Mini-Skript
Lineare Algebra I
Prof. Dr. W. Plesken
WS 2000/2001
Autoren:

Claus R. F. Overbeck / David Havenith

Die Nummerierung in diesem Skript entspricht nicht der Nummerierung des Originalskriptes (Rettet des Genitiv!)

Dieses Document wurde mit $\LaTeX$ erstellt.

Inhaltsverzeichnis

Vorwort

Dieses Dokument ist als Wiederholung des Stoffes für LA1 gedacht. Es stellt eine grobe Zusammenfassung der Vorlesungsmitschrift dar. Dabei wurde der Schwerpunkt auf die Definitionen und Sätze gelegt, die unserer Meinung nach die Grundlage der Vorlesung bilden. Das Mini-Skript beinhaltet nicht triviale Grundlagen, Beispiele oder offensichtliche Folgerungen. Es ist als Nachschlagewerk für das Lernen gedacht. Es erhebt keinen Anspruch auf Vollständigkeit und Richtigkeit, und es schränkt auch nicht den Stoff der Vorlesung ein.
Dieses Skript wird Euch am meisten helfen, wenn Ihr es von vorne nach hinten durcharbeitet, denn die hier erklärten Begriffe bauen stark aufeinander auf.

Viel Spass wünschen David und Claus.

Kapitel 1

Einleitung: Mengen und Abbildungen

1.1 Abbildungen

1.1.1 Menge aller Abbildungen

Seien M und N Mengen. M^N bezeichnet die Menge aller Abbildungen $M \longrightarrow N$

$$M^N \ := \ \{f \mid f \ := \ M \longrightarrow N\}$$

Achtung: M^2 bezeichnet das Kartesische Produkt $M \times M$!

1.1.2 Identitätsabbildung

Die Identitätsabbildung bildet jedes $m \in M$ auf sich selbst ab.
i.Z. $Id_s \ : \ S \longrightarrow S \ : \ m \mapsto m$
(Bsp. 1.11)

1.1.3 Einbettung

$T \neq \emptyset, \ T \subseteq S \quad \Longrightarrow \{(s,s) \mid s \in T\} \subseteq T \times S$ ist eine Abbildung $T \longrightarrow S$ und wird *Einbettung* von T in S genannt.

$$\iota = \iota_{T,S} : T \longrightarrow S \ : s \longmapsto t$$

1.1.4 konstante Abbildung

M, N Mengen; $n \in N \Longrightarrow M \times \{n\}$ $(\subseteq M \times N)$ ist eine Abbildung, die mit z_n bezeichnet wird und heisst *konstante Abbildung*

1.1.5 Einschränkung

Sei $f : M \longrightarrow N$ und $\emptyset \neq T \subseteq M$
Dann ist: $f_{/T} : f \cap (T \times N)$ eine Abbildung $T \longrightarrow N$
$f_{/T} : T \longrightarrow N : t \longmapsto f(t)$
$f_{/T}$ heisst die *Einschränkung* von f auf T.

1.1.6 Assoziativität der Komposition

A, B, C, D Mengen
$\alpha : A \longrightarrow B,\ \beta : B \longrightarrow C,\ \gamma : C \longrightarrow D$
Es gilt:

$$(\gamma \circ \beta) \circ \alpha = \gamma \circ (\beta \circ \alpha)$$

1.1.7 Bijektivität

Eine Abbildung $f : M \longrightarrow N$ heisst *bijektiv*, falls

$$g := \{(n,m) \in N \times M \mid (m,n) \in f\}$$

eine Abbildung von $N \longrightarrow M$ ist.
g heisst die zu f *inverse* Abbildung oder *Umkehrabbildung* und wird mit f^{-1} bezeichnet.

1.1.8 Kardinalität

$M \neq \emptyset$ und *endlich*, dann heisst die Anzahl der Elemente von M *Kardinalität* von M. $|M| = n$.

1.1.9 Faser

Sei $f : M \longrightarrow N$
Für $n \in N$ heisst

$$f^{-1}(\{n\}) := \{m \in M \mid f(m) = n\}$$

die *Faser* von f über n oder das volle Urbild von n in M.
Vorsicht: nicht mit der Umkehrabbildung verwechseln!

