Skript für

Mathematik 1

Erstellt von : Ostermeier Reinhard
Dieses Skript hat keinen Anspruch auf Vollständigkeit!
Gedruckt am 24. Januar 2003

Inhaltsverzeichnis

1. Mengen

1.1 Definition: (Cantor, 1845 - 1918)

Eine Menge ist eine Zusammenfassung bestimmter wohlunterschiedener Objekte unserer Anschauung oder unseres Denkens - welche die Elemente der Menge genannt werden - zu einem ganzen.

1.2 Schreibweisen:

-	{...}	aufzählen aller Elemente
-	{ x | x hat Eigenschaft }	
-	{} , $\emptyset$	Leere Menge
-	$x \in M$	x ist Element aus M
-	$x \notin M$	x ist nicht Element aus M

1.3 Definition:

A und B seien Mengen:
wenn für jedes $x \in A$ gilt, $x \in B$, so schreibt man $A \subset B$ und sagt A ist Teilmenge von B.
$A \not\subset B$ wenn A nicht Teilmenge von B.

1.4 Definition:

A und B seien Mengen:

1. A = B :⇔ A ❄ B und B ❄ A
2. A ∩ B := { x | x ✐ A und x ✐ B }
3. A ∪ B := { x | x ✐ A oder x ✐ B }
4. A ✈ B := { x | x ✐ A und X ➻ B }
5. A und B heißen disjunkt, wenn gilt A ⚮ B = {}
6. Falls A ⊂ B dann heißt A ✈ B das Komplement von A in B
   Falls klar ist was B ist, so schreibt man auch kurz ❵ := B ✈ A

1.5 Satz:

A und B seien Mengen:

1. $A \cup B = B \cup A$
2. $A \cap B = B \cap A$
3. $(A \cup B) \cup C = A \cup (B \cup C)$
4. $(A \cap B) \cap C = A \cap (B \cap C)$
5. $A \cap \emptyset = \emptyset$
6. $A \cup \emptyset = A$
7. A ✈ $\emptyset$ = A
8. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
9. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

1.6 Definition:

A und B seien Mengen:
$A \times B := \{ x, y \mid x \in A, y \in B \}$
Menge aller geordneten Paare (x, y) mit $x \in A$ und $y \in B$
oder kartesisches Produkt von A und B

1.7 Beispiel:

$A = \{a_1, a_2\}$, $B = \{b_1, b_2, b_3\}$ $\quad A \times B = \{(a_1, b_1), (a_1, b_2), (a_1, b_3), (a_2, b_1), (a_2, b_2), (a_2, b_3)\}$

1.8 Definition:

M ist Menge:
P(M) := Menge aller Teilmengen von M = $\{ A \mid A \subset M \}$ ✡Potenzmenge✠

1.9 Definition: (unendlicher Durchschnitt / Vereinigung)

Sei I Menge (beliebig) ✡Indexmenge✠
Für jedes $i \in I$ sei eine Menge A_i gegeben
Dann: $\bigcup_{i \in I} A_i := \{ x \mid x \in A_i \text{ für mindestens ein } i \in I \}$

∩ A_i := { x | x ∈ A_i □ i ∈ I }

2. Abbildungen

2.1 Definition:

Eine Abbildung f von X nach Y ist eine Vorschrift, die jedem Element von X genau ein Element von Y zuordnet.

Statt f ist Abbildung von X nach Y schreibt man kurz:

$f : X \to Y$

Die Abbildungsvorschrift - welche jedem $x \in X$ genau ein $y \in Y$ zuordnet - schreibt man:

$x \mapsto y =: f(x)$

kurz aber vollständig : $f : X \to Y$

$x \mapsto f(x)$

X heißt Definitionsbereich

Y heißt Wertebereich

2.2 Definition:

X, Y Mengen $f : X \to Y$ Abbildung

$A \subset X$ $B \subset Y$

Dann heißen die Mengen:

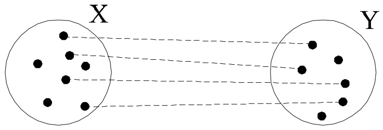
- $f(A) := \{ f(x) \mid x \in A \} \subset Y$ ✡Bild von A unter f✠
- $f^{1}(x) := \{ x \in X \mid f(x) \in B \} \subset X$ ✡Urbild von B✠
- $\Gamma_f := \{ (x, f(x) \mid x \in X \} \subset X \times Y$ ✡Graph von f✠

2.3 Definition:

gegeben: $f : X \to Y$

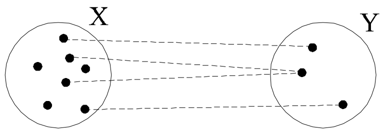
f heißt injektiv, wenn keine zwei Elemente von X auf das selbe Element von Y abgebildet werden.

$x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$

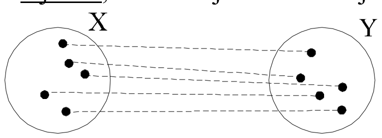


f heißt surjektiv, wenn jedes Element $y \in Y$ ein f(x) ist.

zu jedem $y \in Y$ existiert ein $x \in X$ mit $y = f(x)$



f heißt bijektiv, wenn f injektiv und surjektiv ist.



