}$ ist injektiv und
$|| : \text{Pot}_{endlich}(\mathbb{N}) - \{\emptyset\} \to \mathbb{N} : M \longmapsto |M|$ ist surjektiv, denn
$|| \cdot \_ = \text{Id}_{\mathbb{N}}$

1.22 Satz

Sei M eine Menge : Folgende Aussagen sind äquivalent :

1. M endlich
2. Jede injektive Abbildung $\eta : M \to M$ ist surjektiv
3. Jede surjektive Abbildung $\tau : M \to M$ ist injektiv

Beispiel:

1. 1. $\Rightarrow$ 2. :
   Sei $|M| = n$ und $M = \{m_1, \ldots, m_n\}$ und $\eta : M \to M$ injektiv
   η inj.

$\Rightarrow |\eta_{(\{m_1\})}| = 1, |\eta_{(\{m_1,m_2\})}| = 2, \ldots, |\eta_{(\{m_1,\ldots,m_k\})}| = k (k = 1, 2, \ldots, n)$ (mit Induktionsbeweis zu beweisen)
$\rightarrow |\eta_{(M)}| = n = |M|$ also $\eta_{(M)} = M$, d.h. η surjektiv

2. 2. $\rightarrow$ 3.
   Sei $\mathrm{Id}_\tau : M \rightarrow M$ surjektiv und nach 1.20 2 $\rightarrow$
   $\eta : M \rightarrow M$ mit $\tau \circ \eta = \mathrm{Id}_M$ und η ist injektiv $\Rightarrow$ η surjektiv $\Rightarrow$ η bijektiv und $\tau = \eta^{-1}$ ist injektiv.
3. 3. $\Rightarrow$ 1.
   Zeige nicht 1. $\rightarrow$ nicht 3.
   Also Annahme:
   M nicht endlich
   $\Rightarrow$ es existiert eine injektive Abbildung $f : \mathbb{N} \rightarrow M$, also eine Folge $f_1, f_2, f_3, \ldots$ mit $f_i \neq f_j$ für $i \neq j$. Benutze diese Folge um eine Abbildung von $\mathbb{N} \rightarrow \mathbb{N}$, die surjektiv aber nicht injektiv ist, auf M zu übertragen.
   Klar : $\alpha : \mathbb{N} \rightarrow \mathbb{N} : i \longmapsto \begin{cases} i-1 & i > 1 \\ 1 & i = 1 \end{cases}$ surjektiv aber nicht injektiv
   Übertragung :
   $\tau : M \rightarrow M : m \longmapsto \begin{cases} f_{i-1} & \text{falls } m = f_i \text{ für ein } i > 1 \\ f_1 & m = f_1 \\ m & m \notin f_{(\mathbb{N})} \end{cases}$
   τ wohldefiniert (da f injektiv). τ surjektiv aber nicht injektiv q.e.d.

• Lineare Gleichungssysteme 1

1.23 Beispiel

Gesucht sind alle $(x, y, z) \in \mathbb{R}^3$ mit $3x + 7x^2 + 14xz = 7(x+z)^2 - 3 + y - 7z^2$
$2x + 14z = 7(x+z) - 2$

$\leadsto$

$\dagger$:
$3x - y = -3$
$-5x + 7z = -2$

$\leadsto$

$$\begin{pmatrix} 3 & -1 & 0 \\ -5 & 0 & 7 \end{pmatrix}$$

$\leadsto$

$\alpha : \mathbb{R}^3 \rightarrow \mathbb{R}^2 : (x, y, z) \longmapsto (3x - y, -5x + 7z)$ $\dagger$ lösen $\Leftrightarrow$ Faser von $(-3, -2)$ unter α bestimmen.

1.24 Definition

Ein *Lineares Gleichungssystem* (über $\mathbb{R}$) mit m Gleichungen und n Unbestimmten $x_1 \ldots x_n$ ist gegeben durch :
(*):
$A_{1,1}x_1 + \ldots A_{1,n}x_n = b_1$
$A_{2,1}x_1 + \ldots A_{2,n}x_n = b_2$

$\vdots$
$A_{m,1}x_1 + \ldots A_{m,n}x_n = b_n$

wobei $A = (A_{ij)} \in \mathbb{R}^{m \times n}$ eine (gegebene) Matrix ist und $b = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \in \mathbb{R}$ eine (gegebene) Spalte ist. A heisst die *Matrix* von (*), $(A, b) \in \mathbb{R}^{m \times (n+1)}$ die *erweiterte Matrix* von (*). Dabei ist (A, b) definiert als $(A, b) : \underline{n} \times \underline{n+1} \Rightarrow \mathbb{R} : (i, j) \longmapsto \begin{cases} A_{ij} & j \in n \\ b_i & i = n+1 \end{cases}$

1.25 Definition

Sei $A : \underline{m} \times \underline{n} \to \mathbb{R} : (i, j) \longmapsto A_{i,j}$ eine reelle $m \times n$ Matrix. Kurz $A = (A_{ij}) \in \mathbb{R}^{m \times n}$ Die von A *induzierte lineare Abbildung* $\overline{A} : \mathbb{R}^{n \times 1} \to \mathbb{R}^{m \times 1} : x \longmapsto Ax$ ist definiert durch
$\overline{A}\left(\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}\right) = A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} A_{11}x_1 + \ldots + A_{1,n}x_n \\ A_{2,1}x_1 + \ldots + A_{2,n}x_n \\ \vdots + \ldots + \vdots \\ A_{m,1}x_1 + \ldots + A_{m,n}x_n \end{pmatrix}$ A_x heisst das *Produkt* der Matrix A mit der Spalte x.
Formal :
$x : \{1, \ldots, n\}x\{1\} \to \mathbb{R} : (i, j) \longmapsto x_{(i,j)}$ (Spalte) $Ax = Y$
$y_{(j,1)} = A_{(j,1)}x_{(1,1)} + A_{(j,2)}x_{(2,1)} + \ldots + A_{(j,n)}x_{(n,1)} = \sum_{i=1}^{x} A_{(j,i)}x_{(i,1)}$

1.26 Definition

Seien $a = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}, b = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \in \mathbb{R}^{m \times 1}$
Dann ist die *Summe* $a + b \in \mathbb{R}^{m \times 1}$ definiert durch :
$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} + \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} a_1 + b_1 \\ \vdots + \vdots \\ a_n + b_n \end{pmatrix}$ $(+ : \mathbb{R}^{n \times 1} \times \mathbb{R}^{n \times 1} \to \mathbb{R}^{n \times 1})$
Ist weiter $c \in \mathbb{R}$ so ist $a \in \mathbb{R}^{n \times 1}$ definiert durch
$c \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} ca_1 \\ \vdots \\ ca_n \end{pmatrix}$

1.27 Bemerkung

1. $\bar{A}_{(x)} = Ax = x_1 \cdot A_{-,1} + x_2 \cdot A_{-,2} + \ldots + x_n \cdot A_{-,n}$
   d.h. Ax ist *Linearkombination* der Spalten $A_{-,i}$ von A mit Koeffizienten $x_1, \ldots, x_n$
   Insbesondere:
   (*) aus 1.24 ist genau dann lösbar, wenn die Spalte b als Linear Kombination der Spalten von A dargestellt werden kann.
2. $\bar{A}$ ist eine *lineare Abbildung* in dem folgenden Sinne, dass $\bar{A}$ mit der Bildung von Linearkombinationen verträglich ist, d.h. für alle $s, t \in \mathbb{R}$ und alle Spalten $x, y \in \mathbb{R}^{n \times 1}$ gilt $\bar{A}(sx + ty) = s\bar{A}(x) + t\bar{A}(y)$

1.28 Beispiel

Ein Werk braucht Rohstoffe vom Typ R1 und R2 um Zwischenprodukte vom Typ Z1,Z2,Z3 zu produzieren.Die genauen Mengen sind :

	Z_1	Z_2	Z_3
R1	1	2	3
R2	2	3	4

$A : \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \end{pmatrix} \in \mathbb{R}^{2\times 3}$ Matrix

$\bar{A} : \mathbb{R}^{3\times 1} \to \mathbb{R}^{2\times 1} : z \longmapsto A_z$

Eine Spalte z $\begin{pmatrix} Z_1 \\ Z_2 \\ Z_3 \end{pmatrix}$ repräsentiert die Mengen z1,z2,z3 der zur Produktion von Z_1, Z_2, Z_3 notwendigen Rohstoffe.

entsprechend r= $\begin{pmatrix} r_1 \\ r_2 \end{pmatrix}$ repräsentiert die Mengen r1,r2 der Rohstoffe R1,R2.

Az=r sagt aus, wie viele Rohstoffe man braucht, um die Zwischenprodukte herzustellen.

Beachte : Für gegebenes z $\in \mathbb{R}^{3\times 1} \rightsquigarrow$ eindeutigem r $\in \mathbb{R}^{2\times 1}$ aber $\bar{A}$ nicht injektiv: Für vorgegebenes r $\in$Bild($\bar{A}$) eine ganze Faser voll Möglichkeiten für z mit Az=r.

Zum Beispiel:

r1=2 , r2 = 3

$1Z_1 + 2Z_2 + 3Z_3 = 2$

$2Z_1 + 3Z_2 + 4Z_4 = 3$

Andererseits :

$\bar{A}$ ist surjektiv : Jedes r ist möglich. Zu jedem $r \in x$, ein z mit $Az = \surd$

1.29 Beispiel

System mit 4 Zuständen, etwa eine Maus in einem Haus mit 4 Zimmern.

Spalte $w = \begin{pmatrix} w_1 \\ \vdots \\ w_4 \end{pmatrix}$ mit $w_i \in \mathbb{R}, 0 \leq w_i \leq 1$, $w_1 + \ldots + w_4 = 1$

wird interpretiert w_1 : Wahrscheinlichkeit, dass das System im Zustand i ist z.B.

$\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \equiv$ Maus ist mit Sicherheit in Zimmer 1

$$A = \begin{pmatrix} 1/2 & 1/3 & 0 & 0 \\ 1/2 & 1/3 & 1/3 & 0 \\ 0 & 1/3 & 1/3 & 1/2 \\ 0 & 0 & 1/3 & 1/2 \end{pmatrix} \in \mathbb{R}^{4\times 4}$$

$A_{i,j}$ wird interpretiert als Wahrscheinlichkeit dafür, dass das System vom Zustand j in den Zustand i übergeht.

Beachte :

$0 \leq A_{i,j} \leq 1 i = 1..4$

$A_{1,j} + \ldots + A_{4,j} = 1$

Abbildung $\bar{A} : \mathbb{R}^{4\times 1} \to \mathbb{R}^{4\times 1} : w \longmapsto Aw$

Kann man mit Hilfe von A feststellen, wie sich die Wahrscheinlichkeit beim Übergang von w aus ändert .

Ausgangszustände : $\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$

Wir betrachten $w := \{w \in \mathbb{R}^{4\times 1} | 0 \leq w_i \leq 1 \forall i = 1,2,3,4, w_1 + w_2 + w_3 + w_4 = 1\}$

Interpretiere $\bar{A}^2\left(\left(\begin{pmatrix}1\\0\\0\\0\end{pmatrix}\right)\right) = \bar{A}\left(\bar{A}\left(\left(\begin{pmatrix}1\\0\\0\\0\end{pmatrix}\right)\right)\right) = A\begin{pmatrix}1/2\\1/2\\0\\1\end{pmatrix} = \begin{pmatrix}5/12\\5/12\\1/6\\0\end{pmatrix}$

Beachte :

$A_{w_0} = w_0$ für $w_0 = \begin{pmatrix}1/5\\3/10\\3/10\\1/5\end{pmatrix}$

$w, Aw_1 = w_2, Aw_2 = w_3, \ldots \to w_0$ (konvergiert nach w_0)

1.30 Satz

Seien $A \in \mathbb{R}^{m\times n}, B \in \mathbb{R}^{n\times 0}$ (n in beiden Teilen das gleiche n!)
$\Rightarrow$ Komposition $\bar{A}\circ\bar{B}$ der linearen Abbildung.
$\bar{A} : \mathbb{R}^{n\times 1} \to \mathbb{R}^{m\times 1}$ und $\bar{B} : \mathbb{R}^{o\times 1} \to \mathbb{R}^{n\times 1}$ ist wieder eine lineare Abbildung $\bar{A}\circ\bar{B} : \mathbb{R}^{0\times 1} \to \mathbb{R}^{m\times 1}$ und es gilt :
$\bar{A}\circ\bar{B} = \bar{AB}$ wo $C = AB \subset \mathbb{R}^{m\times o}$ die Spalten $C_{-,j} = AB_{-,j}$ hat für $j, \ldots, 0$ 1. Beweismöglichkeit (Spaltenphilosophie):

1. Behauptung : $\bar{A}\circ\bar{B}$ lineare Abbildung
   Beweis : $s, t \in \mathbb{R}, x, y \in \mathbb{R}^{o\times 1}$
   $\Rightarrow (\bar{A}\circ\bar{B})(sx+ty) =$
   $= \bar{A}_{(\bar{B}_{(sx+ty)})}$
   $= \bar{A}_{(s\bar{B}_{(x)}+t\bar{B}_{(y)})}$
   $= s\bar{A}_{(\bar{B}_{(x)})} + t\bar{A}_{(\bar{B}_{(y)})}$
   $= s(\bar{A}\circ\bar{B})_{(x)} + t(\bar{A}\circ\bar{B})_{(y)} \checkmark$
2. Behauptung : $\gamma : \mathbb{R}^{0\times 1} \to \mathbb{R}^{m\times 1}$ linear
   $\Rightarrow \gamma = \bar{G}$ mit $G \in \mathbb{R}^{m\times o}$ mit Spalten
   $$G_{-,j} = \gamma_{e_i} \text{ wo } e_i = (I_0)_{-,i} = \left.\begin{pmatrix}0\\\vdots\\0\\1\\0\\\vdots\\0\end{pmatrix}\right\} o \text{ Elemente (wobei die 1 an Position i steht)}$$
   wobei $I_0 = O \times O$-Einheitsmatrix
   $I_0 : \underline{o}\times\underline{o} \to \mathbb{R} : (i,j) \longmapsto \delta_{i,j} := \begin{cases}1 & i=j\\ 0 & i\neq j\end{cases}$ (Kronecker-δ)
3. Behauptung : $C_{-,j} = AB_{-,j}$ (aus der Form dieses Satzes)
   Beweis : $C_{-,j} \underbrace{=}_{Beh.2} (\bar{A}\circ\bar{B})(e_i) = \bar{A}_{(\bar{B}_{(e_i)})} = \bar{A}_{(B_{-,i})} = AB_{-,i}$ q.e.d.

2. Beweismöglichkeit (Substitutionsphilosophie):
$\bar{B}_{(x)} = y$ heisst
$y_i = \sum_j B_{ij}x_i, \bar{A} = z$ bedeutet $z_j = \sum_k A_{jk}y_k$
Sei $(\bar{A}\circ\bar{B})_{(x)} = z'$
$\Rightarrow z'_j = \sum_k A_{j,k}y_k \underbrace{=}_{y_k=y_i} \sum_k A_{j,k}\sum_e A_{k,e}x_e$
$= \sum_e(\sum_k A_{j,k}B_{k,l})x_e \Rightarrow$ Behauptung q.e.d.

1.31 Beispiel

1. (Fortsetzung von 1.29) (Mäusematrix)= $A \in \mathbb{R}^{4\times 4}$
$$A^2 = A \cdot A \begin{pmatrix} 1/2 & 1/3 & 0 & 0 \\ 1/2 & 1/3 & 1/3 & 0 \\ 0 & 1/3 & 1/3 & 1/2 \\ 0 & 0 & 1/3 & 1/2 \end{pmatrix} \begin{pmatrix} 1/2 & 1/3 & 0 & 0 \\ 1/2 & 1/3 & 1/3 & 0 \\ 0 & 1/3 & 1/3 & 1/2 \\ 0 & 0 & 1/3 & 1/2 \end{pmatrix}$$
$$= \begin{pmatrix} 5/12 & 5/18 & 1/9 & 0 \\ 5/12 & 7/18 & 2/9 & 1/6 \\ 1/6 & 2/9 & 7/18 & 5/12 \\ 0 & 1/9 & 5/18 & 5/12 \end{pmatrix}$$
Experiment A^n (für n gross) " nahe bei "
$$= \begin{pmatrix} 1/5 & 1/5 & 1/5 & 1/5 \\ 3/10 & 3/10 & 3/10 & 3/10 \\ 3/10 & 3/10 & 3/10 & 3/10 \\ 1/5 & 1/5 & 1/5 & 1/5 \end{pmatrix}$$

2. (Fortsetzung von 1.28) $A_z = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \end{pmatrix} \underbrace{\begin{pmatrix} z_1 \\ z_2 \\ z_3 \end{pmatrix}}_{Zwischenprodukte} = \underbrace{\begin{pmatrix} r_1 \\ r_2 \end{pmatrix}}_{Rohstoffe}$
$$B_e := \begin{pmatrix} 1 & 2 \\ 2 & 3 \\ 3 & 4 \end{pmatrix} \cdot \underbrace{\begin{pmatrix} e_1 \\ e_2 \end{pmatrix}}_{Endprodukt} = \begin{pmatrix} z_1 \\ z_2 \\ z_3 \end{pmatrix}$$
Es ist $AB = \begin{pmatrix} 14 & 20 \\ 20 & 29 \end{pmatrix}$
Interpretation :
$(AB)_e = \begin{pmatrix} 14 & 20 \\ 20 & 29 \end{pmatrix} \begin{pmatrix} e_1 \\ e_2 \end{pmatrix} = \begin{pmatrix} r_1 \\ r_2 \end{pmatrix}$
Beachte $\overline{AB}$ ist bijektiv ohne dass$\bar{A}$ oder $\bar{B}$ bijektiv wären.
Aber $\bar{B}$ injektiv und $\bar{A}$ surjektiv.