1.1.10 Injektivität

f heisst *injektiv* oder eineindeutig, falls jede Faser von f aus höchstens einem Element besteht.
d.h.

$$m, n \in M \ und\ m \neq n \Longleftrightarrow f(m) \neq f(n)$$

1.1.11 Surjektivität

f heisst *surjektiv* oder eine Abbildung *auf* N, falls keine Faser von f leer ist, d.h zu jedem $n \in N\ \exists\ m \in M\ mit\ f(m) = n$

1.1.12 Linksinverses, Rechtsinverses

Sei $\alpha : M \longrightarrow N$ eine lineare Abbildung, dann gilt:

1. $\alpha\ injektiv\ \Longrightarrow \exists\ \beta : N \longrightarrow M\ mit\ \beta \circ \alpha = Id_M$
   β heisst *Linksinverses* von α.
2. $\alpha\ surjektiv\ \Longrightarrow \exists\ \gamma : N \longrightarrow M\ mit\ \alpha \circ \gamma = Id_N$
   γ heisst *Rechtsinverses* von α.
3. Das Linksinverse berechnet man mit : $\alpha^{tr} \circ \beta^{tr} = Id_M^{tr}$
   Man berechnet nun mit dem Gaußalgorithmus wie ein Rechtsinverses und nimmt danach $\beta = {\beta^{tr}}^{tr}$
4. Sei M Menge, folgende Aussagen sind äquivalent:
   (a) M ist endlich.
   (b) Jede injektive Abbildung $\eta : M \longrightarrow M$ ist auch surjektiv.
   (c) Jede surjektive Abbildung $\tau : M \longrightarrow M$ ist auch injektiv.

1.2 Lineare Gleichungssystem

1.2.1 Definition Lineares Gleichungssystem

Ein*Lineares Gleichungssystem* mit m Gleichungen und n Unbestimmten $x_1, \ldots, x_n$ ist gegeben durch:

$$\begin{aligned} A_{11}x_1 + A_{12}x_2 + \cdots + A_{1n}x_n &= b_1 \\ A_{21}x_1 + A_{22}x_2 + \cdots + A_{2n}x_n &= b_2 \\ \vdots \qquad\quad \vdots \qquad\quad & \vdots \\ A_{m1}x_1 + A_{m2}x_2 + \cdots + A_{mn}x_n &= b_m \end{aligned}$$

wobei $A = (A_{ij}) \in \mathbb{R}^{\mathrm{m \times n}}$ eine gegebene Matrix und $b = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \in \mathbb{R}^{\mathrm{m \times 1}}$ eine gegebene Spalte ist.
A heisst die Matrix des Gleichungssystems.
$(A, b) \in \mathbb{R}^{\mathrm{m \times (n+1)}}$ heisst die *Erweiterte Matrix* des GLS.

1.2.2 Induzierte lineare Abbildung

Sei $A : \underline{m} \times \underline{n} \longrightarrow \mathbb{R} : (i,j) \longmapsto A_{ij}$ eine reelle $m \times n$ Matrix
Die von A *induzierte lineare Abbildung*
$\overline{A} : \mathbb{R}^{n \times 1} \longrightarrow \mathbb{R}^{m \times 1} : x \longmapsto Ax$ ist definiert durch:

$$\overline{A}\left(\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}\right) = A \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} A_{11}x_1 + \cdots + A_{1n}x_n \\ \vdots \\ A_{m1}x_1 + \cdots + A_{mn}x_n \end{pmatrix}$$

Definition: Ax heisst des *Produkt* der Matrix A mit der Spalte x.

1.2.3 Lineare Abbildung

Seien $s, t \in \mathbb{R}$ *und* $x, y \in \mathbb{R}^{nx1}$ dann ist $\overline{A}$ eine *lineare Abbildung*, wenn gilt:

$$\overline{A}(sx + ty) = s\overline{A}(x) + t\overline{A}(y)$$

1.2.4 Matrixprodukt

Seien $A \in \mathbb{R}^{m \times n}$, $B \in \mathbb{R}^{n \times o}$
Das Matrixprodukt ist definiert als:

$$AB = C \in \mathbb{R}^{m \times o} \ mit \ C_{-,j} = AB_{-,j} \ mit \ j = 1, \ldots, o$$

Bemerkung: $C_{i,j} = A_{i,-}B_{-,j}$ ("Zeile mal Spalte").

1.2.5 Komposition

Die Komposition $\overline{A} \circ \overline{B}$ der linearen Abbildungen ist wieder eine lineare Abbildung. $\overline{A} \circ \overline{B} = \overline{AB}$

1.2.6 Assoziativität der Matrixmultiplikation

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

1.3 Gaußalgorithmus (Fang-Cheng)

Wir haben uns aus Zeitgründen dafür entschieden, dass wir den Gaußalgorithmus nicht komplett beschreiben, da dieser so grundlegend ist, dass wir davon ausgehen, dass ihn jeder beherrscht.