2.4 Definition:

$f : X \to Y$ und $g : Y \to Z$ sind Abbildungen

Dann heißt die Abbildung

$g \circ f : X \to Z$ Hintereinanderausführung von g nach f

$x \mapsto g(f(x))$

2.5 Definition:

$f^{1} : \; Y \to X$

$y \mapsto x_y$

heißt Umkehrabbildung oder Inverse von f

2.6 Satz:

$f : A \rightarrow B$ sei Abbildung, dann gilt:
f ist injektiv $\Leftrightarrow$ es gibt eine Abbildung $g : B \rightarrow A$ mit $g \circ f = id_A$
f ist surjektiv $\Leftrightarrow$ es gibt eine Abbildung $h : B \rightarrow A$ mit $f \circ h = id_B$
f ist bijektiv $\Leftrightarrow$ g und h wie in a) und b) dann ist $g = h = f^{-1}$

3. Relationen / Äquivalenzrelationen

3.1 Definition:

M und N sind Mengen. Eine Teilmenge $R \subset M \times N$ heißt <u>Relation</u> zwischen den Elementen von M und N.
Anstatt $(x, y) \in R$ schreibt man auch xRy.
Sei M Menge und $R \neq M \times M$ eine Relation zwischen den Elementen von M.
R heißt <u>Äquivalenzrelation</u> auf M, falls folgendes gilt:

(Ä1)	$(a, a) \in R \ \forall a \in M$	(reflexiv)
(Ä2)	$(a, b) \in R \Rightarrow (b, a) \in R$	(symetrisch)
(Ä3)	$(a, b) \in R$ und $(b, c) \in R \Rightarrow a, c) \in R$	(transitiv)

Ist R eine Äquivalenzrelation auf M so schreibt man statt $(a, b) \in R \neq M \times M$ auch
$a \sim_R b$ oder kurz $a \sim b$ falls klar ist, um welche Äquivalenzrelation es sich handelt.
Man sagt a ist <u>äquivalent</u> zu b wenn $a \sim b$.

3.2 Definition:

M Menge, $\sim$ Äquivalenzrelation auf M
$A \subset M$ heißt <u>Äquivalenzklasse</u> von M bezüglich $\sim$
falls gilt:
$A \neq \emptyset$
$a, b \in A \Rightarrow a \sim b$
$a \in A, m \in M, a \sim m \Rightarrow m \in A$

3.3 Bemerkung:

M Menge, $\sim$ Äquivalenzrelation auf M
dann:
Jedes Element $a \in M$ gehört zu einer Äquivalenzklasse
$[a] := M(a) := \{ x \in M \mid x \sim a \}$
A, A' Äquivalenzklassen, dann gilt:
entweder $A = A'$ oder $A \cap A' = \emptyset$

Die Bemerkung besagt: M läßt sich als disjunkte Vereinigung von Äquivalenzklassen darstellen. oder:
$\sim$ ist eine disjunkte Zerlegung von M in Äquivalenzklassen.

4. Mächtigkeit von Mengen / Abzählbarkeit

4.1 Definition:

$<1, n> := \{ x \in N \mid 1 \leq x \leq n \} = \{ 1, 2, \ldots n \}$
eine Menge M heißt <u>endlich</u>, wenn es eine bijektive Abbildung
$f : <1, n> \rightarrow M$ gibt

4.2 Bemerkung:

Wenn es eine bijektive Abbildung $f : <1, n> \rightarrow M$ gibt, so ist n eindeutig bestimmt.
$n =: card(M) =: |M|$

4.3 Definition:

Eine Menge M heißt <u>abzählbar</u>, wenn es eine surjektive Abbildung $f : N \rightarrow M$ gibt.

4.4 Satz:

R ist nicht abzählbar.

5. Vollständige Induktion

Wir werden sehen, daß R eine Anordnung besitzt. Damit auch $N \subset R$.

5.1 Satz 1:

Jede nicht leere Teilmenge M von N hat ein kleinstes Element.

5.2 Satz 2: (Induktionsprinzip)

Sei $M \subset N$ mit folgenden Eigenschaften:
$1 \in M$
wenn k ✐ M $\Rightarrow$ $k+1 \in M$
Dann $M = N$

6. Kombinatorik

6.1 Satz:

M und N endliche Mengen mit n := |M| = |N|
Dann gibt es n*(x-1)*(n-2)* ... 2*1 =: n! verschiedene bijektive Abbildungen
$f : M \rightarrow N$

6.2 Definition:

Sei M = N endliche Mengen, dann nennt man die bijektive Abbildung $M \rightarrow N$ auch <u>Permutation</u>.
Also es gibt |M|! verschiedene Permutationen.

6.3 Definition:

M endliche Menge mit |M| = n
Sei 0 ✂ k ✂ n dann gibt es endlich viele verschiedene Teilmengen aus M mit k Elementen.
Diese Anzahl wird mit $\binom{n}{k}$ bezeichnet.
Also ist $\binom{n}{k}$ anzahl der k-elementigen Teilmengen aus einer Menge mit n Elementen.

6.4 Satz 1:

Es gilt 0 ✂ k ✂ n

$$\binom{n}{k} = \binom{n}{n-k}$$

6.5 Satz 2:

1. $\binom{n}{k} = \frac{n!}{k!(n-k)!}$
2. $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$

6.6 Satz: (Binomischer Lehrsatz)

$x, y \in R \qquad n \in N_0 \qquad$ dann gilt:

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} * x^k * y^{n-k}$$

7. Zahlentheorie

7.1 Definition:

A, $b \in Z$ $\quad b \neq 0$

a heißt durch b teilbar oder „b teilt a“ – geschrieben b \ a, wenn es eine ganze Zahl q gibt, so daß $a = b * q$

Teilbarkeitsregeln:

1.) $c \setminus b$ und $b \setminus a \Rightarrow c \setminus a$
2.) $b_1 \setminus a_1$ und $b_2 \setminus a_2 \Rightarrow b_1 * b_2 \setminus a_1 * a_2$
3.) $b \setminus a_1$ und $b \setminus a_2 \Rightarrow b \setminus (\alpha_1 a_1 + \alpha_2 a_2)$ mit $\alpha_1, \alpha_2 \in Z$
4.) $b \setminus a$ und $a \setminus b \Rightarrow a = b$ oder $a = -b$

7.2 Satz: (Division mit Rest)

Für zwei ganze Zahlen a, b und $b \neq 0$ gibt es eine Darstellung der Form

$$a = b * q + r$$

mit $q, r \in Z$ und 0 ✃ r |b|

q heißt Quotient, r heißt Rest

7.3 Definition:

$a, b \in Z$ und es gelte $d \setminus a$ und $d \setminus b$. So heißt d ein gemeinsamer Teiler von a und b

Wenn gilt: d gemeinsamer Teiler von a und b und für jeden weiteren Teiler c von a und b gilt $c \setminus d$ so heißt d größter gemeinsamer Teiler von a und b.