1.32 Folgerung

(aus der Assoziativität der Komposition)
Matrixmultiplikation ist assoziativ
Genauer :
$A \in \mathbb{R}^{m\times n}, B \in \mathbb{R}^{n\times o}, C \in \mathbb{R}^{0\times p}$
$\Rightarrow (AB)C = A(BC)$
Beweis:
$\overline{(AB)C}$
$= \overline{(AB)} \circ \bar{C}$ nach 1.30
$= (\bar{A} \circ \bar{B}) \circ \bar{C}$ nach 1.30
$= \bar{A} \circ (\bar{B} \circ \bar{C})$ nach 1.15
$= \bar{A} \circ \overline{BC}$ nach 1.30
$= \overline{A(BC)}$ nach 1.30 q.e.d.

1.33 Beispiel

In 1.29 offene Frage :
Bildet $\bar{A}$ die Menge

$W := \{w \in \mathbb{R}^{4\times 1} | 0 \leq w_i \leq 1; i = 1, \ldots, 4; w_1 + \ldots + w_4 = 1\}$
(Der W-Wert) in sich ab?
letzte Bedingung :
$(1,1,1,1)A = (1,1,1,1)$
$(1,1,1,1)(Aw) = ((1,1,1,1)A)w = (1,1,1,1)w$
d.h. letzte Bedingung für Aw erfüllt, falls für w erfüllt

1.34 Beispiel

1.28 + 1.31 :
Preisliste für Rohstoffe als Zeile :
$(2,3) \in \mathbb{R}^{1\times 2}$
$(2,3)\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \end{pmatrix} = (8,13,18)$ (Preisliste für Zwischenprodukte)
$(2,3)AB =$ Preisliste für Rohstoffanteil der Endprodukte

1.35 Bemerkung

$A \in \mathbb{R}^{m\times n}, B \in \mathbb{R}^{m\times o}$
$C = AB \in \mathbb{R}^{m\times o} \Rightarrow$

1. $C_{ij} = A_{i,-}B_{-,j}$ (Zeile und Spalte)
2. $C_{-,j} = AB_{-,j}$ (Spaltenorientiert)
3. $C_{i,-} = A_{i,-}B$ (Zeilenorientiert)
4. $C = A_{-,1}B_{1,-} + A_{-,2}B_{2,-} + \ldots + A_{-,n}B_{n,-}$ (Spalte · Zeile)

1.36 Definition

Sei $M \in \mathbb{R}^{s\times t}$

1. Für $i \in \underline{s} := \{1, \ldots, 5\}$ ist der *i-te Stufenindex*
   $St_i(M)$ definiert als :
   $St_i(M) = min\{j \in \underline{t} | M_{ij} \neq 0\}$
   Falls $M_{i,-} =$ Nullzeile, dann $St_i(M) := t + i$
2. M ist in *Stufenform* :
   falls die Folge $St(M) := (St_1(M), St_2(M), \ldots, St_5(M))$ streng monoton steigt. D.h. :
   $ST_1(M) < St_2(M) < \ldots < St_5(M)$
   Falls zusätzlich noch für jeden Stufenindex $j := St_i(M) \leq t$ für die entsprechende Spalte von M gilt : $M_{-,j} = (I_s)_{-,i}$ ist M in *strikter Stufenform.*

1.37 Beispiel

$1z_1 + 2_z 2 + 3_z 3 + 21z_4 = 2$
$2z_1 + 4z_2 + 4z_3 + 28z_4 = 3$
$\rightsquigarrow \left(\begin{array}{cccc|c} 1 & 2 & 3 & 21 & 2 \\ 2 & 4 & 4 & 28 & 3 \end{array}\right)$
Stufenfolge : (1,1), also nicht in Stufenform

$\rightsquigarrow \left(\begin{array}{cccc|c} 1 & 2 & 3 & 21 & 2 \\ 0 & 0 & -2 & -14 & -1 \end{array}\right) (2 \cdot Zeile1 - Zeile2)$

Stufenfolge : (1,3), also in Stufenform

$$\rightsquigarrow \left(\begin{array}{cccc|c} 1 & 2 & 0 & 0 & 1/2 \\ 0 & 0 & 1 & 7 & 1/2 \end{array}\right)$$

$\rightsquigarrow$ Gleichungssystem

$$\begin{array}{cccccc} z_1 & +2z_2 & & & = & 1/2 \\ & & z_3 & +7z_4 & = & 1/2 \end{array}$$

Lösen : Für Nichtstufenindizes(z_2, z_4) neue Gleichungen einfhren :
$z_2 = p_1$, $z_4 = p_2$ $(p_1, p_2 \in \mathbb{R}$: Parameter)

$$\begin{array}{cccccc} z_1 & +2z_2 & & & = & 1/2 \\ & & z_3 & +7z_4 & = & 1/2 \\ & z_2 & & & = & p_1 \\ & & & z_4 & = & p_2 \end{array}$$

$$\rightsquigarrow \left(\begin{array}{cccc|c} 1 & 2 & 0 & 0 & 1/2 \\ 0 & 0 & 1 & 7 & 1/2 \\ 0 & 1 & 0 & 0 & p_1 \\ 0 & 0 & 0 & 1 & p_2 \end{array}\right) \rightarrow \left(\begin{array}{cccc|c} 1 & 0 & 0 & 0 & 1/2 \cdot 2p_1 \\ 0 & 1 & 0 & 0 & p_1 \\ 0 & 0 & 1 & 0 & 1/2 - 7p_2 \\ 0 & 0 & 0 & 1 & p_2 \end{array}\right)$$

Also Lösung :
$z_1 = 1/2 - 2p_1$
$z_2 = p_1$
$z_3 = 1/2 - 7p_2$
$z_4 = p_2$ mit $p_1, p_2 \in \mathbb{R}$

1.38 Lemma

Sei $M \in \mathbb{R}^{s \times t}$, die wir als erweiterte Matrix eines linearen Gleichungssystems auffassen. Folgende Veränderungen der Matrix M zu einer Matrix N ändern die Lösungsmenge des zugehörigen Gleichungssystems nicht :

1. Add(i, j, a) für $i, j \in \underline{s}, i \neq j, a \in \mathbb{R}$ d.h. addiere das a-Fache der i-ten Zeile auf die j-te Zeile von M:
$$N_{k,-} = \begin{cases} M_{k,-} & k \neq j \\ M_{j,-} + aM_{i,-} & k = j \end{cases}$$
2. Mul(i, a),$i \in \underline{s}, a \in \mathbb{R} - \{0\}$, d.h. multipliziere die i-te Zeile von N mit a :
$$N_{k,-} = \begin{cases} M_{k,-} & k \neq i \\ aM_{i,-} & k = i \end{cases}$$
3. Ver(i, j), $i, j \in \underline{s}, i \neq j$: d.h. vertausche die i-te mit der j-ten Zeile:
$$N_{k,-} = \begin{cases} M_{?,?} & k \neq i, k \neq j \\ M_{i,-} & k = j \\ M_{j,-} & k = i \end{cases}$$

Beweis : Klar :
x Lösung des Gleichungssystems zu M
$\Rightarrow x$ Lösung des Gleichungssystems zu N

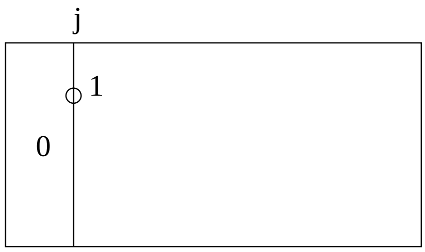
Die Umkehrung folgt, da jede der drei Operationen rückgängig gemacht werden kann.
Add(i, j, a) durch Add$(i, j, -a)$
Mul(i, a) durch Mul$(i, 1/a)$
Ver(i, j) durch Ver(i, j) q.e.d.

1.39 Algorithmus

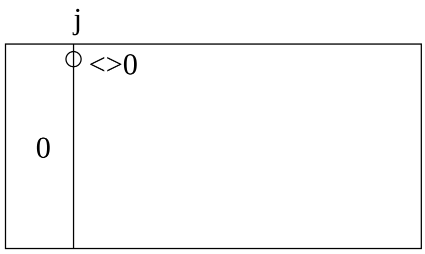
Gegeben : $M \in \mathbb{R}^{s \times t}$ erweiterte Matrix eines lin. Gleichungssystems
Gesucht : Lösungsmenge des Gleichungssystems

Algorithmus (Gauß) :

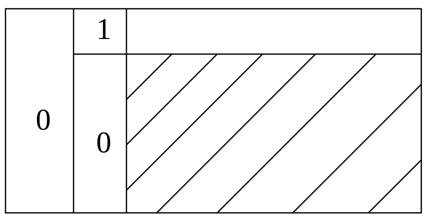
1. Teil : Überprüfe ob M in Stufengestalt ist
   Finde den kleinsten Spaltenindex j, mit $M_{-,j} \neq 0$



Finde den kleinsten Zeilenindex i mit $M_{i,j} \neq 0$
Falls $i \neq 1$ vertausche 1. und i-te Zeile, so dass wir von $i = 1$ ausgehen können.

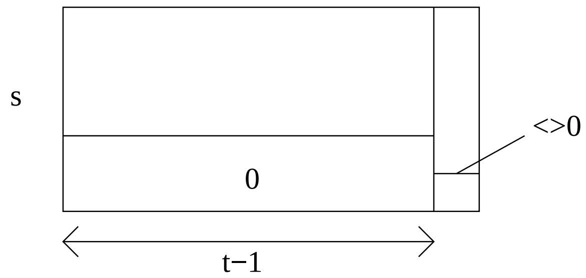


Falls $M_{1,j} \neq 1$, wende $\mathrm{Mul}(1, M_{1,j}^{-1})$ an also $M_{1,j} = 1$
Räume die j-te Spalte aus durch Subtraktion des $M_{i,j}$-fachen der 1.Zeile von der i-ten Zeile $(i = 2, 3, \ldots)$ $(\mathrm{Add}(1, i, -M_{i,j})$ anwenden)



Wiederhole dieses Verfahren mit der Teilmatrix von M, die aus M durch streichen der 1.Zeile und der 1. j Spalten hervorgeht.

Wiederhole:
Am Ende hat man eine Matrix M in Stufengestalt mit derselben Lösungsmenge wie die Ausgangsgleichung. Letztere ist genau dann leer, wenn t ein Stufenindex ist.



2. Teil : Mache Lösungen explizit
   Falls t kein Stufenindex ist, streiche die Nullzeilen von M und füge für jeden Nichtstufenindex $i_1, \ldots, i_d$ eine neue Zeile $((I_{t-1})_{i,-|p_l})$ hinzu, wobei p_l ein Parameter ist.
   Bringe die neue Matrix durch die Operationen $\mathrm{Ver}(i,j)$ und $\mathrm{Add}(i,j,a)$ auf strikte Stufengestalt$(I_{t-1}|L)$ wobei L eine Spalte ist, die die Lösung des Gleichungssystems in Abhängigkeit von den Parametern p_i angibt.

1.40 Beispiel

Aufgabe :
Bestimme alle Parabeln die durch die Punkte (1,0) und (3,2) gehen mit der Leitlinie parallel zur x-Achse.

Lösung :
Jede derartige Parabel hergestellt durch eine Funktion
$f : \mathbb{R} \mapsto \mathbb{R} : x \longmapsto ax^2 + bx + c$ mit $f_{(1)} = 0$ und $f_{(3)} = 2$
$\Leftrightarrow$ zu linearem Gleichungssystem :

$$\begin{array}{cccccc} a & +b & +c & = & 0 \\ 9a & +3b & +c & = & 2 \end{array}$$

$$\left(\begin{array}{ccc|c} 1 & 1 & 1 & 0 \\ 9 & 3 & 1 & 2 \end{array}\right) \to \left(\begin{array}{ccc|c} 1 & 1 & 1 & 0 \\ 0 & -6 & -8 & 2 \end{array}\right)$$

$$\to \left(\begin{array}{ccc|c} 1 & 0 & -1/3 & 1/3 \\ 0 & 1 & 4/3 & -1/3 \\ 0 & 0 & 1 & p \end{array}\right) \to \left(\begin{array}{ccc|c} 1 & 0 & 0 & 1/3 + p/3 \\ 0 & 1 & 0 & -1/3 - 4p/3 \\ 0 & 0 & 1 & p \end{array}\right)$$

1.41 Beispiel

Aufgabe:
Beschreibe Bild$\bar{A}$, mit

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

$\bar{A} = \mathbb{R}^{4\times1} \to \mathbb{R}^{3\times1}$
Lösung mit Gauss Algorithmus :

$$A = \left(\begin{array}{cccc|c} 1 & 2 & 3 & 4 & x \\ 2 & 3 & 4 & 5 & y \\ 3 & 4 & 5 & 6 & z \end{array}\right) \text{ (x,y,z : Bildvektor)}$$

$$\to A = \left(\begin{array}{cccc|c} 1 & 2 & 3 & 4 & x \\ 0 & -1 & -2 & -3 & y - 2x \\ 0 & -2 & -4 & -6 & z - 3x \end{array}\right) \to A = \left(\begin{array}{cccc|c} 1 & 2 & 3 & 4 & x \\ 0 & 1 & 2 & 3 & -y + 2x \\ 0 & 0 & 0 & 0 & z - 3x - 2y + 4x \end{array}\right)$$

Lösbar :$\Leftrightarrow'$ Die Bedingung $x - 2y + z = 0$ ist erfllt.
Weiteres vorgehen : die Bedingung lösen

1.42 Beispiel

Aufgabe:
Sei $A \in \mathbb{R}^{2\times 3}$ gegeben durch $A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \end{pmatrix}$
Überprüfe, ob $\bar{A} : \mathbb{R}^{3\times 1} \mapsto \mathbb{R}^{2\times 1}$ ein Rechtsinverses hat und berechne <u>alle linearen</u> rechtsinversen.

Lösung :
Gesucht alle $B \in \mathbb{R}^{3\times 2} mitAB = I_2$
Zwei lineare Gleichungssysteme:
$AB_{-,1} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}) = ((I_2)_{-,1})$
$AB_{-,2} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}) = ((I_2)_{-.2})$

$$\left(\begin{array}{ccc|cc} 1 & 2 & 3 & 1 & 0 \\ 2 & 3 & 4 & 0 & 1 \end{array}\right) \rightarrow \left(\begin{array}{ccc|cc} 1 & 2 & 3 & 1 & 0 \\ 0 & -1 & -2 & -2 & 1 \end{array}\right)$$

$$\rightarrow \left(\begin{array}{ccc|cc} 1 & 0 & -1 & -3 & 2 \\ 0 & 1 & 2 & 2 & -1 \end{array}\right) \rightarrow \left(\begin{array}{ccc|cc} 1 & 0 & -1 & -3 & 2 \\ 0 & 1 & 2 & 2 & -1 \\ 0 & 0 & 1 & a & b \end{array}\right)$$

$$\rightarrow \left(\begin{array}{ccc|cc} 1 & 0 & 0 & -3+a & 2+b \\ 0 & 1 & 0 & 2-2a & -1-2b \\ 0 & 0 & 1 & a & b \end{array}\right)$$

Also $B = \begin{pmatrix} -3+a & 2+b \\ 2-2a & -1-2b \\ a & b \end{pmatrix}$
$A \cdot B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ $\bar{B}$: lineare Rechtsinverse
(Bemerkung : lineares Linksinverses kann nur bei inj existieren)

1.43 Definition

Ist $A : \underline{m} \times \underline{n} \rightarrow \mathbb{R} : (i,j) \longmapsto A_{i,j}$ eine Matrix, so heisst
$A^{tr} : \underline{m} \times \underline{n} \rightarrow \mathbb{R} : (i,j) \longmapsto A_{j,i}$ die *transponierte Matrix* oder die *Transponierte* von A

1.44 Lemma

Sind $A \in \mathbb{R}^{m\times n}, B \in \mathbb{R}^{n\times o}$
$\Rightarrow (AB)^{tr} = B^{tr}A^{tr}$
Ist $\bar{A}$ surjektiv mit rechtsiversem $\bar{B}$, so ist $\bar{A}^{tr}$ injektiv mit linksinversem $\bar{B}^{tr}$ und umgekehrt.

- **Partitionen,Äquivalenzrelationen**

1.45 Definition

Sei M eine Menge

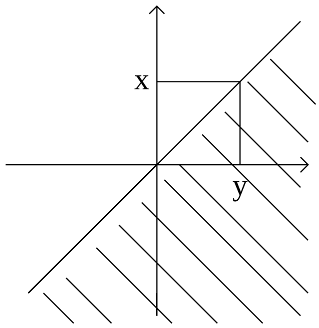
1. Eine *Relation* R auf M ist eine Teilmenge von $M \times M$. Statt $(m,n) \in reals$ schreibt man auch mRn (m steht in Relation R zu n)
2. Eine Relation heisst *reflexiv*, falls mRm gilt für alle $m \in M$.
3. Eine Relation heisst *symmetrisch*, falls mRn immer nRm impliziert.