1.3.1 Stufenindex

Der *Stufenindex* $St_i(M)$ einer Matrix M $\in \mathbb{R}^{s \times t}$ ist definiert als:

$$St_i(M) := min\{j \in \underline{t} \mid M_{i,j} \neq o\}$$

Falls $M_{i,-}$ = Nullzeile, dann $St_i(M) := t + i$

$$St(M) := (St_1(M), \ldots, St_s(M)$$

wenn $St_1(M) < St_2(M) < \ldots < St_s(M)$ so ist M in Stufenform.
falls zusätzlich fr jeden Stufenindex $j := St_i(M) \leq t$ gilt:

$$M_{-,j} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \leftarrow \text{i-te Zeile}$$

1.3.2 Transponierte Matrix

Sei $A = (a_{i,j})$ eine Matrix: $A^{tr} = (a_{j,i})$, heisst die *Transponierte* von A. Also werden die Zeilen zu Spalten. "A wird an der Diagonale von linksoben nach rechtsunten gespiegelt".
Bemerkung: Sind $A \in \mathbb{R}^{m \times n}$ und $B \in \mathbb{R}^{n \times o}$ dann gilt:

$$(AB)^{tr} = B^{tr} A^{tr}$$

1.4 Partition und Äquivalenzrelation

1.4.1 Relation

1. Eine *Relation* auf einer Menge M ist Teilmenge von $M \times M$.

$$R \ni (m, n) = mRn \quad \text{"m steht in Relation zu n"}$$

2. Eine Relation heisst reflexiv, wenn gilt:

$$mRm \ \ \forall m \in M$$

3. Eine Relation heisst symmetrisch, wenn gilt:

$$mRn \text{ impiziert } nRm$$

4. Eine Relation heisst transitiv, wenn gilt:

$$mRn \text{ und } nRo \text{ impliziert } mRo$$

5. Gilt für eine Relation 2. - 4. so heisst sie Äquivalenzrelation.

1.4.2 Partition

Eine Partition P ist definiert durch:

1. Teilmenge von Pot(M).
2. Die Mengen in der Partition sind disjunkt ($p_1 \cap p_2 = \emptyset \quad \forall p_1, p_2 \in P$)
3. $\emptyset \notin P$
4. $M = \dot{\bigcup\limits_{p \in P}} p$

Die Elemente von P heissen auch *Klassen.*
Ist $X \in P$ eine Klasse, so heissen die Elemente von X auch Vertreter der Klasse X.

1.4.3 Vertretermenge, Transversale

Eine Teilmenge von M, in der genau ein Vertreter jeder Klasse von P enthalten ist, heisst auch Vertretermenge oder Transversale.
Eine Abbildung $v : P \longrightarrow M$ mit Bild(v) ist eine Transversale, so heisst v Vertreterabbildung oder auch Transversale.

1.4.4 Äquivalenzklassen

1. Sei eine Äquivalenzrelation auf der Menge M. Die Äquivalenzklasse von m_0 ist definiert durch:

   $$[m_0] := [m_0]_\sim := \{m \in M \mid m \sim m_0\}$$

   wenn m_o ein Vertreter einer Klasse der Partition ist.
2. Die Menge der Äquivalenzklassen bezeichnet mit $M_{/\sim}$
3. $m \sim_P n$ heisst, dass m und n in der gleichen Klasse der Partition P liegen, eine Äquivalenzrelation.
4. $M_{/\sim_P} = P$

Bemerkung: Zwei Äquivalenzklassen sind entweder gleich, oder disjunkt!

1.4.5 Hauptsatz 1.50

$$\gamma_f : M \longrightarrow M_{/\sim f} : m \longmapsto f^{-1}(\{f(m)\})$$

Alle m, die auf das gleiche f(m) abbgebildet werden, liegen in der gleichen Faser von f(m). m wird auf die Faser von f(m) abgebildet.

$$\overline{f} : M_{\sim f} \longrightarrow N : f^{-1}(\{f(m)\}) \longmapsto f(m)$$

Die Faser von f(m) wird auf das zugehörige f(m) abbgebildet.

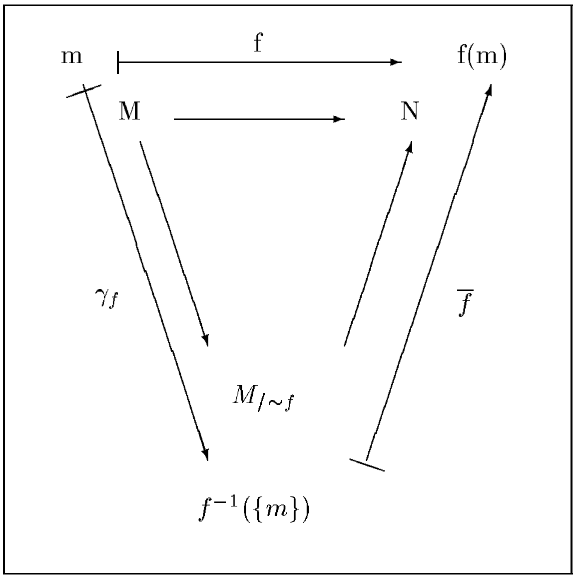

Abbildung 1.