7.4 Satz:

Wenn es einen ggT gibt, so ist er bis aufs Vorzeichen eindeutig.

denn: d, e seien gemeinsame größte Teiler von a, b

$\Rightarrow e \setminus d$ und $d \setminus e \Rightarrow d = e$ oder $d = -e$

7.5 Hilfssatz 1:

$a, b, q \in Z$ $\quad$ Dann: $d = ggT(a, b) \Leftrightarrow d = ggT(b, a - qb)$

7.6 Hilfssatz 2:

ist $a = bq$, so ist $b = ggT(a, b)$

7.7 Satz: (Euklidscher Algorithmus)

seien $a, b \in Z$ $\quad a \neq 0 \quad b \neq 0$

- dann gibt es genau einen positiven größten gemeinsamen Teiler $d = ggT(a, b)$
- Weiterhin gibt es ganze Zahlen α, β mit

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

7.8 Primzahlen:

$p \in N$ heißt Primzahl wenn $p \neq 1$ und 1 und p die einzigen Teiler von p sind.

7.9 Theorem:

Jede natürliche Zahl läßt sich als Produkt von Primzahlen darstellen. Diese Parstellung ist (bis auf die Reihenfolge) eindeutig.

7.10 Theorem:

Es gibt unendlich viele Primzahlen.

8. Rechnen mit Restklassen

8.1 Definition:

Zwei ganze Zahlen $a, b \in Z$ heißen „kongruent modulo m“, wenn die Differenz $a - b$ durch m teilbar ist.

geschrieben: $a \equiv b \mod m$

8.2 Satz:

Zu festem m $\in N$ heißt a $\equiv$ b mod m eine Relation auf $Z \times Z$

$$R = \{(a,b) \in Z \times Z | a \equiv b \text{ mod } m\}$$

Diese ist eine Äquivalenzrelation

8.3 Satz:

a, b $\in Z$ sind genau dann kongruent modulo m, wenn sie bei division durch m den gleichen Rest besitzen.

8.4 Definition:

Ist a $\in Z$, m $\in N$ so wird der Rest bei Division durch m mit a mod m bezeichnet

(nicht verwechseln: a $\equiv$ b mod m $\Rightarrow$ wahr / falsch   a mod m $\Rightarrow$ Zahl)

Die Aussage des letzten Satzes lautet:

a $\equiv$ b mod m $\Leftrightarrow$ a mod m = b mod m

Erinnerung: Zwei Äquivalenzklassen sind entweder gleich oder disjunkt:

$$[v] := \{a \in Z | a \equiv r \text{ mod } m\}$$

8.5 Satz:

Die Äquivalenzklassen der Relation „ $\equiv$ mod m“ sind genau die Äquivalenzklassen von 0, 1, ... m-1

d.h. $Z = [0] \cup [1] \cup \ldots \cup [m-1]$

8.6 Definition:

Die Äquivalenzklassen bezüglich „ $\equiv$ mod m“ heißen auch <u>Restklassen</u>.

1, 2, ... m-1 sind Repräsentanten der m verschiedenen Restklassen.

Mit Restklassen kann man „rechnen“ – addieren und multiplizieren – wie in Z

8.7 Definition:

a, b seien Repräsentanten zweier Restklassen (m $\in N$)

([a], [b])

dann setzt man: a $\oplus$ b := [a] $\oplus$ [b] := [a + b] = [a + b mod m]

a $\otimes$ b := [a] $\otimes$ [b] := [a * b] = [a * b mod m]

8.8 Satz:

(a mod m) + (b mod m) $\equiv$ (a + b) mod m

(a mod m) * (b mod m) $\equiv$ (a * b) mod m

8.9 Theorem: (kleiner Fermatscher Satz)

p $\in N$ fest, p Primzahl

$[a] \neq [0]$ $[a]^{p-1} = [1]$

Was besagt er: p Primzahl, a nicht durch p teilbar

dann gilt: p \ $(a^{p-1} - 1)$

---

9. Algebraische Strukturen

9.1 Definition:

Eine <u>Gruppe</u> ist ein Paar (G,*) mit einer Menge G und einer Verknüpfung * auf G – d.h. eine Abbildung

$* : G \times G \to G$

$(a, b) \mapsto a * b$

mit folgenden Eigenschaften:

(G1) (a * b) * c = a * (b * c)

(G2) es gibt ein Element e in G (<u>neutrales Element</u>) mit

(G2a) e * a = a $\forall$ a $\in$ G

(G2b) zu jedem a $\in$ G gibt es ein a‘ $\in$ G mit a * a‘ = e (<u>inverses Element</u>)

Eine Gruppe (G, *) heißt <u>abelsche Gruppe</u> oder auch <u>kommutative Gruppe</u> wenn gilt:

(G3) a * b = b * a $\forall$ a, b $\in$ G

Falls klar ist, welche Verknüpfung gemeint ist, schreibt man auch kurz G statt (g, *) Schreibweisen: $ab = a * b$

9.2 Bemerkung:

Sei $(G, *)$ Gruppe

a) für ein neutrales Element $e \in G$ gilt $a * e = a \; \forall a \in G$

b) es gibt genau ein $e \in G$ mit $ea = a \; \forall a \in G$

c) ist a' inverses Element zu a, dann gilt auch $a * a' = e$

d) zu jedem $a \in G$ gibt es genau ein inverses Element – welches auch mit a^{-1} bezeichnet wird