4. Eine Relation heisst *transitiv*, falls mRn und nRo stehts mRo zur Folge hat$(m, n, o \in M)$

5. Eine reflexive, symmetrische und transitive Relation R auf M heisst *Äquivalenzrelation*. Statt mRn sagt man auch m und n sind äquivalent bezüglich R.

1.46 Beispiel

1. $\leq$ ist eine Relation auf $\mathbb{R}$
   $\leq$ ist :
   reflexiv ($<$ ist nicht reflexiv)
   nicht symmetrisch
   transitiv $(x \leq y \wedge y \leq z \Rightarrow x \leq z)$
   $\Rightarrow \leq$ ist keine Äquivalenzrelation



2. Sei $G : M \to N$ (G wie Gesichtspunkt)
   $\sim_G \subseteq M \times M$ sei definiert durch
   $m \sim_G m' :\Leftrightarrow G_{(m)} = G_{(m')}$
   $\Rightarrow \sim_G$ ist eine Äquivalenzreaktion "Bildgleichheit" bezüglich G
   z.B.:
   $G : \mathbb{R}^2 \to \mathbb{R}(x, y) \longmapsto x - y$
   $(x, y) \sim_G (x', y') \Leftrightarrow x - y = x' - y'$

   $G : \mathbb{R}^2 \to \mathbb{R} : (x, y) \longmapsto x^2 + y^2$
   $(x, y) \sim_G (x', y') \Leftrightarrow x^2 + y^2 = (x')^2 + (y')^2$
3. M Menge, $f : M \to M$
   $m, n \in Mm \sim n :\Leftrightarrow$ es existieren $a, b \in \mathbb{N}$ mit
   $f^a_{(m)} = f^b_{(n)}$
   $f^1_{(m)} = f_{(m)}$
   $f^{n+1}_{(m)} = f_{(f^a_{(m)})}$
   $|M| < \infty$

1.47 Definition

M Menge $(\neq \emptyset)$

1. Eine Partition P von M ist eine Menge von nicht leeren Teilmengen von M, also $P \subseteq \mathrm{Pot}(M)$ und $X \neq 0$ für alle $X \in P$, mit
   (a) $M = \bigcap_{X \in P}$ und
   (b) $X \bigcap Y = \emptyset$ für $X, Y \in P$ mit $X \neq Y$

Kurz : für a und b $M = \bigcup_{X \in P} X$

2. Sei P eine Partition auf M. Die Elemente von P heissen auch *Klassen.*Ist X eine Klasse, so nennt man ein Element von X auch *Vertreter* der Klasse X. Eine Teilmange von M, die aus jeder Klasse von P genau einen Vertreter enthält nennt man auch *Vertretermenge* oder *Transversale.*
   Eine Abbildung $v : P \to M$ mit Bild(v) eine Transversale heisst auch *Vertreterabbildung* oder *Transversale.*

   Klar : P eine Partition von M, so gehört jedes Element von M zu genau einem $X \in P$ (genau einer Klasse), d.h.
   $f_p : M \to P : n \longmapsto X \in P$ mit $m \in X$ (f_p : natürliche Abbildung zu P)

1.48 Satz

1. Ist $\sim$ eine Äquivalenzrelation auf der Menge M, so bilden die *Äquivalenzklassen* definiert durch $[m_0] := [m_0]_N := \{m \in M | m \sim m_0\}$ für $m_0 \in M$ eine Partition von M
   Äquivalenzklassen bezeichnet man mit $M_{/\sim}$
2. Ist P eine Partition von M, so ist $\sim_P$ definiert durch
   $m \sim_P n :\Leftrightarrow$ existiert $X \in P$ mit $m \in X, n \in X$ $(m, n \in M)$ eine Äquivalenzrelation auf M
3. Es gilt $M_{\sim_P} = P$ für alle Partitionen P von M und $\sim_{(M_{/\sim})} = \sim$ (links vom Gleich steht eine Partition)

Beweis:

1. $m_0 \in [m_0] \neq \emptyset$ für alle $m_0 \in M$
   $\Rightarrow \bigcup_{m_0 \in M} [m_0] = M$
   Zwei verschiedene Äquivalenzklasen sind sicherlich disjunkt :
   $[m_1] \cap [m_2] \neq \emptyset$; existiert, $m_0 \in [m_1] \cap [m_2]$
   $\Rightarrow [m_1] = [m_0] = [m_2]$
2.
3. Nach Definition von $\sim_P$ sind die Äquivalenzklassen von $\sim_P$ gerade die Klassen von P, d.h. die Menge der $M_{/\sim_P} = P$
   Andererseits : Sei $\sim$ eine Äquivalenzrelation auf M
   Zeige $m, n \in M : m \sim n \Leftrightarrow n \sim_{M_{/\sim}} n$
   Beides heisst aber, daßm und n zu derselben Menge von $M_{/\sim}$ gehören q.e.d.

1.49 Bemerkung

Sei $f : M \to N$ eine Abbildung
$\to \{f^{-1}_{(\{m\})} | n \in f_{(M)}\}$ ($n \in f_{(M)}$ entspricht $n \in$ Bild(f))
ist eine Partition zur Äquivalenzrelation $\tilde{f}$ =Bildgleichheit bezüglich f. d.h. $M_{/\sim_f} = \{f^{-1}_{(\{m\})} | n \in f_{(M)}\}$

1.50 Hauptsatz

Sei $f : M \to N$ eine Abbildung.
Dann faktorisiert f als $f = \bar{f} \circ \nu_f$ mit ν_f surjektiv und$\bar{f}$ injektiv, wo
$\nu_f : M \to M_{/\sim_f} : m \longmapsto f^{-1}_{(f_{(m)})}$

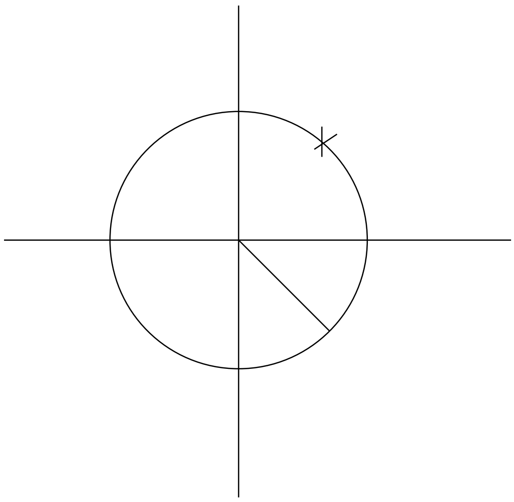
Die natürliche Abbildung von $\sim_f$ ist und $\bar{f}$ durch $\bar{f} : M_{/\sim_f} \to N : f^{-1}_{\{f_{(m)}\}} \longmapsto f_{(m)}$ definiert ist. Statt $f = \bar{f} \circ \nu_f$ sagt man auch, daßdas Diagramm
kommutiert.

Beweis :

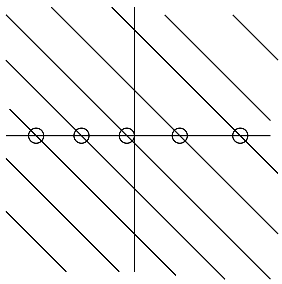
1. Klar : ν_f wohl definiert und surjektiv, da $\sim_f$ eine Äquivalenzrelation ist.
2. Zeige : $\bar{f}$ wohldefiniert :
 $m, m' \in M$ mit $f^{-1}_{(f_{(m)})} = f^{-1}_{(f_{(m')})}$
 $\Rightarrow f_{(m)} = f_{(m')} \surd$ nach Definition von Abbildungen (Vertreterunabhngig)
 Zeige $f = \bar{f} \circ \nu_f$, sofort aus Definition von $\nu und \bar{f}$

1.51 Beispiel

1. $f : \mathbb{R}^2 \to \mathbb{R} : (x, y) \longmapsto \sqrt{x^2 + y^2}$
 Fasern : Kreise mit Mittelpunkt $(0, 0)$
 ν_f ordnet jedem Punkt den Kreis zu, auf dem er liegt.
 $\bar{f}$ ordnet dem Kreis seinen Radius zu.



2. Sei $f : \mathbb{R}^2 \to \mathbb{R} : (x, y) \longmapsto x + y$
 Fasern : Geraden parallel $x + y = 0$ ν_f stellt fest, auf welcher dieser Geraden mein Punkt liegt.
 $\bar{f}$ identifiziert jede dieser Geraden mit ihrem Schnittpunkt mit der x-Achse



3. Sei $f : \mathbb{Z} \to \{0, 1\} : x \longmapsto xmod2$ Fasern :
 $\{$ gerade Zahlen $\}$
 $\{$ ungerade Zahlen $\}$

ν_f stellt fest zu welcher dieser beiden Mengen meine Zahl gehört.
$\bar{f}$ identifiziert diese Mengen mit ihrem Standardvertretern 0 bzw. 1.

4. Ist m eine Menge und $P' \subseteq \text{Pot}(M)$ eine endliche Teilmenge der Gestalt
$P' \subseteq \{A_1, B_1 := M - A_1, A_2, B_2 := M - A_2, \ldots, A_n, B_n := A_n - M\}$ (keine Menge mehrfach aufgezählt)
$m \in M : [m] = \bigcap\limits_{\substack{X \in P \\ m \in P}} X, \Rightarrow P = \{[m] | m \in M\}$ Partition von M. Weiter $\log_2(2n) \leq |P| \leq 2^n$
Klar, wenn man die Abbildung
$\xi : M \to \{0,1\}^n : m \longmapsto (\chi_{A_1}(m), \chi_{A_2}(m), \ldots, \chi_{A_n}(m))$
betrachtet.
Fasern$=[m]$ von oben.

1.52 Beispiel

1. $f : \mathbb{Z} \to \{0,1\} : x \longmapsto x \bmod z$
$\sim_f$ ist verträglich mit $+$ und $\cdot$ in $\mathbb{Z}$
" ungerade $\cdot$ ungerade $=$ ungerade " etc.
$\rightsquigarrow$ auf $\mathbb{Z}_{/\sim_f} = \mathbb{Z}_{/2\mathbb{Z}}$
Addition und Multiplikation (vertreterweise Definiert) [1]+[1]=[0]
2. $A \in \mathbb{R}^{m\times n}, f := \bar{A} : \mathbb{R}^{m\times 1} \to \mathbb{R}^{m\times 1} : x \longmapsto Ax$
Auf $M = \mathbb{R}^{n\times 1}$ $+$ (und Multiplikation mit reellen Zahlen)
Ebenso auf $N = \mathbb{R}^{m\times 1}$. f respektiert diese $+,\cdot$
$Ax = b$ (*)
Übertrage $+$ von M oder N auf $\mathbb{R}^{m\times n}_{/\sim_f}$
$\to f^{-1}_{(\{b\})} = f^{-1}_{(\{b'\})} := f^{-1}_{(\{b+b'\})} b, b' \in \text{Bild}_(f)$
$\bar{f}$ macht Bijektion zwischen den Lsungsmengen von (*) und den rechten Seiten von (*).
Diese Bijektion ist additiv (sogar linear)

2 Algebraische Strukturen

Die Gruppenaxiome :

2.1 Definition

Sei $A \neq \emptyset$ Menge. Eine *innere Verknüpfung* von A ist eine Abbildung
$o : A \times A \to A : (a,b) \longmapsto a \circ b$
Eine *äußere Verknüpfung* ist eine Abbildung $M \times A \to A$ (M Menge) Eine *algebraische Struktur* ist eine Menge $A \neq \emptyset$ zusammen mit einer Menge von Verknüpfungen.

2.2 Beispiel

1. $\mathbb{R}, +, \cdot$ algebraische Struktur ($+,\cdot$ innere Verknüpfungen)
2. $A = \{0,1\}$ Zwei innere Verknüpfungen : $\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array}$ und $\begin{array}{c|cc} \cdot & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}$
3. $A = \mathbb{R}^{n\times 1}, +$ innere Verknüpfungen
$$M = \mathbb{R}, \mathbb{R} \times \mathbb{R}^{n\times 1} \to \mathbb{R}^{n\times 1} : \left(a \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \right) \longmapsto \begin{pmatrix} ax_1 \\ \vdots \\ ax_n \end{pmatrix}$$

2.3 Definition

Eine algebraische Struktur (G,·) heißt *Gruppe*, falls die folgenden drei Axiome erfüllt sind :

1. (Assosiativgesetz) : $x \cdot (y \cdot z) = (c \cdot y) \cdot z$ für alle $x, y, z \in G$
2. (Einselement) : Es existiert ein eindeutiges Element $\underline{1}$ inG mit $1 \cdot g = g \cdot 1 = g$ für alle $g^{\in}G$
3. (Inverses Element) : Zu jedem $g \in G$ existiert ein g^{-1} mit $g \cdot g^{-1} = g^{-1} \cdot g = 1$ Oft : gh statt $g \cdot h$; Falls noch folgende Bedingung gilt, heißt G auch *abelsche Gruppe* oder kommutative Gruppe
4. (Kommutativgesetz) : $gh = hg$ für alle $h, g \in G$
   Bei kommutativen Gruppen manchmal + statt ·,dann Einselement 0 und heißt Nullelement

2.4 Beispiel

1. $M \neq \emptyset$ und $S_M :=\sim (M)$
   := Die Menge der bijektiven Abbildungen $M \to M$
   (Bei $M = \underline{n} = \{1, \ldots, n\}, S_n$ statt $S_{\underline{n}}$)
   Darin S_M zusammen mit der Komposition von Abbildungen ist eine Gruppe.
2. Sei $GL(n, \mathbb{R})$:= Menge der invertierbaren Matrizen $\mathbb{R}^{n \times n}$
   (Erinnerung : $A \in \mathbb{R}^{n \times n}$ ist invertierbar, fass $B \in \mathbb{R}^{n \times n}$ existiert mit $AB = I_n \Leftrightarrow BA = I$)
   $\Rightarrow GL(n, \mathbb{R})$ zusammen mit Matrixprodukt ist eine Gruppe mit Einselement I_n
   $GL(n, \mathbb{R})$ generelle lineare Gruppe über $\mathbb{R}$
3. Ist $M \neq \emptyset$ Menge, so ist $\mathbb{R}^M$ eine kommutative Gruppe mit werteweiser Addition:
   $f, g \in \mathbb{R}^M, (f + g)(m) := f_{(m)} + g_{(m)}$ für alle $m \in M$
   Beachte : 0-Element : 0-Abbildung $0 : M \to \mathbb{R} : m \longmapsto 0 \in \mathbb{R}$
   Beachte : $\mathbb{R}^{n \times 1}$ und $\mathbb{R}^R$ beides Spezialfälle.

2.5 Definition

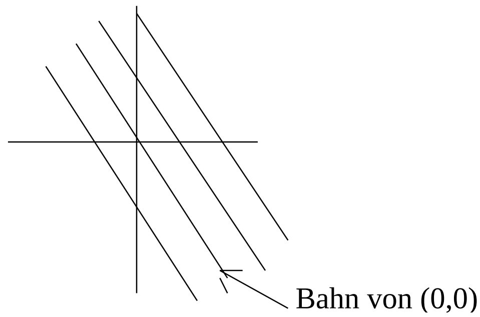
Sei G eine Gruppe und M eine Menge.

1. G *operiert* auf M, falls eine Abbildung $w : G \times M \to M : (g, m) \longmapsto gm$ gegeben ist mit Op 1 : $\underline{1} \cdot m = m$ für alle $m \in M$ (1= 1-Element der Gruppe) Op 2 : $g(hm) = (gh)m$ für alle $g, h \in G$ und $m \in M$
   w heißt Operation von G auf M
2. G operiere auf M und $m \in M$. Dann heiss t $Gm := \{gm | g \in G\} \subseteq M$ die *Bahn* von m unter G.

2.6 Beispiel

Gruppe $G = (R, +), M = \mathbb{R}^2$ Menge

1. erste Operation :
   $\mathbb{R} \times \mathbb{R}^2 \to \mathbb{R}^2 : (t, (x, y)) \longmapsto (x + t, y - 2t)$



2. zweite Operation :
   $\mathbb{R} \times \mathbb{R}^2 \to \mathbb{R}^2 : (t, (x, y)) \longmapsto (e^t x, e^{-t} y)$
   Bahnen = halbe Hyperbeln und { (0,0) }
   Beachte :$x \cdot y = e^z x \cdot e^{-t} y$

2.7 Beispiel

1. S_M operiert auf M durch Anwenden.
   Die Bahn eines jeden Elementes ist ganz M.
2. S_M operiert auf M^M durch
   $S_M \times M^M \to M^M : (g, h) \longmapsto g \circ f \circ g^{-1}$

2.8 Satz

Die Gruppe G operiere auf der Menge M. Dann bilden die Bahnen Gm mit $m \in M$ von G auf M eine Partition von M.
Beweis :
$\sim_G$ Relation auf M
$m, n \in M \; m \sim_G n :\Leftrightarrow$ ex. $g \in G$ mit $gm = n$

Behauptung : $\sim_G$ ist eine Äquivalenzrelation :
Reflexiv : $m \sim_G m \; \underline{1} \in G(\underline{1}m = m)$
Symmetrie : $m \sim_G n \Rightarrow$ ex. $g \in G$ mit $gm = n \underset{g^{-1} \in G}{\Rightarrow} m = g^{-1} n \Rightarrow n \sim_G m$
Transitivität : $m \sim_G m', m' \sim_G m''$
$\Rightarrow$ ex. $g, h \in G$ mit $gm = m', hm' = m''$
$\Rightarrow \underbrace{h(gm)}_{(hg)m} = m'' \Rightarrow m \sim_G m''$
Also : $\sim_G$ Äquivalenzrelation auf M
Die Äquivalenzklassen von $\sim_G$ sind die Bahnen von G auf M. q.e.d.