Kapitel 2

Algebraische Stukturen

2.1 Die Gruppenaxiome

2.1.1 innere und äussere Verknüpfung

Sei $A \neq \emptyset$ und M eine Menge; $a, b \in A$.

$$\text{eine innere Verknüpfung ist eine Abbildung: } \alpha : A \times A \longrightarrow A : (a, b) \longmapsto a \circ b$$

$$\text{eine äussere Verknüpfung ist eine Abbildung: } \beta : M \times A \longrightarrow A$$

2.1.2 algebraische Stuktur

Eine *algebraische Stuktur* ist eine Menge A mit einer Menge von Verknüpfungen.

2.1.3 Gruppe, Gruppenaxiome

Eine algebraische Struktur $(G, \cdot)$ heisst Gruppe, falls die folgenden drei Axiome erfüllt sind.

1. Assoziativgesetz $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
2. Einzelelement $\exists\ 1 \in G$ mit $1 \cdot g = g \cdot 1 = g\ \forall\ g \in G$
3. Inverses Element $\exists\ g^{-1} \in G$ mit $g \cdot g^{-1} = g^{-1} \cdot g = 1\ \forall\ g \in G$

2.1.4 abelsche Gruppe

Falls auch noch folgende Bedingug gilt, heist G **abelsche Gruppe**

4. Kommutativgesetz $g \cdot h = h \cdot g\ \forall\ g, h \in G$

Bei kommutativen Gruppen ist manchmal + statt $\cdot$ $(G, +)$, dann ist das Einzelelement 0.

2.1.5 generelle lineare Gruppe Gl(n,$\mathbb{R}$)

Gl(n,$\mathbb{R}$) := Menge der invertierbaren Matrizen in $\mathbb{R}^{n \times n}$

2.1.6 Operation

G eine Gruppe, M eine Menge. G operiert auf M falls eine Abbildung gegeben ist:

$$\omega : G \times M \longrightarrow M : (g, m) \longmapsto gm \text{ mit:}$$

1. $1m = m \;\forall\; m \in M$
2. $g(h, m) = (gh)m \;\forall\; g, h \in G$

2.1.7 Bahn

G operiere auf M und $m \in M$ dann ist die Bahn von m unter G:

$$Gm := \{gm \mid g \in G\} \quad (\subseteq M)$$

Die Bahnen G_m von G auf M bilden eine Partition von M.

$$M_{/\sim_G} = \{G_m \mid m \in M\}$$

2.1.8 Invariante, trennende

Sei G eine Gruppe, die auf der Menge M operiert.
Eine Abbildung f heisst **Invariante der Operation**, wenn gilt:

$$f(gm) = f(m)$$

die Invariante heisst **trennend** falls f(m) = f(m') für $m, m' \in M$ mit Gm = Gm'.
das soll glaube ich heissen, dass m und m' unter der Abbildung f das gleiche Bild haben, falls sie in der gleichen Bahn liegen. Also $\sim_f = \sim_G$

2.2 Körper und Ringe

2.2.1 Körper

Sei K eine *nichtleere* Menge mit zwei Verknpfungen + und $\cdot$
$(K, +, \cdot)$ heisst Körper, falls

1. (K,+) ist eine abelsche Gruppe mit neutralem Element 0.
2. Für $(K, \cdot)$ gilt das Assoziativgesetz.
   Die Existenz des 1-Elements $1 \neq 0$
   das Kommutativgesetz.
   Weiter: Für $K^* = K - \{0\}$ ist $(K^*, \cdot)$ abelsche Gruppe mit neutralem Element 1.
   Insbesondere haben alle Elemente ein multiplikativ Inverses = reziprokes Element $a^{-1} = 1/a$
3. Es gilt das Distributivgesetz $a(b + c) = ab + ac$

Verzichtet man auf den Zusatz, dass $(K^*, \cdot)$ abelsche Gruppe ist, so heisst $(K, +, \cdot)$ ein **Kommutativer Ring mit 1**.

Beispiele

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, sonder nur ein Kommutativer Ring mit 1.
4. $\mathbb{Z}_{/2\mathbb{Z}}$ ist ein Körper.

2.2.2 Körper der komplexen Zahlen

Sei $\mathbb{C} := \{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R}\}$ zusammen mit der Matrzenaddition und -multiplikation der Körper $(\mathbb{C}, +, \cdot)$ der komplexen Zahlen.
Abkürzung: a + bi für $\begin{pmatrix} a & b \\ -\beta & a \end{pmatrix}$
$\mathbb{R}$ ist Teilkörper von $\mathbb{C}$

2.3 Euklidischer Algorithmus

2.3.1 a modulo b

$a, b \in \mathbb{Z} \Longrightarrow \exists q, r \in \mathbb{Z}$ mit $a = qb + r$ und $0 \leq r < |b|$
r heisst auch der kleinste positive Rest von a modulo b

2.3.2 Erster Teil

Gegeben: $a, b \in \mathbb{Z}$ mit $a, b \neq 0$
Gesucht: grösster gemeinsamer Teiler t von a und b. (ggT(a,b)).
Setze: $a_1 = a, a_2 = b$ für n> 2.