---

9.3 Satz:

$(G, *)$ genau dann eine Gruppe wenn:

(G1) gilt und wenn es zu je zwei Elementen $a, b \in G$ ein $x \in G$ und $y \in G$ gibt so daß:

$x * a = b$

$a * y = b$

x und y sind dann (durch a und b) eindeutig bestimmt

9.4 Bemerkung:

G Gruppe $a, b \in G$

a) $(a^{-1})^{-1} = a$

b) $(ab)^{-1} = b^{-1} * a^{-1}$

9.5 Definition:

sei $(G, *)$ Gruppe

$H \subset G, H \neq 0$ heißt Untergruppe von G wenn:

1. $a * b \in H$ $a, b \in H$
2. $(H, *)$ ist Gruppe

---

10. Ringe

10.1 Definition:

Ein Tripel $(R, +, *)$ bestehend aus der Menge $R \neq 0$ und zwei Verknüpfungen

$+ : R \times R \to R$

$(a, b) \mapsto a + b$

$* : R \times R \to R$

$(a, b) \mapsto a * b$

heißt Ring wenn gilt:

(R1) $(R, +)$ ist abelsche Gruppe (mit neutralem Element 0 und negativem zu $a := -1$)
Schreibweise: $a + (-b) =: a - b$

(R2) Assoziativgesetz:
$(a * b) * c = a * (b * c) \; \forall a, b, c \in R$

(R3) Distributivgesetz:
$a * (b + c) = a * b + a * c$
$(a + b) * c = a * c + b * c$

10.2 Definition:

a) $(R, +, *)$ heißt kommutativer Ring, wenn gilt:
$a * b = b * a \; \forall a, b \in R$

b) ein Element $1 \in R$ heißt Einselement von R falls gilt:
$1 * a = a \; \forall a \in R$

c) Schreibweisen:
so erklärt man die Potenz induktiv durch:
$a^1 := a$
$a^k := aa^{k-1}$ k ✄ $2, k \in N$
Falls R ein Einselement besitzt so schreibe auch
$a^0 := 1$

10.3 Bemerkung:
(r, +, *) Ring
a) $a * 0 = 0 * a = 0$
b) $(-a) * b = -(a * b)$
c) $(-a) * (-b) = a * b$
d) $a \in R \quad m, n \in N$
$a^m * a^n = a^{m+n}$
$(a^m)^n = a^{mn}$

10.4 Definition und Satz:
(R, +, *) Ring
$S \subset R$ (S, +, *) ist genau dann ein Ring, wenn:
(S, +) Untergruppe von (R, +) und $a * b \in S \ \forall\ a, b \in S$
S heißt dann <u>Unterring</u> von R

---

11. Körper

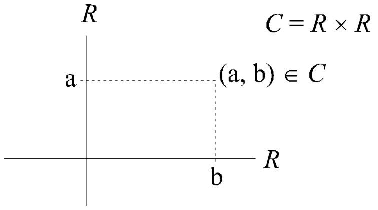
11.1 Definition:
Ein Tripel (K, +, *) mit zwei Vernüpfungen
$+ : K \times K \to K$
$* : K \times K \to K$
keißt Körper wenn gilt
a) (K, +, *) ist kommutativer Ring
b) es gibt ein $1 \in K$ mit $a * 1 = 1 * a = a \ \forall a \in K$
c) zu $a \in K^* := K \setminus \{0\}$ existiert ein $a^{-1} \in K$ mit $a * a^{-1} = 1$

11.2 Satz:
(Z|p, +, *) ist Körper $\Leftrightarrow$ p ist Primzahl

---

12. Körper der Komplexen Zahlen

12.1 Definition:
$C := R \times R = R^2 = \{(a, b) \mid a, b \in R\}$
Vorstellung:



algebraische Strukturen auf C:
1. Auf C läßt sich eine Addition definieren:
$+ : C \times C \to C$
$((a, b), (c, d)) \mapsto (a, b) + (c, d) := (a + c, b + d)$
1‘. Es gibt auch eine sogenannte Skalarmultiplikation:
$* : R \times C \to C$
$(\lambda, (a, b)) \mapsto \lambda * (a, b) := (\lambda a, \lambda b)$
(C mit + und obigem $* : R \times C \to C$ bildet eine sogenannten Vektorraum über R)

Bemerkung: (c, +) ist eine ablesche Gruppe

Frage: Gibt es eine Multiplikation von $C \times C \to C$, so daß (C, +, *) ein Körper wird ? Ja!

2. $* : C \times C \to C$
$((a, b), (c, d)) \mapsto (a, b) * (c, d) := (ac - bd, ad + bc)$

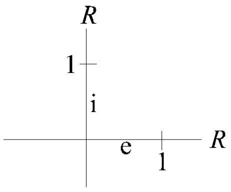
12.2 Satz:

C mit Abbildungen + und * wie in 1. und 2. angegeben ist ein Körper: Körper der Komplexen Zahlen

Nullelement: $0 = (0, 0)$
Einselement: $e = (1, 0)$
Inverses zu x = (a, b): $x^{-1} = \frac{1}{a^2 + b^2} * (a, -b)$

12.3 Definition:

e := (1, 0) ∈ *C* Einselement
i := (0, 1) ∈ *C* imaginäre Zahl
Anschaulich:



Damit: $C : R \times R = R * e + R * i$
Denn: (a, b) = a * e + b * i
es gilt auch: $i^2 = -e$

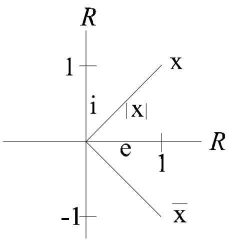
12.4 Definition:

Sei x = (a, b) ∈ *C*

$\bar{x} := \overline{(a,b)} := (a, -b)$ konjugierte komplexe Zahl

$|x| := \sqrt{a^2 + b^2}$ Betrag der komplexen Zahl

Anschaulich:



12.5 Interessante Formel:

$x = (a, b) \in C$

$x * \bar{x} = (a,b) * (a,-b) = (aa + bb, -ab + ba) = (a^2 + b^2, 0) = (a^2 + b^2) * (1,0) = (a^2 + b^2) * e = |x|^2 * e$

$x * \bar{x} = |x|^2 * e$

12.6 Definition:

x = a + ib ∈ *C*
a) Re(x) := a Realanteil von x
b) Im(x) := b Imaginäranteil von x

12.7 Regeln über Absoloutbetrag:

x, y ∈ *C*
1. |x| ✂ 0; |x| = 0 ⇔ x = 0
2. |x * y| = |x| * |y|
3. |x + y| ✁ |x| + |y|
4. |x – y| ✁ |x| + |y|
5. |x| ✁ |Re(x)|+|Im(x)|

12.8 Theorem:

Hauptsatz der Algebra

Jede Gleichung $a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = 0$

mit $a_i \in C$, i = 0, 1, ... k hat in *C* eine Lösung.

13. Lineare Algebra

13.1 Definition:

(K, +, *) sei Körper

Ein Tripel (V, +, *) heißt Vektorraum über dem Körper K, wenn gilt:

+, * sind Abbildungen:

$+ : V \times V \to V$ Addition

$(u, w) \mapsto v + w$

$* : K \times V \to V$ Skalarmultiplikation

$(\lambda, v) \mapsto \lambda * v$

für die gilt:

(V1) (V, +) ist kommutative Gruppe

(mit neutralem Element 0 und $-v \in V$ ist negativer Vektor zu $v \in V$)

(V2) $\forall\, v, w \in V \quad \lambda, \mu \in K$

a) $(\lambda + \mu) * v = \lambda * v + \mu * v$

b) $\lambda * (v + w) = \lambda * v + \lambda * w$

c) $(\lambda * \mu) * v = \lambda * (\mu * v)$

d) $1 * v = v$

Elemente von V heißen Vektoren

Elemente von K heißen Skalare

Statt $\lambda * v$ auch λv

Vektorräume über dem Körper *R* nennt man auch reelle Vektorräume

13.2 Definition:

$x = (x_1, \ldots, x_n)$

$y = (y_1, \ldots, y_n)$

$+ : V \times V \to V$

$(x, y) \mapsto x + y := (x_1 + y_1, \ldots, x_n + y_n)$

$* : K \times V \to V$

$(\lambda, x) \mapsto \lambda x := (\lambda x_1, \ldots, \lambda x_n)$

13.3 Bemerkung:

a) $0 * v = 0$

$\lambda * 0 = 0$

b) $\lambda * v = 0 \Rightarrow \lambda = 0$ oder $v = 0$

$(-1) * v = -v$

13.4 Definition:

(V, +, *) sei Vektorraum über K

$W \subset V$

W heißt Untervektorraum von V falls gilt:

(UV1) $W \neq 0$

(UV2) $v, w \in W \Rightarrow v + w \in W$

(UV3) $\lambda \in K, v \in V \Rightarrow \lambda v \in W$

(W ist abgeschlossen bezüglich + und *)

13.5 Bemerkung:

- $W \subset V$ sei Untervektorraum von V, dann ist (W, +, *) wieder Vektorraum über K
- Der Schnitt mehrerer Untervektorräume ist wieder ein Untervektorraum

14 Dimensionen

14.1 Definition:

V sei Vektorraum über K

$v_1, ..., v_r \in V$

$\lambda_1, ..., \lambda_r \in K$

a) $\lambda_1 v_1 + ... + \lambda_r v_r$ heißt Linearkombination der Vektoren $v_1, ..., v_r$

b) $L(v_1, ..., V_r) := \{\lambda_1 v_1 + ... + \lambda_r v_r \mid \lambda_i \in K\}$ ist Menge der Linearkombinationen der Vektoren $v_1, ..., v_r$ heißt Lineare Hülle der Vektoren $v_1, ..., v_r$

$L(v_1, ..., v_r) = Kv_1 + ... + Kv_r$

c) $v_1, ..., v_r$ heißen linear unabhängig, wenn eine Linearkombination von $v_1, ..., v_r$ nur dann den Nullvektor ergibt, wenn alle Koeffizienten $\lambda_1, ..., \lambda_r = 0$ sind:

$\lambda_1 v_1 + ... + \lambda_r v_r = 0 \Rightarrow \lambda_1 = ... = \lambda_r = 0$

14.2 Satz:

$(v_1, ..., v_r)$ linear unabhängig $\Leftrightarrow$ keiner der Vektoren $v_1, ..., v_r$ ist Linearkombination der anderen.

14.3 Definition:

V sei Vektorraum über K

Ein n-Tupel von Vektoren aus V (v1, ..., vn) heißt Basis von V wenn gilt:

1. $L(v_1, ..., v_n) = V$
2. $v_1, ..., v_n$ linear unabhöngig

14.4 Satz:

Ist $(v_1, ..., v_n)$ eine Basis von V so gibt es zu jedem Vektor genau ein $(\lambda_1, ..., \lambda_n) \in K^n$ mit

$v = \lambda_1 v_1 + ... + \lambda_n v_n$

15. Dimensionsbegriff

15.1 Satz: (Basisergänungssatz)

V sei Vektorraum über K

$v_1, ..., v_r \in V$

$w_1, ..., w_s \in V$

wenn gilt:

1. $(v_1, ..., v_r)$ linear unabhängig
2. $L(v_1, ..., v_r, w_1, ..., w_s) = V$

dann kann man $(v_1, ..., v_r)$ durch eventuelle hinzunahme von Vektoren aus $(w_1, ..., w_s)$ zu einer Basis von V ergänzen.