Wichtig : $M_{/\sim_G} = \{Gm | m \in M\}$ ($Gm = \{gm | g \in G\}$: Bahnen)

2.9 Beispiel

Sei $A \in \mathbb{R}^{m \times n}$ und $\bar{A} : \mathbb{R}^{n \times 1} \longmapsto \mathbb{R}^{n \times 1} x \longmapsto Ax$
Frage : Ist Bildgleichheit bez. $\bar{A}$ induziert von einer Gruppenoperation?
$x, y \in \mathbb{R}^{n \times 1} | x \sim y \Leftrightarrow \substack{\bar{A}(x) = \bar{A}(y) \\ Ax = ay}$
Antwort :
Ja: Gruppe ist $\bar{A}^{-1}_{(\{0\})} = \{x \in \mathbb{R}^{n \times 1} | Ax = 0\} \neq \emptyset$ denn $0 \in \bar{A}^{-1}_{(\{0\})}$
$x, y \in \bar{A}^{-1}_{(\{0\})} \Rightarrow \bar{A}_{x+y} = A_{x+y} = ax + Ay = 0 + 0 = 0, Ax = 0, Ay = 0$

d.h. $x+y \in \bar{A}^{-1}_{(\{0\})}$
($0 =$ neutrales Element von $A^{-1}_{(\{0\})}$)
$x \in \bar{A}^{-1}_{(\{0\})} \Rightarrow -x \in \bar{A}^{-1}_{(\{0\})}$
Also : $\bar{A}^{-1}_{(\{0\})}$ Gruppe (Untergruppe von $\mathbb{R}^{n\times 1}$
Operation von $\bar{A}^{-1}_{(\{0\})}$ auf $\mathbb{R}^{n\times 1}$
$\bar{A}^{-1}_{(\{0\})} \times \mathbb{R}^{n\times 1} \to \mathbb{R}^{n\times 1}, (b,x) \longmapsto b+x$
Klar : $\bar{A}$ ist konstant auf der Bahn ($\bar{A}_{(b+x)} = 0 + \bar{A}_{(x)}$)
Sei umgekehrt : $x,y \in \mathbb{R}^{n\times 1}$ mit $\bar{A}_{(x)} = \bar{A}_{(y)}$
$\Rightarrow x-y \in \bar{A}^{-1}_{(\{0\})}$ und $x = (x-y)+y$
Alsao : Bahnen von $\bar{A}^{-1}_{(\{0\})}$ sind die $\sim$-Äquiv.

2.10 Definition

Sei G eine Gruppe, die auf der Menge M operiert. Eine Abbildung $f : M \to N$ heißt *Invariante* der Operation, falls $f_{(gm)} = f_{(m)}$ für alle $m \in M$ und $g \in G$ gilt .Die Invariante heißt *trennend* , falls $f_{(m)} = f_{(m')}$ für $m, m' \in M$ bereits $G_m = G_{m'}$ impliziert (d.h. $\sim_f = \sim_G$)

2.11 Beispiel

1. S_n operiert auf $Pot_{(\underline{n})}$ durch $S_n \times Pot_{(\underline{n})} \to Pot_{(\underline{n})}$:
   $(g,T) \longmapsto gT := \{g^t | t \in T\}$
   d.h. : $||: Pot_{(\underline{n})} \to \mathbb{Z} : T \longmapsto |T|$ ist trennende Invariante.
2. früher : $\mathbb{R} \times \mathbb{R}^2 : (t,(x,y)) \longmapsto (e^t x, e^{-t} y\}$
   Op. $\emptyset : \mathbb{R}^t \to \mathbb{R} : (x,y) \longmapsto xy$ ist eine Invariante, die nicht trennt.

2.12 Beispiel

$Gl_n(\mathbb{R}) \times \mathbb{R}^{m\times n} \to \mathbb{R}^{m\times n} : (g,A) \longmapsto gA$
Zeige : S_n operiert auf $Pot_{(\underline{m})}$= Menge der Partitionen von $\{1,\ldots,n\}$
Bahnen $\Leftrightarrow$ { Partitionen von m }
Also : $Pot_{(\underline{n})} \to \{Pot$ von $m\}$ trennende Invariante.

Körper und Ringe

2.13 Definition

Sei K eine nicht leere Menge mit zwei Verknüpfungen $+$ und $\cdot$. $(K,+,\cdot)$ heißt Körper, falls

1. $(K,\cdot)$ eine abelsche Gruppe mit neutralem Element 0 ist.
2. Für $(K,\cdot)$ gilt das Assoziativgesetz, die Existenz des 1-Elements $\underline{1} \neq 0$ und das Kommutativgesetz. Weiter ist $(K,\cdot)$ mit $K = K - \{0\}$ eine abelsche Gruppe mit neutralem Element $\underline{1}$ (Insbesondere haben alle Elemente $\neq 0$ multiplikatives inverses(=reziprokes) Element ($a^{-1} = \frac{1}{a}$)

3. Es gilt das Distributivgesetz
   $a(b+c) = ab + ac$ für alle $a, b, c \in K$

Verzichtet man auf den Zusatz, das $(K^*; \cdot)$ abelsche Gruppe ist, so heißt $(K, +, \cdot)$ ein *kommutativer Ring* mit 1.

2.14 Bemerkung

Sei K ein Körper, dann gilt :

1. $0 \cdot a = 0$ für alle $a \in K$
2. Statt ab^{-1} schreibt man auch $\frac{a}{b}$ $(a \in K, b \in K^*)$)
   Es gilt : $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$ $(b, d \in K^*; a, c \in K)$

Beweis:

1. $0a = (0+0)a = 0a + 0a \Rightarrow 0a = 0$
2. Ü

2.15 Beispiel

1. $(\mathbb{R}, +, \cdot)$ Kurz : $\mathbb{R}$ ist ein Körper
2. $\mathbb{Q}$ ist ein Körper (Teilkörper von $\mathbb{R}$)
3. $\mathbb{Z}$ ist kein Körper sondern nur ein kommutativer Ring mit $\underline{1}$
4. $\mathbb{Z}_{/2}\mathbb{Z}$ Körper, vgl.2.2 .2

2.16 Beispiel

$\mathbb{Z}_{/2}\mathbb{Z} = F_2$

Aufgabe : Invertiere $A = (F_2)^{3\times 3}$ mit $A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$

Lösung : (mit Gauss Algorithmus)

$$\left(\begin{array}{ccc|ccc} 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{array}\right) = \left(\begin{array}{ccc|ccc} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{array}\right) = \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \end{array}\right)$$

Probe : $\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

2.17 Satz

Sei $\mathbb{C} := \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} | a, b \in \mathbb{R} \right\}$ zusammen mit der Matrizenmultiplikation und Matrizenaddition. Dann ist $(\mathbb{C}, +, \cdot)$ ein Körper gennant der Körper der *komplexen Zahlen.*
Abkürzung : $a + bi$ für $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$. Durch Identifikation $a \in \mathbb{R}$ mit $a + 0i \in \mathbb{C}$ wird $\mathbb{R}$ zu einem Teilkörper von $\mathbb{C}$, d.h. $\mathbb{R} \subseteq \mathbb{C}$ und die Addition und Multiplikation komplexer Zahlen eingeschränkt auf reelle Zahlen ist die bekannte Addition und Multiplikation in $\mathbb{R}$.

Beweis :
Multiplikation wohldefiniert ! (führt nicht aus der Menge $\mathbb{C}$ raus)
Viele Eigenschaften folgen aus den entsprechenden Eigenschaften für Matrizenaddition bzw. Multiplikation.

Kommutativität der Multiplikation :
$(a+bi)(c+di) := (ac-bd)+(ad+bc)i = (c+di)(a+bi)$

Das zu $a+bi \neq 0$ reziproke Element ist $\frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i = \frac{1}{a^2+b^2}(1-bi)$

Das $\mathbb{R}$ Teilkörper von $\mathbb{C}$ ist, folgt aus der Kommutativität. (s.o.) q.e.d.

Konjugiert komplexe Zahl :
Für $a+bi \in \mathbb{C}$ heißt $a-bi =: \overline{a+bi}$ die zu $a+bi$ konjugiert komplexe Zahl.

2.18 Satz

Sei $p \in \mathbb{N}$ eine Primzahl, also eine natürliche Zahl $p \neq$ mit $p = mn$ in $\mathbb{N} \Rightarrow n = 1$ oder $m = 1$
Sei $\sim_p$ eine Äquivalenzrelation auf $\mathbb{Z}$ definiert durch :
$a \sim_p b :\Leftrightarrow p|a-b$ (sprich p teilt $a-b$ d.h. ex. $\alpha \in integers$ mit $p\alpha = (a-b)$
Dann:

1. Die Addition und Multiplikation in $\mathbb{Z}$ ist verträglich mit $\sim_p$, d.h. $[a],[b] \in \mathbb{Z}_{/\sim_p}$ mit $\alpha \in [a], \beta \in [b]$
   $\Rightarrow$
   $\alpha + \beta \in [c]$
   $\alpha\beta \in [d]$
   d.h. auf $\mathbb{Z}_{/\sim_p}$ ist eine Addition und Multiplikation (vertreterweise) definiert.
   Statt $\mathbb{Z}_{/\sim_p}$ schreibt man $\mathbb{Z}_{/p}\mathbb{Z}$ für $(\mathbb{Z}_{/\sim_p}, +, \cdot)$ statt [a] schreibt man $a+p\mathbb{Z}$ $(= \{a+pz|z \in \mathbb{Z}\})$
2. $\mathbb{Z}_{/p}\mathbb{Z}$ ist ein Körper. Bez. : F_p

Beweis :

1. Seien $\alpha, \alpha' \in [a], \beta, \beta' \in [b]$
   $\Rightarrow$ ex. $z, u \in \mathbb{Z}$ mit
   $\alpha' = \alpha + pz$
   $\beta' = \beta + pu$
   $\Rightarrow \alpha' + \beta' = \alpha + \beta + p(z+u)$, d.h. $\alpha' + \beta' \sim_p \alpha + \beta$
   entsprechend für Multiplikation.
   Damit ist + und - von Äquivalenzklassen über Vertreter wohldefiniert.
2. (a) $\mathbb{Z}_{/p}\mathbb{Z}$ kommutativer Ring mit $\underline{1}$ (gilt für beliebige $p \in \mathbb{Z}$)
   Alle Eigenschaften (Assoziativität für +,.. etc.) übertragen sich
   von $\mathbb{Z}$ auf $\mathbb{Z}_{/p}\mathbb{Z}$ $0 + p\mathbb{Z} = [0]$
   1-Element von $\mathbb{Z}_{/p}\mathbb{Z}$ $1 + p\mathbb{Z} = [1]$
   (b) $\mathbb{Z}_{/p}\mathbb{Z}$ Körper : Zeige nur noch $a + p\mathbb{Z} = p\mathbb{Z}$
   $\Rightarrow$ ex $b + p$ mit $(a+p\mathbb{Z})(b+p\mathbb{Z}) = 1 + p\mathbb{Z}$, d.h. ex. $n \in \mathbb{Z}$ mit
   $a + b + np = \underline{1}$ Nach Euklidischem Algorithmus : q.e.d. (s.u.)

2.19 Bemerkung

Seien $a, b \in \mathbb{Z} b \neq 0$
$|b| := \begin{cases} b & b \leq \\ -b & b < 0 \end{cases}$ (Absolutbetrag)
Dann ex. ein $q, r \in \mathbb{Z}$ mit
$a = qb + r$ und $0 \leq r < |b|$
r heißt auch der kleinste positive Rest von a modula b ($b/a \Leftrightarrow r = 0$)

2.20 Algorithmus(Euklidischer) 1.Teil

Gegeben : $a, b \in \mathbb{Z}, a = 0, b \neq 0$
Gesucht : Der größt gemeinsame Teiler t von a und b ,
d.h.$\underbrace{t|aundt|b}_{*1}$ und $\underbrace{d|a, d|b \Rightarrow d|t}_{*2}$

Algorithmus :
Setze $a_1 := a, a_2 = b$ und für $n > 2$ $a_n := a_{n-2} mod a_{n-1}$ falls $a_{n-1} \neq 0$
Nach endlich vielen Schritten bekommt man ein $k \in \mathbb{N}$ mit $a_{k+1} = 0, a_k \neq 0$
$\Rightarrow a_h = ggT(a, b)$ (Größte gemeinsamen Teiler von a und b)
$\mathbb{R}, +$ Gruppe und operiert auf $\mathbb{R}^2$
$1 : \omega_1 \mathbb{R} * \mathbb{R}^2 \to \mathbb{R}^2 : (t, (x, y)) \longmapsto (x + t, y - 2t)$
$2 : \omega_1 \mathbb{R} * \mathbb{R}^2 \to \mathbb{R}^2 : (t, (x, y)) \longmapsto (e^t x, e^{-t} y)$

Oder (etwas anschaulicher) :
Gegeben : $a, b \in \mathbb{Z} - \{0\}$
Gesucht : $ggT(a, b)$

Algorithmus : $a_1 := a, a_2 := b, a_3 := b$
$a_n := a_{n-2} mod a_n - 1$
$\Rightarrow$ existiert ein kleinstes k mit $a_{k+1} = 0$
Weiter gilt : $a_k = ggT(a, b)$

Beweis :

1. Terminierend : Klar, wenn $a_n \in \mathbb{Z}_{\geq 0} \forall v \geq 3$ und ab dem dritten Glied ist die Folge streng monoton fallend : $a_{n-1} > a_n \forall n \geq 3$.
2. $a_k = ggT(a, b)$ genügt zu zeigen : $ggT(a_{n-2}, a_{n-1}) = ggT(a_{n-1}, a_n)$
Klar denn : $a_{n-2} = q_{n-2} a_{n-1} + a_n$ mit $q_{n-2} \in \mathbb{Z}$ im letzten Schritt : $ggT(a_k, 0) = a_k$
q.e.d.

2.21 Bemerkung

Sei $E := \left\{ \begin{pmatrix} a \\ b \end{pmatrix} | a, b \in \mathbb{Z}, b \neq 0 \right\}$ und $\epsilon : E \to \mathbb{Z}^{2\times 1} : \begin{pmatrix} a \\ b \end{pmatrix} \longmapsto \begin{pmatrix} b \\ amodb \end{pmatrix}$

1. Eukl. Algorithmus:
Iteriere das Anwenden von ϵ solange es geht :
d.h. $\epsilon^{k-1} \left(\begin{pmatrix} 0 \\ b \end{pmatrix} \right) = \begin{pmatrix} t \\ 0 \end{pmatrix}$
$\Rightarrow t = ggT(a, b)$

2. Es gilt :
$\epsilon\left(\begin{pmatrix} a \\ b \end{pmatrix}\right) = \begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} b \\ r \end{pmatrix}$
(q hängt von a und b ab.) Wobei $a = bq + r$ mit $q \in \mathbb{Z}, 0 \leq r < |b|$

2.22 Algorithmus(Euklidischer) 2.Teil

Gegeben : $a, b \in \mathbb{Z} - \{0\}$
Gesucht : $t = ggT(a, b)$ und $\alpha, \beta \in \mathbb{Z}$ mit $\alpha a + \beta b = t$

Algorithmus :
Wie oben $a_n = q_n a_{n+1} + a_{n+2}$
Definiere :
$A_1 := \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix}$,
$A_n := \begin{pmatrix} 0 & 1 \\ 1 & -q_n \end{pmatrix} A_{n-1}$
Dann liefert die 1. Zeile von A_{n-1} das gewünschte Paar (α, β):
$A_{k-1}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} t \\ 0 \end{pmatrix}$
$\begin{pmatrix} \alpha & \beta \\ egal & egal \end{pmatrix}$

2.23 Beispiel

1. Bestimme $ggT(1002, 912)$:
   Folge : $1002, 912, 90, 12, 6, 0$ also $ggT(1002, 912) = 6$
2. Bestimme $(25 + 31\mathbb{Z})^{-1}$ in $\mathbb{Z}_{/31\mathbb{Z}} = F_{31}$
   $31 = 1 \cdot \underline{25} + \underline{6}$
   $25 = 4 \cdot \underline{6} + \underline{1}$
   $6 = 6\ cdot 1 + 0$
   $$\begin{pmatrix} 0 & 1 \\ 1 & -6 \end{pmatrix}\left(\begin{pmatrix} 0 & 1 \\ 1 & -4 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}\right) = \begin{pmatrix} -4 & 5 \\ egal & egal \end{pmatrix}$$
   $-4 \cdot 31 + 5 \cdot 25 = \underline{1}\ (/mod 31)$
   $(5 + 31\mathbb{Z})(25 + 31\mathbb{Z}) = 1 + 31\mathbb{Z}$
   $1 + 31\mathbb{Z} = \{1 + 31z | z \in \mathbb{Z}\} = \{..., -30, 1, 32, ...\}$ Äquivalenzklassen von $\mathbb{Z}_{/31\mathbb{Z}}$ heißen *Restklassen.*

2.24 Folgerung

1. Sei $p \in \mathbb{N}$ eine Primzahl.
   Für beliebige $a, b \in \mathbb{Z}$ gilt : $p|ab \Rightarrow p|a$ oder $p|b$
2. Jedes Element $a \neq 0$ mit $a \in \mathbb{Z}$ hat bis auf die Reihenfolge und Vorzeichen eine <u>eindeutige</u> Produktzerlegung in Primfaktoren.