$$a_n := a_{n-2} \; mod \; a_{n-1} \text{ falls } a_{n-1} \neq 0$$

Nach endlich vielen Schritten k bekommt man: $a_k = 0$ und $a_{k-1} = ggt(a, b)$
Beispiel: 40, 24, 16, $\underline{8}$, 0

2.3.3 Zweiter Teil

Erklärung anhand eines Beispiels: Finde das Inverse $(25 + 31\mathbb{Z})^{-1}$ *in* $\mathbb{F}_{31}$
Gegeben: $a, b \in \mathbb{Z}$ mit $a, b \neq 0$
Lösung: Finde ggT(a,b) und α, β mit $\alpha a + \beta b = t$
$31 = \underline{1} \cdot 25 + 6$
$25 = \underline{4} \cdot 6 + \mathbf{1}$ 1 ist ggT(31,25) = t
$6 = \underline{6} \cdot 1 + 0$
nun werden die unterstrichenen Zahlen in folgendes System eingesetzt:

$$\begin{pmatrix} 0 & 1 \\ 1 & -\underline{6} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -\underline{4} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -\underline{1} \end{pmatrix} = \begin{pmatrix} -4 & 5 \\ egal & egal \end{pmatrix} \text{ -4 und 5 sind } \alpha \text{ und } \beta$$

$$\alpha a + \beta b = t$$

$$-4 \cdot 31 + 5 \cdot 25 = 1 \quad | \; mod \; 31 \text{ (-4 } \cdot \text{ 31 liegt in der 0-Restklasse)}$$

$$(5 + 31\mathbb{Z}) \cdot (25 + 31\mathbb{Z}) = 1 + 31\mathbb{Z}$$

Also ist $5 + 31\mathbb{Z}$ das multiplikativ Inverse zu $25 + 31\mathbb{Z}$

2.3.4 Quotientenkörper

Sei R ein Kommutativer Ring mit 1, in dem gilt: ab = 0 ⇒ a = 0 oder b = 0.
Dann gibt es einen Quotientenkörper K von R mit

$$K = \{a/b \mid a, b \in R, b \neq 0\}$$

2.4 Vektorräume

Leider habe ich noch nicht herausgefunden, wie die Altdeutschen Buchstaben erstellt werden. Bis mir jemand mitteilt, wie das geht werden die Vektorräume mit *kursiven Buchstaben* bezeichnet.

2.4.1 Definition K-Vektorraum

Sei K Körper, Eine abelsche Gruppe (V,+) zusammen mit einer äusseren Verknüpfung

$$K \times V \longrightarrow V : (a, X) \longmapsto aX$$

heisst Vektorraum über K oder K-Vektorraum falls gilt:

1. Distributivgesetz (links- und rechtsseitig)
2. Assoziativgesetz
3. Existenz des 1 Elementes.

Die Elemente von V heissen Vektoren.

2.4.2 Teilräume

Sei V ein Vektorraum. T heisst Teilvektorraum, falls gilt:

1. $T \neq \emptyset$
2. $X, Y \in T$ *und* $a, b \in K \Longrightarrow aX + bY \in T$

2.4.3 äussere direkte Summe

komponentenweise Addition

$$V \oplus_a W = \{(V, W) \mid V \in V, W \in V\}$$

basierend auf dem Karthesischen Produkt.

2.4.4 innere direkte Summe

V K-Vektorraum, $T_1, T_2 \leq V$

$$V := T_1 \oplus_i T_2 := \{T_1 + T_2 \mid T_1 \in T_1, T_2 \in T_2\}$$

nennt man die (innere) direkte Summe.

2.4.5 komponentenweise Multiplikation

komponentenweise Multiplikation $a \in K$

$$a \cdot V = \{aV \mid V \in V\}$$

2.4.6 K-Homomorphismus, Isomorphismus etc.

Seien V und W K-Vektorräume. Ist $\varphi : V \longrightarrow W$ eine lineare Abbildung, so heisst sie ein **K-Homomorphismus**. Ist φ auch noch bijektiv, so heisst φ **Isomorphismus**.
Ist $V = W$, so heisst φ auch **Endomorphismus**.
Bijektive Endomorphismen heissen **Automorphismen**.

2.4.7 Kern und Bild

Sei $\varphi : V \longrightarrow W$ eine lineare Abbildung (Homomorphismus).

1. $Kern(\varphi) := \varphi^{-1}(\{0\}) \leq V$ heisst der **Kern** von φ
   Das heisst: alle Elemente von V , die durch φ auf das 0-Element von W abgebildet werden.