15.2 Satz: (Austauschlämma)

Seien $(v_1, ..., v_n)$ und $(w_1, ..., w_m)$ Basen von V, dann gibt es zu jedem v_i ein w_j, so daß aus $(v_1, ..., v_n)$ wieder eine Basis entsteht, wenn v_i durch w_j ersetzt wird.

15.3 Satz:

V sei Vektorraum über K

Wenn V eine Basis $(v_1, ..., v_n)$ besitzt und $(w_1, ..., w_m)$ eine weitere Basis von V ist, dann gilt n = m.

15.4 Definition:

Besitzt ein Vektorraum V über K eine Basis $(v_1, ..., v_n)$ so ist n eindeutig bestimmt. Diese ist also nur von V abhängig, und heißt:

n =: dim(V) (Dimension von V)

dann ist V endichdimensional.

15.5 Satz:

V sei Vektorraum über K dim(V) = n

dann sind mehr als n Vektoren immer linear abhängig.

15.6 Satz:

Sei V endlichdimensional und $W \subset V$ ein Untervektorraum

$\Rightarrow$ W ist auch endlichdimensional und es gilt:

dim(W) ✂ dim(V)

15.7 Definition:

Sei V Vektorraum über K

U_1 und U_2 seien Untervektorräume von V

$$U_1 + U_2 := \{u_1 + u_2 \mid u_1 \in U_1, u_2 \in U_2\} \subset V$$

dies ist ein Untervektorraum von V

15.8 Satz: (Dimensionsformel)

U_1 und U_2 seien endlichdimensionale Untervektorräume von V

$$\dim(U_1 \cap U_2) + \dim(U_1 + U_2) = \dim(U_1) + \dim(U_2)$$

16. Lineare Abbildungen

16.1 Definition:

V und W seien Vektorräume über dem gleichen Körper K

Eine Abbildung $f : V \to W$ heißt linear (oder Vektorraumhomomorphismus) wenn gilt:

$f(a + b) = f(a) + f(b)$

$f(\lambda * a) = \lambda * f(a)$

$a, b \in V \qquad \lambda \in K$

16.2 Bemerkung:

a) $V \xrightarrow{f} W \xrightarrow{g} Y$ mit V, W, Y sind Vektorräume über K und f, g sind linear

dann gilt: $g \circ f : V \to Y$ ist linear

b) $id : V \to Y$ ist linear

16.3 Definition:

$f : V \to W$ sei lineare Abbildung

a) $Bild(f) := Im(f) := f(V) \subset W$ — Bild von f

b) $Kern(f) := f^{-1}(\{0\}) = \{v \in V \mid f(v) = 0\} \subset V$ — Kern von f

16.4 Satz:

Kern(f) ist Untervektorraum von V

Im(f) ist Untervektorraum von f

16.5 Satz:

V, W seien Vektorräume über K

$(v_1, ..., v_n)$ ist Basis von V ($\dim(V) = n$)

$w_1, ..., w_n$ beliebige Vektoren aus W

dann gibt es genau eine lineare Abbildung

$f : V \to W$ mit $f(v_i) = w_i \qquad i = 1, ..., n$

16.6 Bemerkung:

Dieser Satz besagt, daß eine Abbildung dadurch festgelegt ist, wenn man eine Basis von V kennt, und deren Bilder in W.

16.7 Satz:

$f : V \to W$ sei linear

a) f ist surjektiv $\Leftrightarrow Im(f) = W$

b) f ist injektiv $\Leftrightarrow Kern(f) = \{0\}$

16.8 Satz:
$f : V \to W$ sei linear
$v_1, ..., v_n$ ist Basis von V, dann gilt:
$Im(f) = L(f(v_1), ..., f(v_n))$

16.9 Satz:
$f : V \to W$ sei linear $(v_1, ..., v_n)$ ist Basis von V
f bijektiv $\Leftrightarrow$ f ist injektiv und surjektiv $\Leftrightarrow$ Kern(f) = {0} und Im(f) = W $\Leftrightarrow$ $f(v_1), ..., f(v_n)$ ist Basis von W

16.10 Folgerung:
Je zwei n-dimensionale Vektorräume sind <u>Isomorph</u> – d.h. es Existiert eine bijektive lineare Abbildung
$f : V \to W$

16.11 Definition:
$f : V \to W$ sei lineare Abbildung
rg(f) := dim(Im(f)) (<u>Rang</u>)

16.12 Bemerkung:
falls W endlichdimensional:
a) rg(f) ✄ dim(W)
b) rg(f) = dim(W) $\Leftrightarrow$ f ist surjektiv

16.13 Theorem: (<u>Dimensionsformel</u> für lineare Abbildungen)
V sei n-dimensionaler Vektorraum über K
W sei beliebiger Vektorraum über K
 $f : V \to W$ lineare Abbildung
dann gilt:
 dim(Kern(f)) + rg(f) = n

---

17 Lineare Gleichungssysteme

17.1 Definition:
Unter einem <u>linearen Gleichungssystem</u> versteht man ein System mit m linearen Gleichungen und n unbekannten $x_1, ..., x_n$.

$$a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n} + x_n = b_1$$
$$a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n} + x_n = b_2 \qquad \text{(Dieses System wird fortan mit (*) bezeichnet)}$$
$$\vdots$$
$$a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn} + x_n = b_m$$

Unter einer Lösung von (*) versteht man ein $(a_1, ..., a_n) \in R^n$, so daß x_i mit a_1 eingesetzt (*) löst.
Unter dem Lösungsraum von (*) versteht man
 $L := \{a \in R^n \mid a \text{ ist Lösung von } (*)\}$

17.2 Schreibweisen:
gegeben: $A : R^n \to R^m$
 $(e_1, ..., e_n)$ = kanonische Basis
Schreibe die n Vektoren $a_i = A(e_i) \in R^m$ i = 1, ..., n als Spalten in folgendem System nieder:

$$\begin{array}{cccc} \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & & & \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \\ \uparrow \quad \uparrow \qquad \quad \uparrow \\ A(e_1)\, A(e_2) \quad A(e_n) \end{array}$$

m Zeilen und n Spalten

17.3 Definition:

Dieses System nennt man eine Matrix.
geschrieben:

(a_{ij}) i = 1, ..., m
i = 1, ..., n

Also durch die Angabe einer m×n Matrix wird eindeutig eine lineare Abbildung $A : R^n \to R^m$ beschrieben.