Beweis :

1. Annahme : $p \not| a \underset{Eukl.Alg: ggT(p,a)=1}{\Rightarrow}$ ex. $\alpha, \beta \in \mathbb{Z}$ mit $\alpha p + \beta a = 1$
   $\Rightarrow p|(\alpha p + \beta a)b = b$

2. (Skizze): Sei $a \in \mathbb{Z}, a \neq 0$ ist a Prim : $\surd$
   Andernfalls ex $b, c \in \mathbb{Z}$ mit $a = bc, 1 < |b|, |c| < |a|$
   Faktorisiere weiter (b und c). Terminiert nach endlich vielen Schritten $\rightsquigarrow$ Zerlegung in Primzahlen.
   Eindeutigkeit folgt aus 1) . q.e.d.

2.25 Satz

Sei R ein kommutativer Ring mit 1, in welchem gilt :
$a, b \in \mathbb{R}, ab = 0 \Rightarrow a = 0$ oder $b = 0$. Dann gibt es einen Körper K, genannt der *Quotientenkörper* von R, der R enthält.
Genauer :

1. Die Elemente von K werden geschrieben als $\frac{a}{b}$ mit $a, b \in R, b \neq 0$
   Es gilt : $\frac{a}{b} = \frac{a'}{b'} \Leftrightarrow ab' = ba'$
   Das Element $r \in \mathbb{R}$ wird mit $\frac{r}{1} \in K$ identifiziert.
2. $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{ba}$ und $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$

Beweis (Motivation+Skizze):
Wir wollen die Gleichungen $bx_{a,b} = a$ mit $a, b \in R, b \neq 0$ lösen.
Gefühl : $(cb)x_{a,cb} = (ca)$ sollte $x_{a,b} = x_{ca+cb}$
Äquivalenzrelation auf $\underbrace{R}_{a} \times \underbrace{R}_{b} - \{0\}$
$(a, b) \sim (ca, cb)$
Name für die Äquivalenzklasse von (a, b) : $\frac{a}{b}$
Addition und Multiplikation :
z.B.:
$bx_{a,b} = a \ / \cdot d$
$dx_{c,d} = c \ / \cdot b$
$\Leftrightarrow db(x_{a,b}) + x_{c,d}) = da + cb$ q.e.d. (nicht wirklich aber es soll reichen.)
$\mathbb{Z} = R \rightsquigarrow K = \mathbb{Q}$
Standardvertreter $\frac{a}{b} = \frac{a'}{b'}$ $ggT(a', b') = 1$ geht wegen der eindeutigen Primfaktorzerlegung.

Vektorräume

2.26 Beispiel

Folgende Abbildungen $\varphi : D \to W$ sind linear im Sinne, daß
$\varphi(ax) = a\varphi(x)$
$\varphi(x + y) = \varphi(x) + \varphi(y)$
für alle $a \in X$, $x, y \in D$, X ist ein Körper

1. Sei $A \in K^{m \times n}$, K Körper,
   $D = K^{n \times 1}, W = K^{m \times 1}, \varphi = \bar{A}, K^{n \times 1} \to K^{m \times 1} : x \longmapsto Ax$
2. Sei $K = \mathbb{R}, D$ =Menge der stetig differenzierbaren Funktionen auf $\mathbb{R}(\mathbb{R} \to \mathbb{R})$
   W = Menge der stetigen Funktionen $\mathbb{R} \to \mathbb{R}$
   $\varphi : f \longmapsto f' =$ 1. Ableitung von f
3. Sei $D = W$ = Menge der stetigen Funktionen $\mathbb{R} \to \mathbb{R}$
   φ :Integral
   $\varphi : f \longmapsto If$ mit $(If)_{(x)} = \int\limits_a^x f_{(u)} du$

4. Sei $D = W = K^{\mathbb{N}}$, K beliebiger Körper und φ einer der Schiebeoperatoren
   $\varphi : (a_1, a_2, a_3, ...) \longmapsto (a_2, a_3, ...)$
   oder $\varphi : (a_1, a_2, a_3, ...) \longmapsto (0, a_1, a_2, ...)$
5. Sei $D = W = K^{\mathbb{N}}$, K beliebiger Körper und φ der Differenzenoperator
   $\varphi : (a_1, a_2, a_3, ...) \longmapsto (a_2 - a_1, a_3 - a_2, a_4 - a_3, ...)$ und sein Rechtsinverses
   $\varphi : (a_1, a_2, a_3, ...) \longmapsto (a_1, a_1 + a_2, a_1 + a_2 + a_3, ...)$
   (arithmetischer Mitteloperator) $\varphi : (a_1, a_2, a_3, ...) \longmapsto (a_1, fraca_1 + a_2 2, \frac{a_1+a_2+a_3}{3}, ...)$
6. Sei $D =$ Menge der konvergenten reellen Folgen, $K = \mathbb{R}, W = \mathbb{R}, \varphi =$ Grenzwertoperator
   $\varphi : (a_1, a_2, a_3, ...) \longmapsto \underset{n\to\infty}{lim}\ a_n$

2.27 Definition

Sei K ein Körper. Eine abelsche Gruppe $(\mathcal{V}, +)$ zusammen mit einer äußeren Verknüpfung $K \times \mathcal{V} \to \mathcal{V} : (a, X) \longmapsto aX$ heißt *Vektorraum* über K oder *K-Vektorraum* (K-VR) falls gilt (für alle $a, b \in K, X, Y \in \mathcal{V}$) :

1. $a(X + Y) = aX + aY$
2. $(a + b)X = aX + bX$
3. $(ab)X = a(bX)$
4. $\underline{1}X = X$

Die Elemente von $\mathcal{V}$ heißen *Vektoren*.

2.28 Bemerkung

Ist $\mathcal{V}$ ein K-VR (K-Vektorraum), so gilt :

1. $0X = 0$ für alle $X \in \mathcal{V}$ (1. Null $\subseteq K$, 2. Null $\in \mathcal{V}$)
2. $(-1)X = -X$ für alle $X \in \mathcal{V}$

Beweis :

1. $0X = (0 + 0)X = 0X + 0X \Rightarrow 0X = 0$
2. Ü

2.29 Beispiel

Sei K ein Körper, $M \neq \emptyset$ Menge :
$\Rightarrow K^M$ ist ein K-VR mit

1. werteweiser Addition $f, g \in K^M$
   $f + g : M \to K : m \longmapsto f_{(m)} + g_{(m)}$
2. werteweiser Multiplikation
   $af : M \to K : m \longmapsto af_{(m)}\ \forall a \in K, f \in K^M$

Beachte : Spezialfälle : $K^n, K^{1\times n}, K^{m\times n}, K^K, K^{\mathbb{N}}, K = K^1$

2.30 Beispiel

Seien $\mathcal{V}$,$\mathcal{W}$ zwei K-VR.Auf dem kartesischen Produkt $\mathcal{V} \times \mathcal{W}$ definieren wir :
$+ : (V \times W) \times (V \times W) \to (V \times W) : ((v, w), (v', w')) \longmapsto (v+v', w+w')$ eine komponentenweise Addition und durch
$K \times (V \times W) \to (V \times W) : (a, (v, w)) \longmapsto (av, aw)$ eine komponentenweise Multiplikation.

2.31 Definition

Ist $\mathcal{V}$ ein K-VR, so heißt eine Teilmenge $\mathcal{T} \subset \mathcal{V}$. ein *Teil(vektor)raum* oder *Unter(vektor)raum* von $\mathcal{V}$ falls

1. $\mathcal{T} \neq \emptyset$
2. Für $X, Y \in \mathcal{T}$ und $a, b \in K \to aX + bY \in \mathcal{T}$

Schreibweise : $\mathcal{T} \leq \mathcal{V}$.

2.32 Beispiel

Lineare Codes (aus der Nachrichtenübertragung)
F_2 Teilräume von F_2^n (n-Tupel von 0 und 1)
Hamming Code : $\{aA + bB + cC | a, b, c \in F_2\}$
lineare Codes der Länge 7 (=n) mit 8 verschiedenen Folgen :
$A, B, C =$ Zeilen von : $\begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$

2.33 Definition

Sei $\mathcal{V}$ ein K-VR ,$\mathcal{T}_1$.,$\mathcal{T}_2$. $\leq \mathcal{V}$
Falls jedes $V. \in \mathcal{V}$ in eindeutiger Weise als $V - T_1 + T_2$ mit $T_1 \in \mathcal{T}_1$ und $T_2 \in \mathcal{T}_2$ geschrieben werden kann, heißt $\mathcal{V}$ die *(innere) direkte Summe* von $\mathcal{T}_1$ und $\mathcal{T}_2$:
Man schreibt $\mathcal{V} = \mathcal{T}_1 \oplus \mathcal{T}_2$ oder $\mathcal{V} = \mathcal{T}_1 \oplus_i \mathcal{T}_2$

2.34 Definition

Seien $\mathcal{V}$ und $\mathcal{W}$: K-VR.
Eine Abbildung $\varphi : \mathcal{V} \to \mathcal{W}$ heißt linear (oder ein *K-Homomorphismus*) falls für alle $X, Y \in \mathcal{V}$ und alle $a, b \in K$ gilt :
$\varphi(aX + By) = a\varphi_{(x)} + b\varphi_{(Y)}$

Ist φ noch zusätzlich bijektiv(injektiv,surjektiv), so heißt φ ein *Isomorphismus*(*Mono-,Epimorphismus*) (Ist $\mathcal{V} = \mathcal{W}$, so heißt φ auch *Endomorphismus*) (bijektive Endomorphismen heißen *Automorphismen*)
K-VR $\mathcal{V}$ und $\mathcal{W}$, zwischen denen ein Isomorphismus existiert heißen *isomorph*:
Zeichen : $\mathcal{V} \cong \mathcal{W}$

2.35 Satz

Sei $\varphi : \mathcal{V} \to \mathcal{W}$ lineare Abbildung von K-VR
Dann:

1. $Kern(\varphi) := \varphi^{-1}_{(\{0\})} \leq \mathcal{V}$ genannt der *Kern* von φ.
2. $\text{Bild}_{(\varphi)}$

Beweis :

1. $0 \in Kern(\varphi)$, also $Kern(\varphi) \neq \emptyset$
   $X, Y \in Kern(\varphi)$ und $a, b \in K \Rightarrow (aX + bY) = a\varphi(X) + b\varphi(Y) = 0$
   d.h. $aX + bY \in Kern(\varphi)$
2. $0 = \varphi(0) \in Bild(\varphi)$, also $Bild(\varphi) \neq \emptyset$
   Sei $X, Y \in Bild(\varphi)$ $a, b \in K \Rightarrow$ ex. $X', Y' \in \mathcal{V}$ mit $\varphi(X') = X$ und $\varphi(Y') = Y$
   $\Rightarrow \varphi(aX' + bY') = a\varphi(X') + b\varphi(Y') = aX + bY$
   d.h. $aX + bY \in Bild(\varphi)$ q.e.d.

2.36 Beispiel

Sei $\mathcal{V} = \mathcal{T}_1 \oplus \mathcal{T}_2$ ($\oplus_i$) ($\leq \mathcal{V}$)

1. $\pi_i : \mathcal{T}_1 \oplus \mathcal{T}_2 \to \mathcal{T}_i : T_1 + T_2 \longmapsto T_i$
   ist eine lineare Abbildung (Epimorphismus)
   Es gilt :
   $Kern(\pi_1) = \mathcal{T}_2$
   $Kern(\pi_2) = \mathcal{T}_1$

2. $\iota_i : \mathcal{T}_i \to \mathcal{V} = \mathcal{T}_1 \oplus \mathcal{T}_2 : T_i \to T_i$ ist eine injektive ($Kern(\iota_i) = \{0\}$) lineare Abbildung (Monomorphismus)
   " Die Einbettung von $\mathcal{T}_i$ in $\mathcal{V}$"
   Es gilt : $Bild(\iota_i) = \mathcal{T}_i$ $(i = 1, 2)$
   weiter : $\pi_i \circ ???? = Id_{\mathcal{T}_i}$ $(i = 1, 2)$ weiter : $\pi_2 \circ i_1 : \mathcal{T}_1 \to \mathcal{T}_2, T_1 \longmapsto 0$ (Nullabbildung)

2.37 Satz

$A \in K^{m \times n}, b \in K^{m \times 1}$ gegeben.
Das lineare Gleichungssystem
(*) : $Ax = b$ sei lösbar, d.h.$b \in Bild(\bar{A})$

1. Die Lösungsmenge des zugehörigen *homogenen Gleichungssystems*, also
   (*0) $Ax = 0$ (0 = Nullspalte $\in K^{n \times 1}$ nämlich $Kern(\bar{A})$
2. Die nicht leeren Fasern von $\bar{A}$ sind gleichzeitig die Bahnen von $Kern(\bar{A})$ auf $K^{n \times 1}$ unter der Operation $Kern(\bar{A}) \times K^{n \times 1} \to K^{n \times 1} : (X, Y) \longmapsto X + Y$
   Ist insbesondere $X_0 \in K^{n \times 1}$ eine Lösung von (*) so durchläuft $X + X_0$ mit $X \in Kern(\bar{A})$ die Lösungen von (*) (X sind hier die Lösungen des Gl. Systems $Ax = 0$

Beweis :

1. Die Lösungsmenge von $(X_0) = Kern(\bar{A})$
   $\underset{2.35}{\Rightarrow}$ Behauptung

2. Operation $(X \in K^{n\times 1})$:
   $0 \in Kern(\bar{A})$
   $(0, X) \longmapsto 0 + X = X$
   $X_0, X_0' \in Kern(\bar{A})$
   $(X_0 + X_0') + X = X_0 + (X_0' + X)$

   Behauptung : Jede Bahn liegt in einer Lösungsmenge von (*) für ein geeignetes b
   Beweis : $AY = b$ und $X \in Kern(\bar{A}) \Rightarrow A(Y + X) = b$

   Behauptung : Y, Y' Lösungen von (*). ex $X \in Kern(\bar{A})$ mit $Y = X + Y'$
   Beweis : Wähle $X = Y - Y' \in Kern(\bar{A})$ q.e.d.

2.38 Definition

Sei $\mathcal{V}$ ein K-VR. Eine Äquivalenzrelation $\sim$ auf $\mathcal{V}$ heißt verträglich mit der VR-Struktur oder *linear* oder eine *Kongruenz*, falls aus
$X \sim Y, X' \sim Y'$ für $X, X', Y, Y' \in \mathcal{V}$ folgt $aX + bX' \sim aY + bY' \forall a, b \in K$

2.39 Beispiel

1. Ist $\varphi : \mathcal{V} \to \mathcal{W}$ linear und $\sim_\varphi =$ "Bildgleichheit bezüglich φ $(V \sim_\varphi V' \Leftrightarrow \varphi(V) = \varphi(V')$
   $\Rightarrow \sim_\varphi$ ist eine Kongruenz
2. $\mathcal{U} \leq \mathcal{V}$, so ist $\sim_\mathcal{U}$ eine Kongruenz definiert durch :
   $X \sim_\mathcal{U} Y :\Leftrightarrow X - Y \in \mathcal{U}$

2.40 Lemma

Ist $\sim$ eine Kongruenz auf K-VR $\mathcal{V}$. Dann gilt :

1. Die *Kongruenzklasse* [0] der Nullklasse (oder war es der Nullvektor??) ist ein Teilraum von $\mathcal{V}$. $[0] \leq \mathcal{V}$
2. $\sim = \sim_\mathcal{U}$ und $\mathcal{U} = [0]$
3. Die Konguenzklasse $[X]$ von $\mathcal{V}(X \in \mathcal{V})$ ist gegeben durch $X + \mathcal{U} := \{X + U | U \in \mathcal{U}\}$ also durch die Bahn von X unter der Operation von $\mathcal{U}$ auf $\mathcal{V}$ durch Addition

Beweise :

1. $[0] \neq \emptyset$ denn $0 \in [0]$
   $X, Y \in [0], a, b \in K \Rightarrow X \sim 0$ und $Y \sim = \Rightarrow aX + bY \sim a0 + b0 = 0$
   d.h. $aX + bY \in [0]$ q.e.d.
2. Behauptung :
   $\forall X, Y \in \mathcal{U}$
   $X \sim Y \Leftrightarrow X - Y \in \mathcal{U}$
   Klar : $X \sim Y \Leftrightarrow X - Y \sim 0 \Leftrightarrow X - Y \in \mathcal{U}$
3. $Z \in X + U \Leftrightarrow Z = X + U$ für ein $U \sim 0$
   $\Leftrightarrow Z \sim X$, d.h. $Z \in [X]$
   d.h. $[X] = X + \mathcal{U}$
   Klar : $\mathcal{U} \times \mathcal{V} \to \mathcal{V} : (U, V) \to U + V$ ist Operation von $\mathcal{U}$ auf $\mathcal{V}$ und $X + \mathcal{U}$ ist eine Bahn dieser Operation. q.e.d.