2. $Bild(\varphi) \leq W$

2.4.8 zugehöriges homogenes Gleichungssystem

Sei A eine Matrix $A \in K^{m \times n}$ und b eine Spalte $b \in K^{m \times 1}$
Dann ist ein lineares Gleichungssystem gegeben durch: Ax = b $(x \longmapsto Ax)$
Das Gleichungssystem ist **lösbar**, wenn $b \in Bild(\overline{A})$ dann gilt:

1. Die Lösungsmenge des zugehörigen homogenen Gleichungssystems, also Ax = 0 ist nie leer, sondern $Kern(\overline{A})$

2. Mir ist noch nicht so richtig klar geworden, was der zweite Teil von Satz 2.37 aussagt.

2.4.9 vertägliche, lineare Äquivalenzrelation

Sei V ein K-Vektorraum und $X, X', Y, Y' \in V$
Eine Äquivalenzrelatin $\sim$ auf V heisst verträglich oder linear, falls gilt:

$$X \sim Y \text{ und } X' \sim Y' \Longrightarrow aX + bX' \sim aY + bY' \; \forall \quad a, b \in K$$

2.4.10 Kongruenzklasse

Sei $\sim_U$ eine Kongruenz, auf V , mit $V_1 \sim_U V_2 \Leftrightarrow V_1 - V_2 \in U$dann gilt:

1. (Kongruenzklasse) $[0] =: U \leq V$

2. $\sim = \sim_U$

3. Die Kongruenzklasse $[X]$ von $X \in V$ ist gegeben durch:

$$[X] := X + U := \{X + U \mid U \in V\}$$

   also der Bahn von X unter der Operation von U auf V durch Addition.

2.4.11 Restklassen, Quotientenraum, natürlicher Epimorphismus

Die Menge $V_{/\sim}$ der Kongruenzklassen wir mit $V_{/U}$ bezeichnet. (V modulo U).
Die Elemente von $V_{/U}$ heissen auch Restklassen nach V und $V_{/U}$ heisst auch Faktorraum, Quotientenraum oder Restklassenraum von V nach U .

1. $V_{/U}$ wird zusammen mit
   der wohldefinierten Addition (X + U) + (Y + U) := (X + Y) + U
   und der wohldefinierten Multiplikation a(X + U) := aX +U
   zu einem K-Vektorraum.

2. Die Abbildung $\gamma : V \longrightarrow V_{/U} : X \longmapsto X + U$ ist eine lineare Abbildung genannt der natürliche Epimorphismus von V auf $V_{/U}$.
   Es gilt: $Kern(\gamma) = U$.

2.4.12 Homomorphiesatz

Sei $f : V \longrightarrow W$ eine lineare Abbildung.
Sei $\gamma : V \longrightarrow W_{Kern(f)}$ der natürliche Epimorphismus.
Sei $\overline{f} : V_{/Kern(f)} \longrightarrow W : X + Kern(f) \longmapsto f(x)$ ein Monomorphismus.
Das heisst: Wir haben ein kommutatives Diagramm:

$$\begin{tikzcd} V \arrow[rr, "f"] \arrow[dr, "\gamma_f"'] & & W \\ & V_{/Kern(f)} \arrow[ur, "\overline{f}"'] & \end{tikzcd}$$

Abbildung 2.

2.5 Polynomringe

2.5.1 Potenzreihenring

Auf dem K-Vektorraum $K^{\mathbb{Z}\geq 0}$ definieren wir eine Multiplikation:

$$(a_0, a_1, a_2, \ldots)(b_0, b_1, b_2, \ldots) := (c_0, c_1, c_2, \ldots)$$

mit

$$c_n := a_0 b_n + a_1 b_{n-1} + \ldots + a_n b_0$$

$(K^{\mathbb{Z}\geq 0}, +, \cdot)$ zusammen mit der K-Vektorraumstruktur von $K^{\mathbb{Z}\geq 0}$ wird mit $K[[x]]$ bezeichnet, dem Potenzreihenring über K in x, genauer dem Ring der formalen Potenzreihen über K.
Statt $(a_0, a_1, \ldots)$ schreibt man auch $\sum\limits_{i=0}^{\infty} a_i x^i$

2.5.2 Polynom, Polynomring

Eine Potenzreihe heisst Polynom, falls ein $n \in \mathbb{N}$ existiert mit $a_i = 0 \ \forall i > n$
Für $a \neq 0$ heisst das kleinste derartige n der Grad des Polynoms.
Die Menge aller Polynome zusammen mit der K-Vektorraumstruktur und der von $K[[x]]$ ererbten Multiplikation heisst der Polynomring $K[x]$ von K(in x).

2.5.3 Quotientenkörper

Der Quotientenkörper von $K[x]$ wird mit K(x) bezeichnet und heisst der Körper der rationalen Funktionen.