17.4 Definition:

$A : R^n \to R^m$ sei lineare Abbildung
Die zughörige Matrix (a_{ij}) wird ebenfalls mit dem gleichen Buchstaben wie die Abbildung bezeichnet.

$A = (a_{ij})$ i = 1, ..., m j = 1, ..., n

Die Multiplikation wird mit Matrix * Vektor A * x oder kurz mit Ax bezeichnet

$A(x) = A * x = Ax$

17.5 Bezeichnungen:

a) $\mathrm{Hom}(R^n, R^m) := \{A : R^n \to R^m \mid A \text{ linear}\}$
b) $M(n\times m) := \{A \mid A \text{ ist } n\times m \text{ Matrix}\}$

17.6 Schreibweisen:

$L = L(A, b)$ $A \in A(m\times n)$ $b \in R^m$

$L(A, b) = A^{-1}(\{b\})$
$A \in \mathrm{Hom}(R^m, R^n)$
$(*) = Ax = b$

17.7 Beobachtungen:

1. Zwei Zeilen in einem Gleichungssystem dürfen vertauscht werden.
2. Eine Zeile darf mit $\lambda \in R$ multipliziert werden.
3. Addition des λ-fachen einer Zeile zu einer anderen ist erlaubt.

Diese Manipulationen nennt man elementare Zeilenumformungen.

17.8 Definition:

Erweiterte Matrix $(a_{ij} \mid b) = (A|b)$
Zeilenstufenform der erweiterten Matrix: die Anzahl der von 0 verschieden Zeilen ist rg(A|b)

17.9 Satz:

Es gilt: Spaltenrang gleich Zeilenrang der Matrix A

17.10 Definition:

$A \in M(m\times n)$
A^t := Matrix aus A konstruiert, in der die Zeilen mit den Spalten vertauscht werden

transponierte Matrix

dann: $A^t \in M(n\times m)$

17.11 Satz:

$Ax = b$ Gleichungssystem $A \in M(m\times n)$ $b \in R^m$
hat Lösung $\Leftrightarrow$ rg(A) = rg(A|b)

17.12 Satz:

$A : R^n \to R^m$ sei linear $b \in R^m$
und es gilt $A^{-1}(\{b\}) \neq 0$
dann: $L(A, b) = A^{-1}(\{b\}) = x_s + \mathrm{Kern}(A)$
wobei x_s eine (spezielle) Lösung von $Ax = b$ ist.

17.13 Folgerung:

Falls Ax = b eine Lösung hat, dann:
Lösung ist eindeutig $\Leftrightarrow$ Kern(a) = {0} $\Leftrightarrow$ A ist injektiv $\Leftrightarrow$ dim(Kern(A)) = 0 $\Leftrightarrow$ rg(A) = n

18. Determinante

18.1 Satz:

Es gibt eine eindeutig bestimmte Abbildung D : M(n×n) → R mit folgenden Eigenschaften:

1. D ist linear in jeder Spalte:
   a) $D(a_1, \cdots, a_i + \overline{a_i}, a_{i+1}, \cdots, a_n) = D(a_1, \cdots, a_i, a_{i+1}, \cdots, a_n) + D(a_1, \cdots, \overline{a_i}, a_{i+1}, \cdots, a_n)$
   b) $D(a_1, \cdots, \lambda a_i, \cdots, a_n) = \lambda * D(a_1, \cdots, a_i, \cdots, a_n)$
2. D(A) ≠ 0 ⇔ Spalten von A sind linear unabhängig
3. D(E) = 1 (E ist <u>Einheitsmatrix</u>)

Diese Abbildung heißt <u>Determinante</u>

18.2 Definition:

Determinante von Matrix A ∈ M(n×n) kurz det(A)

det : M(n×n) → R

A ↦ det(A)

18.3 Satz:

Sei A ∈ M(2×2)

$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ dann ist

$$\det(M) = \det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$$

det(A * B) = det(A) * det(B)

18.4 Satz:

A ∈ M(n×n)

A‘ entstehe aus A durch vertauschen von zwei Spalten. Dann gilt:

det(A‘) = -det(A)

18.5 Satz:

A ∈ M(n×n)

dann: A^t ∈ M(n×n) und det(A^t) = det(A)

18.6 Berechnung einer 3×3 Matrix:

Regel nach Sarus

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

19. Eigenwerte / Eigenvektoren / charakteristisches Polynom

19.1 Definition:

Sei A ∈ M(n×n) A : $R^n \to R^n$ lineare Abbildung

a) Eine Zahl λ ∈ R heißt <u>Eigenwert von A</u>, wenn es einen Vektor b ∈ R^n mit b ≠ 0 gibt, so daß:
   A(b) = λb ist.
b) Wenn λ ein Eigenwert von A ist, so heißt jeder Vektor b ∈ R^n mit A(b) = λb <u>Eigenvektor von A</u> zum Eigenwert λ.
c) Das Polynom: $X_A(\lambda) := \det(A - \lambda E)$ λ ∈ R
   heißt <u>charakteristisches Polynom von A</u>

19.2 Bemerkung:

Einige Koeffizienten von $X_A(\lambda)$ kann man bereits an der Matrix A ablesen:

$X_A(\lambda) = (-\lambda)^n + \text{Spur}(A) * (-\lambda)^{n-1} + \ldots + \det(A)$

wobei: Spur(A) = Summe der Diagonalelemente von A)