2.41 Satz

Sei $\mathcal{U} \leq \mathcal{V}$ (K-VR) und $\sim:=\sim_{\mathcal{U}}$
Die Menge $\mathcal{V}_{/\sim}$ der Kongruenzklassen wird mit $\mathcal{V}_{/\mathcal{U}}$ bezeichnet (Lies V modulo U). Die Elemente von $\mathcal{V}_{/\mathcal{U}}$ heißen auch *Restklassen* nach $\mathcal{U}$ und $\mathcal{V}_{/\mathcal{U}}$ heißt auch *Faktorraum*, *Quotientenraum* oder *Restklassenraum* von $\mathcal{V}$ nach $\mathcal{U}$

1. $\mathcal{V}_{/\mathcal{U}}$ wird mit der wohldefinierten Addition
   $(X+\mathcal{U})+(Y+\mathcal{U}) := (X+Y)+\mathcal{U}\ \forall X,Y \in \mathcal{V}$
   und Multiplikation :
   $a(X+\mathcal{U}) := aX+\mathcal{U}\ \forall x \in \mathcal{V}, a \in K$
   zu einem K-VR
2. Die Abbildung
   $\gamma : \mathcal{V} \to \mathcal{V}_{/\mathcal{U}} : X \longmapsto X+\mathcal{U}$
   ist eine lineare Abbildung,genannt der *natürliche Epimorphismus* von $\mathcal{V}$ auf $\mathcal{V}_{/\mathcal{U}}$.
   Es gilt : $Kern(\gamma) = \mathcal{U}$

Also : $\mathcal{U} \leq \mathcal{V} \Rightarrow \mathcal{U}$ Kern einer linearen Abbildung.

Beweis:

1. Zeige : + ist Vertreterunabhängig
   d.h. ist
   $X+\mathcal{U} = X'+\mathcal{U}\ (X,X' \in \mathcal{V})$
   $Y+\mathcal{U} = Y'+\mathcal{U}\ (Y,Y' \in \mathcal{V})$
   $\overset{!}{\Rightarrow} (X+Y)+\mathcal{U} = (X'+Y')+\mathcal{U}$
   $\rightarrow$ ex. $U_1, U_2 \in \mathcal{U}$ mit $X' = X+U_1$, $Y' = Y+U_2$
   $\Rightarrow (X'+Y')-(X+Y) = (X+U_1+Y+U_2)-(X+Y) = U_1+U_2 \in \mathcal{U}$ also $\surd$
   Zeige : $X+\mathcal{U} = X'+\mathcal{U} \underset{a\in K}{\overset{!}{\Rightarrow}} aX+\mathcal{U} = aX'+\mathcal{U}$
   ex. $U \in \mathcal{U}$ mit $X' = X+U$
   $(aX')-(aX) = a(X+U)-aX = aU \in \mathcal{U}$ also $\surd$
   Überprüfe Vektorraumaxiome für $\mathcal{V}_{/\mathcal{U}}$:
   $+ : \surd$
   Assoziativität für + : $\surd$ für $\mathcal{V}$ erfüllt,
   0-Element : $0+\mathcal{U} = \mathcal{U}$
   negative zu $X+\mathcal{U} : -X+\mathcal{U}$
   Kommutativität : $\surd$
   (alles bereits für $\mathcal{V}$ erfüllt)
2. $\gamma(aX+bY) = \underbrace{aX+bY+\mathcal{U}}_{Restklasse}\ a,b \in K, X,Y \in \mathcal{V}$
   $= a(X+\mathcal{U})+b(Y+\mathcal{U}) =$
   $= a\gamma(X)+b\gamma(Y)$ (γ linear)
   γ surjektiv : $\surd$, $Kern(\gamma) = \mathcal{U}\ \surd$ qed.

2.42 Hauptsatz(Homomorphiesatz)

Sei $f : \mathcal{V} \to \mathcal{W}$ eine lineare Abbildung von K-VR.
Dann faktorisiert f in die Komposition des natürlichen Epimorphismus $\gamma_f : \mathcal{V} \to \mathcal{V}_{Kern(f)}$ und des Monomorphismus $f : \mathcal{V}_{Kern(f)} \to \mathcal{W} : X+Kern(f) \longmapsto f(x)$
also $f = \bar{f} \circ \gamma$. d.h. wir haben ein kommutatives Diagramm

Beachte : $\bar{f} \rightsquigarrow$ Isomorphismus von $\mathcal{V}_{Kern(f)}$ auf $Bild(f)$

Beweis :
Im Hauptsatz 1.50 bereits für Mengen bewiesen.
Zeige (insbesondere $\bar{f}$ wohldefiniert) nur noch linearität von γ(in 2.41 gezeigt) und $\bar{f}$ (folgt aus der Linearität von f).

2.43 Beispiel

Sei $A \in K^{m\times n}, f = \bar{A} \to K^{m\times 1} : x \longmapsto Ax$ Homomorphiesatz :

1. Diejenigen $b \in K^{m\times 1}$ für die $Ax = b$ lösbar ist, bilden einen Teilraum von $K^{m\times 1}$, nämlich $Bild(f)$
2. Dieser Teilraum $Bild(f)$ ist Isomorph zu $K^{m\times 1}_{/Kern(f)}$ (vermöge $\bar{f}$)
3. Die Lösungsmenge von $Ax = b$ für ein $b + Bild(f)$ ist eine Restklasse (früher Faser) nach $Kern(f)$ und wird durch den Isomorphismus von $K^{m\times 1}_{/Kern(f)}$ auf $Bild(f)$ auf b abgebildet. Insbesondere bildet die Gesamtheit aller Lösungsmengen $\neq \emptyset$ (Restklassen nach $Kern(f)$) einen VR
4. Je größer der Kern von f ist, für desto weniger rechte Seiten b ist das Gleichungssystem lösbar.

2.44 Beispiel

Homomorphiesatz auf $\oplus$ angewendet :
$\pi_1 : \underbrace{\mathcal{T}_1 \oplus \mathcal{T}_2}_{\mathcal{V}} \to \mathcal{T}_1 : T_1 + T_2 \to T_1$ eine surjektive lineare Abbildung (Epimorphismus) mit $Kern(\pi_1) = \mathcal{T}_2$
Homomorphiesatz :
$(\mathcal{T}_1 \oplus \mathcal{T}_2)_{/\mathcal{T}_2} \cong \mathcal{T}_1$
$\mathcal{T}_1$ ist eine Transversale für die Restklassen von $(\mathcal{T}_1 \oplus \mathcal{T}_2)_{/\mathcal{T}_2}$

4) Polynomringe

2.45 Definition

Potenzreihen Sei K ein Körper

1. Auf dem K-VR $K^{\mathbb{Z}\geq 0}$ definieren wir eine Multiplikation :
$(a_0, a_1, ...)(b_0, b_1, ...) := (c_0, c_1, ...)$
mit $c_0 = a_0b_0, c_1 = a_0b_1 + a_1b_0, c_2 = a_0b_2 + a_1b_1 + a_2b_0$
algemein : $n \geq 0$
$c_n = a_0b_n + a_1b_{n-1} + ... + a_nb_0$
$(K^{\mathbb{Z}\geq 0}, +, \cdot)$ zusammen mit der K-VR-Struktur von $K^{\mathbb{Z}\geq 0}$ wird mit $K[[x]]$ bezeichnet, den *Potenzreihenring* , über K in $x := (0, 1, 0, 0, ...)$ genauer den Ring der *formalen Potenzreihen* über K (Statt $(a_0, a_1, ..)$ schreibt man auch $\sum_{i=0}^{\infty} a_ix^i$)
2. Eine Potenzreihe $(a_0, a_1, ...) \in K[[x]]$ heißt *Polynom*, falls ein $n \in \mathbb{Z}_{\geq 0}$ existiert mit $a_i = 0 \forall i > n$. Für $a \neq 0$ heißt das kleinste derartige n der Grad von a. ($Grad(0) = -\infty$)
Die Menge aller Polynome zusammen mit der K-VR-Struktur und der von $K[[x]]$ ererbten Multiplikation heißt der *Polynomring* $K[x]$ von $K(\in x)$.
(Statt x jeder andere Buchstabe möglich)(x heißt auch *Unbestimmte*

2.46 Beispiel

(Schriftliche Multiplikation ohne Überträge)
In $F_5[x]$ berechne ab von
$:= (1,2,3,4,0,0,...)$, $b := (4,3,2,1,0,0,...)$

4	3	2	1	0	0	0	...
0	3	1	4	2	0	0	...
0	0	2	4	1	3	0	...
0	0	0	1	2	3	4	0
4	1	0	0	0	1	4	

2.47 Bemerkung

1. $1 := (1,0,0,...) \in K[x]$ ist das neutrale Element der Multipl. in $K[[x]]$ und $K[x]$.
2. $xa = (0, a_0, a_1, ...) \forall a \in K[[x]]$ (eigentlich nur den Grad erhöhen)
3. Es gilt $x^i x^j = x^{(i+j)} \forall i,j \geq 0$ wobei $x^0 = \underline{1}$
   (Multipl. der *Monome* entspricht der Addition der Exponenten)
   $^*K[x]$ ist der Halbgruppenring von $(\mathbb{Z}_{\geq 0}, +)$
4. Sei $a \in K[x]$ ein Polynom vom Grad n.
   $\Rightarrow a = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n (a_i \in K)$
   $\rightsquigarrow$ Identifikation
   $K \leftrightarrow \{0\} \cup \{a \in K[x] | Grad(a) = 0\}$
5. $K[x]_{Grad<n} := \{0\} \cup \{a \in K[x] | Grad(a) < n\}$ ist Teilvektorraum von $K[x]$
6. Für $a, b \in K[x] - \{0\}$ gilt :
   $Grad(ab) = Grad(a) + Grad(b)$

2.48 Satz

Sei K Körper.

1. $K[x]$ ist ein kommutativer Ring mit 1
2. Für $a, b \in K[x]$ mit $b \neq 0$ ex. eindeutige $q, r \in K[x]$ mit $a = qb + r$, $Grad(r) < Grad(b)$ oder $r = 0$

   Beweis :
   Multipl. kommutativ, 1=1-Element , $\surd$
   Assoziativität der Multiplikation :
   Benutze die Bilinearität (*) der Multipl:
   $(a + b)c = ac + bc$ und $(\alpha a)c = \alpha(ac)$ $\forall a, b \in K[x], \forall \alpha \subset K, \forall c \in K[x]$
   (Kann man auch als Distributivgesetz verstehen)
   (Linearität der Rechtsmultiplikation mit c
   Linearität der Linksmultiplikation mit c wegen Kommutativität)
   Also, da jedes Polynom Linearkombination der x^i ist, reduziert sich wegen (*) die Assoziativität auf Assoziativität der Produkte der x^i :
   $x^i(x^j x^j) = (x^i x^j)x^k$ $\forall i, j, k \in \mathbb{Z}_{\geq 0}$
   Dies ist klar, denn beide Seiten $= x^{i+j+k}$ $((\mathbb{Z}, +)$ ist assoz.)

   Genauer : $a(bc) = (ab)c \forall a, b, c \in K[x]$
   Beweis (durch Induktion nach Grad(c)):
   $\surd$ wenn Grad(c) = 0 (Linearität)

Angenommen : Beh $\surd$ für Grad(c)$\leq n$
Zeige Beh für Grad(c)$= n+1$
Schreibe : $c = c + c_{n+1}x^{n+1}$ mit Grad(c) $\leq n$
$a(bc) = a(b(c + c_{n+1}x^{n+1}))$
$= a(bc + c_{n+1}bx^{n+1})$
$= a(bc) + c_{n+1}a(bx^{n+1})$ (Schieben)
$= (ab)c + c_{n+1}(ab)x^{n+1}$
$= (ab)(c + c_{n+1}x^{n+1})$
$= (ab)c$ Ass. $\surd$
Distributivgesetz : s.o. (Linearität)

3. (Lange Division ohne Überträge)
   Sei Grad(a)=m , Grad(b)=n. Falls $m < n$ fertig.
   Falls nicht ersetze a durch $a - \frac{a_m}{b_n}x^{m-n}b$ und belasse b.
   Nach endlich vielen Schritten ist der Grad des 1. Polynoms kleiner als n und wir können $q = \frac{a_m}{b_n}x^{m-n} + \ldots$
   sowie r= letztes Polynom in der Reihe der a's ablesen
   $\rightsquigarrow$ Existenz von q und r.

   Eindeutigkeit : $a = q_1b + r_1$ mit Grad(r_1) <Grad(b)
   $\Rightarrow r - r_1 = (q - q_1)b$
   Wäre $q - q_1 \neq 0 \Rightarrow$ Grad$(r - r_1)$ $\geq$Grad(b) Widerspruch!!
   Also $q = q_1$ und $r = r_1$ q.e.d.

2.49 Beispiel

$a := x^6 - x - 1, b = x^2 - x + 1 \in \mathbb{Q}[x]$
Suche q (Quotient) , r (Rest)

0	0	0	0	1	-1	1	$1x^4b$
0	0	0	1	-1	1	0	$1x^3b$
0	0	0	0	0	0	0	$0x^2b$
0	-1	1	-1	0	0	0	$-1xb$
-1	1	-1	0	0	0	0	$-1b$
-1	0	0	0	0	0	0	0
1	x	x^2	x^3	x^4	x^5	x^6	

$a = (-1 - x + x^3 + x^4)b + r$
$(r = -x)$

2.50 Folgerung

Sei $0 \neq p \in K[x]$. Dann bilden die Vielfachen (ap mit $a \in K[x]$) von p einen Teilraum $pK[x] \leq K[x]$ von $K[x]$ und der Faktorraum $K[x]/_{pK[x]}$ hat $K[x]_{Grad<n}(n := Grad(p))$ als Vertretersystem. D.h. $K[x] = K[x]_{Grad<n} \oplus pK[x]$. (q oben =p)

2.51 Bemerkung

p etc. wie oben $\Rightarrow$ Die Multiplikation mit x (auf K[x]) induziert eine lineare Abbildung von $K[x]/_{pK[x]}$ in sich mit :

$x^i + pK[x] \to x^{i+1} + pk[x]$ für $i = 0, 1, ..., n-1$
und $x^{n-1} + pK[x] \longmapsto x^n + pK[x] = -a_0 - a_1x - ... - a_{n-1}x^{n-1} + pK[x]$
wo $p = a_0 + a_1x + ... + a_{n-1}x^{n-1} + x^n$ ist.
$-(a_0 + a_1x + ... + a_{n-1}x^{n-1}) \equiv x^n \bmod (pK[x])$

Beweis : Multipliziere mit x auf K[x] linear
Zeige : $\rightsquigarrow$ wohldefinierte (Vertreterunabhängige) Abbildung von $K[x]/p(x)$ in sich
$r + pK[x] = s + pK[x]$ $(r, s \in K[x])$

Behauptung : $xr + pK[x] = xs + pK[x]$
Beweis : $r - s \in pK[x]$,d.h.
$r \cdot s = p \cdot a$ für ein $a \in K[x] \Rightarrow$
$xr - xs = p \cdot ax \in pK[x] \Rightarrow$
$xr + pK[x] = xs + pK[x]$ qed.

Beachte : Die Schreibweise für $a \in K[[x]]$ als $\sum_{i=0}^{\infty} a_ix^i$ ist formal. Im algebraischen Sinne liegt hier keine Summe vor, da Summen nur für endlich viele Summanden definiert sind.

$(1-x)^{-1} = 1 + x + x^2 + x^3 + ..$ (*Geometrische Reihe*)
$(1 - x - x^2)^{-1} = a_0 + a_1x + a_2x^2 + ...$
$a_0 = 1, a_1 = 1, a_{i+2} = a_i + a_{i+1}$ (*Fibonacci*) Vergleich von $\mathbb{Z}$ und $K[x]$:

	$\mathbb{Z}$	$K[x]$
1)	$\lvert ab\rvert = \lvert a\rvert \cdot \lvert b\rvert$	Grad(a,b)=Grad(a)+Grad(b)
2)	Euklidischer Algorithmus wegen Division mit Rest	Euklidischer Algorithmus wegen Division mit Rest
3)	Restklassenkörper : $F_p = \mathbb{Z}/_{p\mathbb{Z}}$, p Primzahl	Restklassenkörper $K[x]/_{pK[x]}$, $p \in K[x]$ irreduzibel
4)	$\mathbb{Q}$	?Quotientenkörper

2.52 Definition

Sei K ein Körper. Der nach 2.25 existierende Quotientenkörper von $K[x]$ $(a, b \in K[x], a, b \neq 0 \Rightarrow ab \neq 0$ Beweis : Grad) wird mit K(X) bezeichnet und heißt der Körper der *rationalen Funktionen* über K (vgl $\mathbb{Z} \to \mathbb{Q}$)
Klar :
Jede rationale Funktion kann geschrieben werden als $\frac{a}{b}$ mit $a, b \in K[x], b \neq 0, ggT(a, b) = \underline{1}$ (Eukl. Algorithmus). Verlangt man noch, daßder höchste Koeffizient von b eins ist, so hat man eine *Normalform* .