2.5.4 Übertragung von $\mathbb{Z}$

$\|ab\| = \|a\| \cdot \|b\|$	Grad(ab) = Grad(a) + Grad(b)
Euklidischer Algorithmus	Euklidischer Algorithmus
Restklassenkörper $\mathbb{F}_p = \mathbb{Z}_{/p\mathbb{Z}}$ p Primzahl	Restklassenkörper $K[x]_{/pK[x]}$ $p \in K[x] irreduzibel$
$\mathbb{Q}$	Quotientenkörper

2.5.5 irreduzibel

$p \in K[x]$ heisst irreduzibel, wenn es keinen Teiler in K[x] gibt mit $0 < Grad_{Teiler} < Grad_p$

2.5.6 Polynomfunktion

Eine Abbildung $f \in K^K$ heisst Polynomfunktion, falls $\exists p \in K[x]$ mit f(a) = p(a) (Einsetzungshomomorphismus) $\forall\ a \in K$.
In diesem Falle heisst f die von p induzierte Polynomfunktion. Die Abbildung des Polynom auf seine Polynomfunktion ist linear. Das Bild (also die Menge der Polynomfunktionen) bezeichnen wir mit Pol-Fu(K).
Die Abbildung ist dann surjektiv, wenn $|K| < \infty$.
Die Abbildung ist dann injektiv, wenn $|K| = \infty$.

2.5.7 algebraisch abgeschlossen

Ein Körper heisst algebraisch abgeschlossen, falls jedes nicht konstante Polynom (Polynome vom Grad 0) eine Nullstelle in K hat, das heisst jedes Polynom zerfällt in ein Produkt von Linearfaktoren (Teiler vom Grad 1).

2.5.8 sogenannter Gaußscher Fundamentalsatz der Algebra

$\mathbb{C}$ ist algebraisch abgeschlossen.

Kapitel 3

Dimension und Basis eines Vektorraumes

3.1 Erzeugen von Teilräumen

3.1.1 Erzeugnis, Vektorraumerzeugnis

Sei V K-Vektorraum und $M \subset V$ von Vektoren.
Das Erzeugnis $< M >$ von M ist der kleinste Teilraum von V, der M enthält.
Genauer: ist $U \leq V$ und $M \subset U$ dann ist $< M >$ der Schnitt aller U also:

$$\bigcap_{\substack{U \leq V \\ M \subseteq U}} U$$

3.1.2 Herstellene des Erzeugnis durch Linear Kombination

Das Erzeugnis von M ist gleich der Menge aller Linearkombinationen von M.

$$< M >= LK(M)$$

3.1.3 Vereinigung und Summe von Vektorräumen

$$T_1 + T_2 =< T_1 \cup T_2 >$$

3.1.4 endlich erzeugt

Ist $V =< M >= LK(M)$ und M ist eine *endliche* Teilmenge von V so heisst V endlich erzeugt.

3.1.5 minimales Erzeugendensystem

Ist $M \subseteq V$ ein minimales Erzeugendensystem, so gilt:
$X \notin < M - \{X\} >$ für alle $X \in M$
das heisst: Die Vektoren X in M sind linear Unabhängig.

3.2 Lineare Unabhängigkeit

3.2.1 Äquivalente Aussagen

Sei $X = (x_1, \ldots, x_n) \in V^n$ und V sei K-Vektorraum.

1. Aus $a_1x_1 + \ldots + a_nx_n = 0$ *mit* $a \in K$ folgt:
   $a_1 = a_2 = \cdots = a_n = 0$

2. $\varphi : K^n \longrightarrow V : a \longmapsto a_1x_1 + \ldots + a_nx_n$ sei eine lineare Abbildung.
   Es gilt: $Kern(\varphi) = \{0\}$

3. Für jedes $V \in < X >$ gibt es genau ein $a \in K^n$ mit

$$V = a_1x_1 + \ldots + a_nx_n$$

   Das heisst: Es gibt nur genau eine Linearkombination der Vektoren von X um jedes V im Erzeugnis von X zu konstruieren.

X heisst linear unabhängig, falls eine der drei Aussagen (und damit alle drei) zutrifft.
Anderenfalls heit X linear abbhängig.
Eine unendliche Menge $X \subseteq V$ heisst linear unabhängig, falls jede endliche Teilmenge von X linear unabhängig ist.

3.2.2 Basis

Sei V ein K-Vektorraum und $X \in V^n$ Folgende Aussagen sind äquivalent:

1. X ist ein minimales Erzeugendensystem von V

2. X ist maximal linear unabhängig in V
   das heisst: X wird durch hinzufügen eines beliebigen Vektors Y linear abbhängig.

3. X ist ein linear unabhängiges Erzeugendensystem.

Ein derartiges X heisst Basis von V

3.3 Steinitzscher Austauschsatz

3.3.1 Hauptsatz

Sei V ein K-Vektorraum und
$X \in V^n$ ein Erzeugendensystem von V und
$Y \in V^s$ linear unabhängig.
$s \leq n$

Nach **geeigneter Umordnung** der x_i ist $(Y_1, \ldots, Y_s, X_{s+1}, \ldots, X_n)$

ein Erzeugendensystem von V. Das heisst X_1 bis X_s wurden durch Y_1 bis Y_s ausgetauscht.
Also: Bildet man X_Y mit geeigneten Vektoren aus X, so ist $< Y >=< X_Y >$
Dieses X_Y sind genau die Vektoren X_1 bis X_s von oben.