19.3 Satz:

$A \in M(n \times n)$

$\lambda \in R$ ist Eigenwert von A $\Leftrightarrow X_A(\lambda) = 0$ (λ ist Nullstelle des charakteristischen Polynoms)

20. Geometrisch- algebraische Zusammenhänge

20.1 Definition:

Die Abbildung:

$<*, *> : R^n \times R^n \to R$

$(x, y) \mapsto x_1, y_1 + \ldots + x_n y_n =: <x, y>$

heißt das <u>übliche Skalarprodukt.</u>

20.2 Satz:

Skalarprodukt hat folgende Eigenschaften:

1. Bilinear: d.h. $<*, *>$ ist linear in jeder Komponente:
   $<a, b + c> = <a, b> + <a, c>$
   $<a, \lambda b> = \lambda * <a, b>$
   $<a + b, c> = <a, c> + <b, c>$
   $<\lambda a, b> = \lambda * <a, b>$
2. Symetrisch:
   $<a, b> = <b, a>$
3. positiv definit:
   $<x, y> > 0$ falls $x \neq 0$

20.3 Definition:

Die Abbildung:

$\| \ \| : R^n \to R$

$x \mapsto \|x\| := \sqrt{\langle x, x \rangle}$

heißt <u>Betrag</u> oder <u>Norm</u>.

20.4 Satz:

Es gilt:

1. $\|x\|$ ✂ $0 \ \forall x \in R^n$
2. $\|x\| = 0 \Leftrightarrow x = 0$
3. $\|\lambda x\| = |\lambda| * \|x\|$
4. $\|x + y\|$ ✁ $\|x\| + \|y\|$

20.5 Theorem:

1. $\|x\|$ ist die <u>Länge des Vektors x</u>
2. $|<x, y>|$ ✁ $\|x\| * \|y\|$ damit gilt:
   $<x, y> = r * \|x\| * \|y\|$ mit $|r|$ ✁ 1 und $r \in R$
   Definiere: $r = \cos(\alpha)$ und α ist <u>Winkel zwischen x und y</u>
   also: $<x, y> = \|x\| * \|y\| * \cos(\alpha)$
3. $|\det(v_1, \ldots, v_n)|$ = <u>Volumen des Spates</u> welcher von den n Vektoren $v_1, \ldots, v_n$ aufgespannt wird.

20.6 Definition:

1. $x, y \in R^n$
   $x \perp y :\Leftrightarrow <x, y> = 0$ (<u>x senkrecht y</u>)
2. n Vektoren $\in R^n$ $(v_1, \ldots, v_n)$ heißen <u>positiv orientiert</u>, wenn $\det(v_1, \ldots, v_n) > 0$ ist.

20.7 Erinnerung:

$a > 0$

$x^2 - a = 0 \quad L = \{\pm \sqrt{a}\}$

$a < 0$

$x^2 - a = 0 \quad L = \{\pm \sqrt{a} * i\}$

20.8 Definition:

$ax^2 + bx + c = 0$ gegeben:

Dann heißt der Ausdruck:

$$D := \frac{b^2}{4a^2} - \frac{c}{a}$$ Diskriminante

Bisher bekannt: $\sqrt{a}$ nur sinnvoll wenn a ✄ 0

Neue Schreibweise:

$$\sqrt{a} = \sqrt{-a} * i \qquad \text{für alle } a < 0$$

Dann Lösungsmenge von $ax^2 + bx + c = 0$

$$L = \left\{ \frac{-b}{2a} \pm \frac{\sqrt{b^2 - 4ac}}{2a} \right\}$$

20.9 Theorem: (Cauchy – Schwarz Ungleichung)

a, b ∈ R^n dann:

<a, b> ✄ $||a||^2 * ||b||^2$

Gleichheit ⇔ a und b sind linear abhängig

Folgerung: |<a, b>| ✄ ||a|| * ||b||

21. Polynomringe

21.1 Definition:

K sei Körper

1. K[x] := {Polynome in x mit Koeffizienten in K}

$$= \left\{ \sum_{i=1}^{n} a_i x^i \middle| a_i \in K, n \in N_0 \right\}$$

2. Sei p(x) ∈ K[x] mit

$p(x) = a_0 + ... + a_n x^n$ und $a_n \neq 0$

$$\deg(p) := \begin{cases} n & falls\ p \neq 0 \\ -\infty & falls\ p(x) \equiv 0 \end{cases}$$ (Grad von p)

an nennt man den Leitkoeffizienten von p

Falls $a_n = 1$, so nennt man p normiert

21.2 Bemerkung:

1. (K[x], +, *) ist kommutativer Ring
   (mit Einselement 1 und null = 0)
2. deg(f * g) = deg(f) + deg(g)

21.3 Theorem:

Division mit Rest in K[x] K sei Körper f, g ∈ K[x]

Polynome mit f ≠ 0 und g ≠ 0

deg(f) =: m deg(g) =: n

Dann gibt es eindeutig bestimmte Polynome q, r ∈ K[x] mit:

f = q * g + r und deg(r) < deg(q)

22. Hornerschema

22.1 Satz:

Sei $f(x) = a_n x^n + ... + a_0$ $a_n \neq 0$ $n \geq 1$ $b \in R$

Für die Zahlen:

$$c_n := a_n$$
$$c_{n-1} := c_n * b + a_{n-1}$$
$$\vdots$$
$$c_{n-k} := c_{n-k+1} * b + a_{n-k}$$
$$\vdots$$
$$c_0 := c_1 * b + a_0$$

gilt:

1. $c_0 = f(b)$
2. $f(x) = (x - b)(c_n x^{n-1} + c_{n-1} x^{n-2} + ... + c_2 x + c_1 + f(b))$

22.2 Regel:

Kennt man eine Nullstelle b eines Polynoms f(x), so bilde zunächst die Faktorisierung:

$f(x) = (x - b)h(x)$

Dann suche Nullstelle von h(x)