2.53 Satz

Ist $p \in K[x]$ *irreduzibel* , d.h. $n := Grad(p) > 0$ und p hat keine Teiler in K[x] vom Grad g mit $0 < g < n$

1. Formulierung :
   Sei Äquivalenzrelation $\sim_p$ auf $K[x]$ definiert durch $a \sim_p b :\Leftrightarrow p|a-b$. Auf den Klassen von $\sim_p$ definieren wir eine Vertreterweise Addition und Multiplikation. Mit dieser Verknüpfung ist $K[x]/_{\sim_p}$ ein Körper, der Restklassenkörper $K[x]/_{pK[x]}$. Wegen der Division mit Rest ist $K[x]_{Grad<n}$ ein Vertretersystem der Klassen von $K[x]/_{pK[x]}$
2. Formulierung :
   $K[x]/_{pK[x]}$ (Ist schon ein Vektorraum) ist mit der Vertreterweisen Multiplikation ein Körper.

2.54 Beispiel

1. (Neue Konstruktion von $\mathbb{C}$)
   In $\mathbb{R}[x]$ ist das Polynom $p = x^2 + 1$ irreduzibel. Bezeichne die Restklasse von x mit $\bar{x}$ $(= x + p\mathbb{R}[x])$
   $\Rightarrow \bar{x}^2 + 1 = 0$ in $\mathbb{R}[x]_{/p\mathbb{R}[x]}$
   $\bar{x}^2 = -1$
   Elemente von $\mathbb{R}[x]_{/p\mathbb{R}[x]}$ gegeben durch :
   $a + b\bar{x}, a, b \in \mathbb{R}$
   $(a + b\bar{x}) \cdot (c + d\bar{x}) = (ac - bd) + (ad + bc)\bar{x}$ $(\bar{x} = i)$
2. (Körper von 4 Elementen)
   In $F_2[x]$ ist $p = x^2 + x + 1$ irreduzibel..
   Damit ist $F_2[x]/_{pF_2[x]}$ ein Körper mit Elementen
   $0, 1, \bar{x} = x + pF_2, \bar{x} + 1$

3. $(\mathbb{Q}(\sqrt[3]{2}))$ $x^3 - 2 \in \mathbb{Q}[x]$ ist irreduzibel
   Sonst hätten wir einen Teiler vom Grad 1 :
   $x - a|x^3 - 2$ $(a \in \mathbb{Q}$, d.h. $a^3 = 2$
   $\bar{x} := x + (x^3 - 2) \in \mathbb{Q}[x]$ $a = \frac{\pm\pi_{p_i}}{\pi_{q_i}}$ $a^3 = 2$ was ein Widerspruch ist.

2.55 Beispiel

Sei K ein Körper

1. Für jedes Körperelement $a \in K$ ist durch $x^i \longmapsto a^i$ eine lineare Abbildung $K[x] \to K$: $p \longmapsto p(a)$ definiert.(*Einsetzungsisomorphismus*). Man nennt a eine *Wurzel* von p, falls beim Einsetzen $p(a) = 0$. Ein Polynom vom Grad n hat höchstens n Nullstellen.
2. Eine Abbildung $f \in K^K$ heißt *Polynomfunktion*, falls ein $p \in K[x]$ mit $f(a) = p(a) \forall a \in K$. In diesem Fall heißt $f =: f_p$ die von p *induzierte Polynomfunktion*. Es ist $K[x] \to K^K$: $p \longmapsto f_p$ eine K-Lineare Abbildung. Das Bild bezeichnen wir mit $PolFu(K)$. Die Abbildung ist genau dann surjektiv, wenn $|K| < \infty$. Die Abbildung ist genau dann injektiv, wenn $|K| > \infty$.

Beweis :

1. Linearität : Klar
   Es gilt : $a \in K$ Wurzel von $p \Leftrightarrow (x - a)|p$
   Sei $q \in K[x]$ $ggT(x - a, q) = 1 \Leftrightarrow q(a) \neq 0$
   $q(a)$ ist der Rest bei Division von q durch x-a. Also angenommen p hat l verschiedene Nullstellen :
   $a_1, .., a_l \Rightarrow (x - a_1)(x - a_2)...(x - a_l)|p$, also $l \leq n$
   $ggT(x - a_i, x - a_j) = 1$ für $i \neq j$
2. Übung : Beachte : Nullstellen von f_p = Wurzel von p (Lagrangeinterpolation)

2.56 Definition

Ein Körper K heißt algebraisch abgeschlossen, falls jedes nicht konstante Polynom $(p \in K[x] - K \Rightarrow$ ex. $a \in K$ mit $p(a) = 0$ also Polinom vom Grad 0) eine Nullstelle in K hat, d.h. jedes Polynom zerfällt in ein Produkt von Linearfaktoren.(Teiler vom Grad 1)

2.57 Satz

(Gauß, sogenannter Fundamentalsatz der Algebra)
$\mathbb{C}$ ist algebraisch abgeschlossen.

3 Dimension und Basis eines Vektorraums

1.) Erzeugen von Teilräumen

3.1 Satz

Sei $T \neq 0$ eine Menge von Teilräumen
$\mathcal{W}$ von $\mathcal{V}$(K-VR) $\Rightarrow \bigcap_{\mathcal{W}\in\mathcal{T}} \mathcal{W} \leq \mathcal{V}$
Beweis :
$\bigcap_{\mathcal{W}\in\mathcal{T}} \mathcal{W} = \emptyset$, denn $0 \in \mathcal{W}\forall\mathcal{W} \in \mathcal{T}$ also $0 \in \bigcap_{\mathcal{W}\in\mathcal{T}} \mathcal{W}$
Seien $X, Y \in \bigcap_{\mathcal{W}} \mathcal{W}, a, b \in K$
$\Rightarrow X, Y \in \mathcal{W}\forall\mathcal{W} \in \mathcal{T}, \dashv, \lfloor \in \mathcal{K}$
$\overset{\Rightarrow}{_{\mathcal{W}\in\mathcal{V}}}$ $aX + bY \in \mathcal{W}\forall\mathcal{W} \in \mathcal{T}$
$\Rightarrow aX + bY \in \bigcap_{\mathcal{W}\in\mathcal{T}} \mathcal{W}$

3.2 Beispiel

Gegeben : Ein lineares homogenes Gleichungssystem
$\Rightarrow$ Lösungsraum = Schnitt der Lösungsräume der einzelnen Gleichungen.

3.3 Definition

Sei $\mathcal{V}$ ein K-VR und $M \subseteq \mathcal{V}$ Vektorraumerzeugnis)

1. Das *Erzeugnis* (Vektorraumerzeugnis) ¡M¿ von M ist der kleinste Teilraum , der M entält. Genauer : $< M >:= \bigcap_{\substack{\mathcal{W}\in\mathcal{V} \\ M\subseteq\mathcal{W}}} \mathcal{W}$
2. Eine *Linearkombination* von Elementen von M ist ein Vektor $V \in \mathcal{V}$, für den ein $n \in \mathbb{N}$ existiert, $a_1, ..., a_n$, kurz $a \in K^n$ und $x_1, ..., x_n \in M$, kurz $x \in M^n$, existieren mit $V = a_1x_1 + a_2, x_2, ..., a_n, x_n$. Ist $M = \emptyset$, so ist der Nullvektor die einzige Linearkombination von Vektoren aus M. Menge aller LK von Elementen aus M : $LK(M)$.

3.4 Satz

Sei $\mathcal{V}$ ein K-VR, $M \subseteq \mathcal{V}$
$\Rightarrow < M >= LK(M)$

Beweis :
Behauptung 1 : $LK(M) \leq \mathcal{V}$
Beweis : $0 \in LK(M)$ $\surd$, also $LK(M) \neq \emptyset$
Seien $V, W \in LK(M), s, t \in K$
$\Rightarrow$ ex. $m, n \in \mathbb{N}, a \in K^m, b \in K^n, x \in M^m, y \in M^n$
mit
$V = a_1x_1 + ... + a_mx_m$

$W = b_1y_1 + ... + b_ny_n$
$\Rightarrow sV + tW = sa_1y_1 + ... + sa_mx_m + (tb_1)y_n + ... + (tb_n)y_n \in LK(M)$. (Klar : $M \subseteq LK(M)$)
Behauptung 2 : Ist $\mathcal{W} \leq \mathcal{V}$mit $M \subseteq \mathcal{W}$
$\Rightarrow \mathcal{LK}(\mathcal{M}) \subseteq \mathcal{W}$
Beweis : Jeder Teilraum entält alle Linearkombinationen seiner Elemente.

Aus 1 und 2 $\Rightarrow$ Behauptung qed.

3.5 Beispiel

1. Seien $\mathcal{T}_1, \mathcal{T}_2 \leq \mathcal{V}$
   $\mathcal{T}_1 + \mathcal{T}_2 :=< \mathcal{T}_1 \cup \mathcal{T}_2 >$
   (andere Schreibweise : $< \mathcal{T}_1, \mathcal{T}_2 >$
   Zusammenhang mit der direkten Summe :
   $\varphi : \mathcal{T}_1 \oplus_a \mathcal{T}_2 \to \mathcal{V} : (T_1, T_2) \longmapsto T_1 + T_2$ ist eine lineare Abbildung mit $Bild(\varphi) = \mathcal{T}_1 + \mathcal{T}_2$ und $Kern(\varphi) = \{(T, -T) | T \in \mathcal{T}_1 \cap \mathcal{T}_2\}$
   Insbesondere : $\mathcal{T}_1 + \mathcal{T}_2 = \mathcal{T}_1 \oplus_i \mathcal{T}_2 \Leftrightarrow \mathcal{T}_1 \cap \mathcal{T}_2 = \{0\}$

3.6 Definition

Ein K-VR $\mathcal{V}$ heißt *endlich erzeugt*, falls eine endliche Teilmenge $M \subseteq \mathcal{V}$ existiert mit $\mathcal{V} =< M >$

3.7 Beispiel

1. $\mathcal{V} = K^{n\times 1}$ ist endlich erzeugt, denn die Spalten der Einheitsmatrix bilden ein Erzeugendensystem.. $< E_1 := I_{-,1} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots, E_n := I_{-,n} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} >$ denn $\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} =$ $a_1E_1 + \ldots + a_nE_n$
2. K[x] ist als K-VR nicht endlich erzeugt, denn für jede endliche Teilmenge $M \subseteq K[x]$ sind die Grade der Polynome in $< M >$ beschränkt durch das Maximum der Grade der Polynome in M.
3. Ist $\mathcal{V}$ ein endlich erzeugter K-VR und $\varphi : \mathcal{V} \to \mathcal{W}$ lineare Abbildung
   $\Rightarrow$ Bild(φ) endlich erzeugter K-VR ($\varphi \Rightarrow \mathcal{W}$ endlich erzeugt)
   Denn : $\mathcal{V} =< x_1, \ldots, x_n >\Rightarrow Bild(\varphi) =< \varphi(x_1), \ldots, \varphi(x_n) >$
4. $\mathcal{V}, \mathcal{W}$ endlich erzeugt $\Rightarrow \mathcal{V} \oplus_a \mathcal{W}$ ist endlich erzeugter K-VR.

3.8 Bemerkung

minimale Erzeugendensysteme?
$< X >= \mathcal{N}, < x - \{x_i\} >\neq \mathcal{V} \forall X_i \in X$

Ist $M \subseteq \mathcal{V}$ ein minimales Erzeugendensystem, so gilt $X \notin< M - \{X\} >$ für alle $X \in M$.

2. Lineare Unabhängigkeit :

Arbeite mit Folgen von Vektoren statt mit Mengen :
(Bislang : $X \subseteq \mathcal{V}, < X >= LK(X)$

Jetzt : $X \in \mathcal{V}^n, < X >=< \{x_1, ..., x_n\} >=< x_1, ..., x_n >)$
Benutze bei Folgen die bisherige Definition für das Bild der Folge.

3.9 Bemerkung

Sei $X = (X_1, ..., X_n) \in \mathcal{V}^n, \mathcal{V}$ K-VR.
Folgende Aussagen sind äquivalent :

1. Aus $a_1X_1 + ... + a_nX_n = 0$ mit $a_i \in K$ FOLGT $a_1 = ... = a_n = 0$
2. Für die linearen Abbildungen
   $\varphi : K^n \to \mathcal{V} : a \longmapsto a_1X_1 + ... + a_nX_n$ dilt : $Kern(\varphi = \{0\}$
3. Für jedes $V \in < X >$ gibt es genau ein $a \in K^n$ mit $V = a_1X_1 + ... + a_nX_n$

3.10 Definition

$X \in \mathcal{V}^n$ heißt *linear unabhängig*, falls eine (und damit alle 3) Aussagen von 3.9 zutreffen. Andernfalls heißt X *linear abhängig*. Eine endliche Teilmenge $\{X_1, ..., X_n\}$ von n Elementen von $\mathcal{V}$ heißt linear linear unabhängig oder linear abhängig, wenn eine Folge $\{X_1, ..., X_n\}$ die entsprechende Eigenschaft hat. Eine unendliche Menge $X \subseteq \mathcal{V}$ heißt linear unabhängig, falls jede endliche Teilmenge von X linear unabhängig ist.

3.11 Beispiel

1. $(E_1, ..., E_n) \in (K^{n\times 1})^n$ (vgl. Beispiel 3.71) ist linear unabhängig
   $(a_1E_1 + ... + a_nE_n = 0$
   $\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \Rightarrow a_1 = \ldots = a_n = 0)$
   (Locker $E_1, ..., E_n$ linear unabhängig Ist $X \subseteq \mathcal{V}^n$ und $\varphi : \mathcal{V} \to \mathcal{W}$ linear.
   $\varphi \circ X = (\varphi(X_1), \ldots, \varphi(X_n)) \in \mathcal{W}^n$ l. u. $\Rightarrow$ X l.u.
   Beweis:
   Sei $a \in X^n$ mit $a_1X_1 + \ldots + a_nX_n = 0$
   $\underset{\varphi(linear)}{\Rightarrow} a_1\varphi(X_1) + \ldots + a_n\varphi(X_n) = 0$
   $\underset{\varphi\circ X(linear)}{\Rightarrow} a_1 = \ldots = a_n = 0$
2. $(sin, cos) \subseteq (\mathbb{R}^{\mathbb{R}})^2$ linear unabhängig.
   Denn $\alpha :< sin, cos >\to \mathbb{R}^2 : f \longmapsto (f(0), f(\frac{\pi}{2}))$ ist linear.
   $\alpha(sin) = (0, 1), \alpha(cos)) = (1, 0)$ sind linear unabhängig (Benutze 2)
3. $(sin \times sin, cos \times cos; K_1$(konstante Abbildung auf 1)$) \in \mathbb{R}^{\mathbb{R}})^3$ linear abhängig denn nach Pythagoras :
   $sin(x)^2 + cos(x)^2 = 1 \forall x \in \mathbb{R}$
   $1sin(x)sin + 1cos(x)cos + (-1)K_1 = 0$-Abbildung

Beachte : erzeugen(Bild(φ)) und linear unabhängig (Kern(φ)) sin dual zueinander.

3.12 Satz

Sei $\mathcal{V}$ ein K-VR und $X = (X_1, ..., X_n, Y) \in \mathcal{V}^n$ Folgende Aussagen sind äquivalent :

1. X ist ein minimales Erzeugendensystem von $\mathcal{V}$

2. X ist maximal linear unabhängig in $\mathcal{V}$, d.h. X ist unabhängig und $(X_1, ..., X_n, Y)$ ist linear abhängig für alle $Y \in \mathcal{V}$
3. X ist ein linear unabhängiges Erzeugendensystem. Ein derartiges X heißt *Basis* von $\mathcal{V}$

Beweis :
"1) $\Rightarrow$ 3)" : Klar : Ausgangspunkt unserer Diskussion linear unabhängig.
"3) $\Rightarrow$ 2)" : DaßX l.u. ist, ist klar (Vorraussetzung) Sei also $Y \leq \mathcal{V}$ Behauptung : $(X_1, ..., X_n, Y)$ linear abhängig Beweis :
Nach 3) : $Y \in LK(X)$, d.h. ex. $a \in K^n$ mit $Y = a_1X_1 + ... + a_nX_n$, d.h. $(A_1, ..., a_n, -1)$ ist eine "lineare Abhängigkeit" von $(X_1, ..., X_n, Y)$ ($\in (Kern(\varphi)$, vgl. 3.9.2) "2) $\Rightarrow$ 1)" : 1. Behauptung : X ist Erzeugendensystem.
Sei $Y \in \mathcal{V} \Rightarrow (X_1, ..., X_n, Y)$ ist linear abhängig, während $(X_1, ..., X_n)$ linear unabhängig ist.
$\Rightarrow$ ex. $a \in K^{n+1}$ mit $a \neq 0$ und $(A_1X_1 + \ldots + a_nX_n + a_{n+1}Y = 0$ und $a_{n+1} \neq 0$ (sonst $(A_1, ..., a_n)$ "lineare Abhängigkeit" von X)
$\Rightarrow Y = \frac{-a_1}{a_{n+1}}X_1 + ... + \frac{-a_n}{a_{n+1}}X_1$,d.h. $Y \in < X >$, d.h. X ist Erzeugendensystem von $\mathcal{V}$.
2.Behauptung : X minimales Erzeugendensystem.
Klar, denn keiner der Vektoren von X ist zum Erzeugen überflüssig. qed.