3.3.2 Dimension

Sei V ein endlich erzeugter K-Vektorraum.

$\Longrightarrow$ jede Basis von V hat genau n Elemente.

Dieses $n \in \mathbb{Z}_{\geq 0}$ heisst **Dimension** von V.

3.3.3 Basisergänzungssatz

Sei $X \in V^l$ linear unabhängig. Ist l kleiner als die Dimension von V , so kann X zu einer Basis von V ergänzt werden. Also $\exists$ eine Basis Y von V mit $Y_i = X_i, \quad i = 1 \dots l$

3.3.4 Dimension von Teilräumen

1. Sei $T \leq V \implies Dim(T) \leq Dim(V)$.
   Ist die Dimension gleich, so sind die Vektorräume gleich.

2. Sei $T \leq V$, dann ist laut Basisergänzungssatz die Basis von $V = (T_1, \dots, T_l, Y_1, \dots Y_k)$
   $\implies (Y_1 + T, \dots, Y_k + T)$ ist eine Basis von $V_{/T}$. (Dies wird einem nach genauem Hinsehen klarer, denn die Basis Vektoren von T sind ja schon in den $+T$ enthalten (denke ich mal?))
   $\implies Dim\, V_{/T} = Dim\, V - Dim\, T$

3.3.5 Ergänzung zum Homomorphiesatz

Sei V ein endlich erzeugter K-Vektorraum und $\alpha : V \longrightarrow W$ eine **K-lineare** Abbildung
$\implies Dim(Bild(\alpha)) + Dim(Kern(\alpha)) = Dim(V)$

3.3.6 Dimension von Addition und Schnitt (Graßmannidentität)

Seien $T_1, T_2 \leq V$
$Dim(T_1 + T_2) + Dim(T_1 \cap T_2) = Dim(T_1) + Dim(T_2)$

3.4 Konstruktive Aspekte

3.4.1 Zeilen- und Spaltenraum

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

1. $Z(A) := < A_{1,-}, \dots, A_{m,-} > \; \leq \; K^{1 \times n}$ heisst der Zeilenraum von A. und seine Dimension heisst der Zeilenrang.
   Bemerkung: Der Zeilenraum ist das Erzeugnis der Zeilen von A und ist Teilraum des Raumes aller $K^{1 \times n}$ Zeilen.

2. $S(A) := < A_{-,1}, \dots, A_{-,n} > \; \leq \; K^{m \times 1}$ heisst der Spaltenraum von A. und seine Dimension heisst der Spaltenrang.
   Bemerkung: Der Spaltenraum ist das Erzeugnis der Spalten von A und ist Teilraum des Raumes aller $K^{m \times 1}$ Spalten.

3.4.2 Bemerkung zu der Menge der invertierbaren Matrizen

Sei $A \in K^{m \times n}$ eine Matrix. und $g \in Gl(m, K)$ eine invertierbare Matrix.

1. A und gA haben denselben Zeilenraum und somit denselben Zeilenrang. Insbesondere produziert der Gaußalgorithmus (Fang Cheng) eine Basis des Zeilenraumes. Bemerkung: Wird klar, wenn man lange genug hinsieht : $\underset{\smile}{\odot\iota\odot}$

2. A und gA haben den gleichen Spaltenrang.

3.4.3 Zassenhausalgorithmus

Seien $X \in T_1^k$ und $Y \in T_2^l$ Erzeugendensysteme für $T_1, T_2 \leq K^{1\times n}$ Gesucht: Basis für $T_1 + T_2$ und $T_1 \cap T_2$.
Wir schreiben uns eine Matrix G mit:

$$G = \left(\begin{array}{c|c} X_1 & X_1 \\ \vdots & \vdots \\ X_k & X_k \\ \hline Y_1 & 0 \\ \vdots & \vdots \\ Y_l & 0 \end{array}\right)$$

Nun wird der Fang Cheng Algorithmus (auch manchmal Gaußalgorithmus genannt) auf diese Matrix angewandt, mit folgendem Resultat:

$$S = \left(\begin{array}{c|c} B_1 & egal \\ \vdots & \vdots \\ B_D & egal \\ \hline 0 & C_1 \\ \vdots & \vdots \\ 0 & C_d \\ \hline 0 & 0 \\ \vdots & \vdots \end{array}\right)$$

mit:
$(B_1, \ldots, B_D)$ Basis von $T_1 + T_2$
$(C_1, \ldots, C_d)$ Basis von $T_1 \cap T_2$