3.13 Folgerung

$X = (X_1, ..., X_n) \in \mathcal{V}^n$. X ist genau dann Basis von $\mathcal{V}$,falls
$\varphi : K^n \rightarrow \mathcal{V} : a \longmapsto a_1X_1 + ... + a_nX_n$ ein Isomorphismus ist,d.h. :
Bei jedem $V \in \mathcal{V}$ ex. genau ein $a \in K^n$ mit $V = a_1X_1 + ... + a_nX_n$.

3. Der Steinitzsche Austauschsatz

3.14 Hauptsatz (Steinitz)

$\mathcal{V}$ K-VR, $X \in \mathcal{V}^n$ Erzeugendensystem von $\mathcal{V}$, d.h. $\mathcal{V} =< X_1, ..., X_n >$, und $Y = (Y_1, ..., Y_s) \in \mathcal{V}^n$ l.u.. Dann $s \leq n$ und nach geeigneter Umordnung der X_i ist $(Y_1, ..., Y_s, X_{s+1}, ..., X_n)$ ein Erzeugendensystem.
Genauer : ex. $\sigma \in S_n$, so daßfür $X' = X \circ \sigma$ gilt :
$(Y_1, ..., Y_s, X_{s+1}, ..., X_n)$ Erzeugendensystem von $\mathcal{V}$
Beweis : Induktion nach s
Induktionsanfang : Sei s=1. Da $Y_1 \in \mathcal{V}$
$\Rightarrow$ ex. $a \in K^n$ mit $Y_1 = a_1X_1 + ... + a_nX_n$
Y_1 l.u. ($bY_1 = 0 \Rightarrow b = 0$,d.h. $Y_1 \neq 0$)
$\Rightarrow a \neq 0$, d.h. ex. ein $i \in \underline{n}$ mit $a_i \neq 0$
obda : (Umordnen)
$i = 1, a_1 \neq 0$
$X_1 = \frac{1}{a_1}Y_1 - \frac{a_2}{a_1}X_2 - \ldots - \frac{a_n}{a_1}X_n$
also $X_1 \in < Y_1, X_2, \ldots, X_n >$, d.h. $\mathcal{V} =< Y_1, X_2, \ldots, X_n >$
Induktions Annahme : Behauptung gilt für s-1 bzw. für $(Y_1, \ldots, Y_{s-1})$
Also : $s - 1 \leq n$ und $(Y_1, ..., Y_{s-1}, X_s, ..., X_n)$ erzeugt $\mathcal{V}$.
Induktions Schritt :
$Y_s \in \mathcal{V} =< Y_1, ..., Y_{s-1}, X_s, ..., X_n >$
$\Rightarrow a \in K^n$ mit $Y_s = a_1Y_1 + \ldots + a_{s-1}Y_{s-1} + a_sX_s + \ldots + a_nX_n$
Y ist l.u. $\Rightarrow Y_s \neq 0$,also $a \neq 0$
Wäre $a_s = \ldots = a_n = 0$ (also $a_{/\underline{n-s-1}} = 0$) so wäre Y l. a.
Also ex. i mit $s \leq i \leq n$ mit $a_i \neq 0$
$\Rightarrow s \leq n$ Nach Umnummerierung

obda : $i = s$
Wie oben :
$X_s \in < Y_1, ...Y_s, X_{s+1}, ..., X_n >$
$\Rightarrow \mathcal{V} = < Y_1, ...Y_s, X_{s+1}, ..., X_n >$ qed.

3.15 Folgerung

Sei $\mathcal{V}$ ein endlich erzeugter K-VR
$\Rightarrow$ ex. ein eindeutiges $n \in \mathbb{Z}_{\geq 0}$, so daßjede Basis von $\mathcal{V}$ genau n Elemente enthält. Dieses n heißt die *Dimension* vo $\mathcal{V}$ (Notation : $Dim(\mathcal{V}) = n = Dim\mathcal{V}$)

Beweis : $\mathcal{V} = \{0\}\surd$. Sei also $\mathcal{V} \neq \{0\}$
Da $\mathcal{V}$ e.e. ex. ein $s \in \mathbb{N}$ und ein Erzeugendensystem $X \in \mathcal{V}^s$. Durch Weglassen von Vektoren können wir erreichen, daßX l.u. Erzeugendensystem ist. Also obda X l.u.. Sei nun $Y \in \mathcal{V}^n$ l.u. $\underset{Steinitz}{\Rightarrow} n \leq s$. Ist zudem Y ein Erzeugendensystem von $\mathcal{V} \underset{X(l.u.)}{\overset{Steinitz}{\Rightarrow}} s \leq n$
Also $n = s$ qed.

3.16 Beispiel

1. $Dim\{0\} = 0$
2. $DimK^n = n$, denn die Standard Basis $S := \{(1,0,\ldots,0),(0,1,0,\ldots),\ldots,(0,\ldots,0,1)\}$ ist offensichtlich eine Basis von K^n und hat n Elemente
3. M beliebige Menge (z.B. endl.)
   $\Rightarrow Dim(K^M) = |M|$
   (a) Im endlichen Fall ($|M| < \infty$) : Basis
   charakteristische Funktionen der einelementigen Teilmengen $\rightsquigarrow$ Basis
   (b) $M \neq \emptyset$ Setze $K^M = \{0\}$
   (c) $|M| = \infty \Rightarrow$ Die charakteristische Funktionen der einelementigen Teilmengen sind linear unabhängig. (jedoch kein Erzeugendensystem mehr) $\Rightarrow Dim(K^M) = \infty = |M|$

3.17 Folgerung

Sei $\mathcal{V}$ ein e.e. K-VR

1. (Basisergänzungssatz) : Ist $X \in \mathcal{V}^l$ l.u., so kann X zu einer Basis von $\mathcal{V}$ ergänzt werden, d.h. $l \leq Dim\mathcal{V} = n$ und es ex. eine Basis $Y \in \mathcal{V}^n$ mit $Y_i = X_i$ für $i = 1, ..., l$
2. Ist $\mathcal{T} \leq \mathcal{V}$, so gilt $Dim\mathcal{T} \leq Dim\mathcal{V}$ mit Gleichheit $\Leftrightarrow \mathcal{T} = \mathcal{V}$
3. Ist $\mathcal{T} \leq \mathcal{V}$ mit Basis $(X_1, \ldots, X_l)$ und $(X_1, \ldots, X_l, Y_1, \ldots Y_k)$ eine Basis von $\mathcal{V}$
   $\Rightarrow (Y_1 + \mathcal{T}, \ldots, Y_k + \mathcal{T})$ ist eine Basis von $\mathcal{V}_{/\mathcal{T}}$
   $Dim\mathcal{V}_{/\mathcal{T}} = Dim\mathcal{V} - Dim\mathcal{T}$

Beweis :

1. Direkt aus dem Satz von Steinitz
2. Linear unabhängige Vektoren von $\mathcal{T}$ sind auch linear unabhängig als Vektoren von $\mathcal{V}$. Also die maximale Zahl der l.u. Tupel aus $\mathcal{T} = Dim(\mathcal{T})$ Also die maximale Zahl der l.u. Tupel aus $\mathcal{V} = Dim(\mathcal{V}) \Rightarrow X + \mathcal{T} = b_1(X_1 + \mathcal{T}) + \ldots + b_k(X_k + \mathcal{T})$

Zeige noch $(Y_1 + \mathcal{T}, \ldots, Y_s + \mathcal{T})$ l.u.
Sei $a \in K^k$ mit
$a_1(Y_1 + \mathcal{T}) + \ldots + a_k(Y_k + \mathcal{T}) = 0 + \mathcal{T}$ d.h.
$a_1Y_1 + \ldots + a_kY_k \in \mathcal{T} \to$ ex. $b \in K^l$ mit $a_1Y_1 + \ldots + a_kY_k = b_1(X_1 + \mathcal{T}) + \ldots + b_l(X_l + \mathcal{T})$
,d.h. ${}_1Y_1 + \ldots + a_kY_k + (-b_1)X_1 + \ldots + (-b_l)X_l = 0$
$\Rightarrow a_1 = \ldots = a_k = 0$ $(= b_1 = \ldots = b_l = 0$
d.h. $a = 0$, also $(Y_1 + \mathcal{T}, \ldots, Y_k + \mathcal{T})$ l.u. qed.

3.18 Folgerung

$\mathcal{V}$ e.e. K-VR, $\alpha : \mathcal{V} \to \mathcal{W}$.
K-linear $\Rightarrow Dim(Bild(\alpha)) + Dim(Kern(\alpha)) = Bim\mathcal{V}$
(Ergänzung zum Homomorphiesatz)
Beweis : Hom. S, : $Bild(\alpha) \cong \mathcal{V}_{/Kern(\alpha)}$
$Dim(Bild(\alpha)) = Dim(\mathcal{V}_{/Kern(\alpha)}) = Dim(\mathcal{V}) - Dim(Kern(\alpha))$ qed.

3.19 Folgerung

Sei $\mathcal{V}$ K-VR , $\mathcal{T}_1, \mathcal{T}_2 \leq \mathcal{V}$
$\Rightarrow Dim(\mathcal{T}_1 + \mathcal{T}_2) = Dim(\mathcal{T}_1 \cap \mathcal{T}_2) = Dim(\mathcal{T}_1) + Dim(\mathcal{T}_2))$
Beweis :
Offenbar ist :
$\alpha : \mathcal{T}_1 \oplus_a \mathcal{T}_2 \to \mathcal{V} : (T_1, T_2 \longmapsto T_1 + T_2$ linear mit
$Bild(\alpha) = \mathcal{T}_1 + \mathcal{T}_2$ und
$Krn(\alpha) = \{(T, -T) | T \in \mathcal{T}_1 \cap \mathcal{T}_2\} \cong \mathcal{T}_1 \cap \mathcal{T}_2$
$\underset{3.18(Beh)}{\Rightarrow} Dim(\mathcal{T}_1 \oplus_a \mathcal{T}_2) = Dim(\mathcal{T}_1) + Dim(\mathcal{T}_2)) \underset{HomS.}{=}$
$= \underbrace{Dim(Kern(\alpha))}_{Dim(\mathcal{T}_1 \cap \mathcal{T}_2)} + \underbrace{Dim(Bild(\alpha))}_{Dim(\mathcal{T}_1 + \mathcal{T}_2)}$ qed.

3.20 Beispiel

Sei $Dim(\mathcal{V}) = 3$
$G(\mathcal{V}) = G := \{\mathcal{U} | \mathcal{U} \leq \mathcal{V}, Dim\mathcal{U} = 2\}$
$P(\mathcal{V}) = P := \{\mathcal{U} | \mathcal{U} \leq \mathcal{V}, Dim\mathcal{U} = 1\}$
$\Rightarrow \mathcal{U}_1, \mathcal{U}_2 \in G, \mathcal{U}_1 \neq \mathcal{U}_2 \Rightarrow \mathcal{U}_1 \cap \mathcal{U}_2 \in P(\mathcal{V})$
$\mathcal{U}_1, \mathcal{U}_2 \in P, \mathcal{U}_1 \neq \mathcal{U}_2 \Rightarrow \mathcal{U}_1 \cap \mathcal{U}_2 \in G(\mathcal{V})$
Interpretation : projektive Geomitrie

4. Konstruktive Aspekte Zur Erinnerung :
$GL(m, K) := \{g \in K^{m \times m} |$ex ein $h \in K^{m \times m}$ mit $gh = I_m\}$ operiert auf $K^{m \times m}$ durch Linksmultiplikation. Linksmultiplikation mit gleichen Elementen von $GL(m, K) \equiv$ elementare Umformungen

3.21 Definition

Sei $A \in K^{m \times n}$

1. $Z(A) :=< A_{1,-}, \ldots, A_{m,-} >\leq K^{1 \times n}$ heißt der *Zeilenraum* von A und seine Dimension heißt der *Zeilenrang* von A.
2. $S(A) :=< A_{-,1}, \ldots, A_{-,n} >\leq K^{m \times 1}$ heißt der *Spaltenraum* von A und seine Dimension heißt der *Spaltenrang* von A.

3.22 Bemerkung

Sei $A \in K^{m \times n}, g \in GL(m, K)$

1. A und gA haben denselben Zeilenraum und somit denselben Zeilenrang. Insbesondere produziert der Gaußalgorithmus eine Basis des Zeilenraumes.
2. A und gA haben denselben Spaltenrang

Beweis:

1. Klar, denn $Z(gA) \subseteq Z(A)$ und $Z(g^{-1}(gA)) \subseteq Z(A)$
2. $\bar{g} : K^{m \times 1} \to K^{m \times 1}$ Isomorphismus induziert einen Isomorphismus von S(A) auf S(gA) $Dim(S(A)) = Dim(S(gA))$ qed.

Beachte : Bei strikter Stufengestalt ist Zeilen und Spaltenrang sofort ablesbar (und gleich)

3.23 Folgerung

$A \in K^{m \times n} \Rightarrow$ Spaltenrang(A) = Zeilenrang(A)
Sie werden mit Rg(A)=Rang von A bezeichnet.

3.24 Folgerung

$A \in K^{m \times n}, Kern(A)$ = Lösungsraum vom kommutativ linearen Gleichungssystem $Ax = 0$ $(x \in K^{n \times 1})$
Es gilt : Dim(Lösungsraum)=$n - Rg(A)$

Beweis :
Dim(Lösungsraum)=Dim Kern($\bar{A}$)
$= n - Dim(Bild\bar{A})$
$= n - Rg(A)$
Denn Bild($\bar{A}$ =S(A)

3.25 Satz

1. GL(m,K) operiert auf $K^{m \times n}$ durch Linksmultiplikation:
   $GL(m, K) \times K^{m \times n} \to K^{m \times n} : (g, A) \longmapsto gA$
   Der Zeilenraum ist eine trennende Invariante, d.h. $A, B \in K^{m \times n}$ sind genau dann in einer Bahn, wenn Z(A)=Z(B)
2. Jede Bahn enthält genau eine Matrix in strikter Stufengestalt.

Beweis : Z(A)=Z(gA) $\surd$ 3.22
d.h. Zeilenraum ist eine Invariante
Sei $A, B \in K^{m \times n}$ mit Z(A)=Z(B)
$\underset{Gauß}{\Rightarrow}$ ex. $g, h \in GL(m, K)$, so daßgA und hB in strikter Stufenform sind.

Behauptung : gA=hB Beweis : konstruiere gA nur aus Z(A)=Z(B)
Zuerst : (Anzahl der Zeilen bei strikter Stufenform $\neq 0$)= Dim(Z(A))
Stufenindizes : strukturell wie folgt :

Definiere für $1 \leq d \leq n$
$\pi_d : Z(A) \to K^{1\times d} : (x_1, ..., x_n) \longmapsto (x_1, ..., x_d)$ und $\pi_\emptyset = 0$ Abbildung von Z(A)
$\Rightarrow$ d Stufenindex $\Leftrightarrow Dim(Bild(\pi_d)) > Dim(Bild(\pi_{d-1}))$
Sei nun d=d max der größte Stufenindex.
$\sigma_d : Z(A) \to K : (x_1, ..., x_n) \longmapsto x_d$
$\underset{Stufengestalt}{\Rightarrow}$ Z(A)=$Kern(\sigma_d) \oplus Kern(\pi_{d-1})$ mit $Dim(Kern(\pi_{d-1})) = 1$
Die letzte Zeile $\neq 0$ der strikten Stufengestalt von A ist durch $Kern(\pi_{d-1})$ festgelegt. Frühere Zeilen durch $Kern(\sigma_d)$:
Jetzt (formale) vollständige Induktion über Zeilenrang möglich.

3.26 Folgerung

Jeder K-dim Teilraum von $K^{1\times n}$ mit $k > 0$ hat eine eindeutige Standardbasis $(Z_1, ..., Z_h)$, die dadurch gekennzeichnet ist, daß$Z(\frac{Z_1}{Z_k}) \in K^{k\times n}$ mit $Z_{i,-} = Z_1$ in strikter Stufengestalt.

3.27 Satz

(Übertragung auf e.e. K-VR:)
Sei $\mathcal{V}$ ein K-VR

1. Die Gruppe GL(n,K) operiert auf $\mathcal{V}^n$ durch $GL(n,K) \times \mathcal{V}^n \to \mathcal{V}^n : (g, X) \longmapsto X_G^{-1}$ wobei
   $(X_1, ...X_n)h := (Y_1, ..., Y_n)$ mit $X_i \in \mathcal{V}, h \in K^{n\times n}$
   $Y_i = \sum_i k_{ji} x_j$
   (Y_i+ (Linearkombination der Spalten von X gemäßder i-ten Spalte von n))

Index