

Lineare Algebra I (lehramtsbezogen)

<https://www.mi.fu-berlin.de/kvv/course.htm?cid=10310>

— kein Skript (nur Notizen und Inhaltsangaben, ohne Garantie) —
— Ich bin dankbar für Hinweise auf Fehler, Korrekturen, Ergänzungen, Verbesserungsvorschläge, etc.
— Version vom 8. Februar 2012 —

Prof. Günter M. Ziegler

Fachbereich Mathematik und Informatik

FU Berlin, 14195 Berlin

Tel. (030) 838 75 668

ziegler@math.fu-berlin.de

<http://page.mi.fu-berlin.de/gmziegler/>

FU Berlin, Winter 2011/2012

0. Lineare Geometrie des n -dimensionalen reellen Raums: \mathbb{R}^2 , \mathbb{R}^3 , Vektoren. Geraden, Ebenen, Skalarprodukt, Abstands- und Winkelmessung, Vektorprodukt, lineare Gleichungssysteme, Lösbarkeitsbedingungen, Gauß-Algorithmus, Lösungsraum
1. Grundbegriffe: Mengen, Abbildungen, Äquivalenzrelationen, grundlegende algebraische Strukturen: Gruppen, Körper
2. Vektorräume und Lineare Abbildungen: Unabhängigkeit, Erzeugendensysteme, Basis, Dimension, Unterraum, Koordinaten, Lineare Abbildungen, Matrizen, Zusammenhang zwischen linearen Abbildungen und Matrizen, Kern und Bild einer linearen Abbildung, Rang einer linearen Abbildung und einer Matrix, Basistransformationen, Transformationsformeln, Lineare Gleichungssysteme
3. Determinanten, Definition, Eigenschaften, Rechenregeln.

Literatur

- [1] Gerd Fischer. *Lernbuch Lineare Algebra und Analytische Geometrie*. Vieweg+Teubner, Wiesbaden, 2011.

Vorbemerkungen

1. Einführung Mi, 19. Oktober
2. *Feststellungstest* Mo, 24. Oktober
3. Zahlen; Zahlbereiche; Rechenregeln; (Körper) Mi, 26. Oktober
4. Beweis auf Widerspruch; Summennotation; vollst. Induktion; reelle Zahlen Mo, 31. Oktober
5. reelle Zahlen; die Menge \mathbb{R}^n Mi, 2. November
6. Vektorraum \mathbb{R}^n ; Geraden, Ebenen etc.: innere und äußere Beschreibung Mo, 7. November
7. Gleichungssysteme, Lösungsraum, Matrix-Darstellung, Gauß-Elimination Mi, 9. November
8. Winkel, Abstände, Skalarprodukt. Cauchy–Schwarz, Pythagoras, Hesse-Nf. . . Mo, 14. November
9. **1.** Mengen, Operationen mit Mengen, Abbildungen, injektiv, surjektiv Mi, 16. November
10. injektiv, surjektiv, Bild, Urbild, Umkehrabbildung, Komposition Mo, 21. November
11. abzählbare Mengen **1.2** Gruppen Mi, 23. November
12. Gruppentafeln, **1.3** Ringe und Körper Mo, 28. November
13. Körper, komplexe Zahlen, endliche Körper Mi, 30. November
14. komplexe Zahlen, **1.4** Polynome, Grad Mo, 5. Dezember
15. Ring der Polynome, Polynomdivision mit Rest, Fundamentalsatz der Algebra .. Mi, 7. Dezember
16. reeller Fundamentalsatz, **2.** Vektorräume Definition Mo, 12. Dezember
17. Lineare Unabhängigkeit, Erzeugendensysteme Mi, 14. Dezember

18. Vektorraum (Wdh.), Untervektorräume, Beispiele: Spaltenraum, Zeilenraum, Kern, Mo, 2. Januar
19. linear unabhängig Mi, 4. Januar
20. Erzeugendensysteme **2.2** Basis und Dimension Mo, 9. Januar
21. **2.3** Lineare Abbildungen, Kern und Bild, Dimensionsformel Mi, 11. Januar
22. **2.4** Matrizen, darstellende Matrix Mo, 16. Januar
23. Matrixmultiplikation Mi, 18. Januar
24. Lineare/homogene Gleichungssysteme, Rang und Kern, Elementarmatrizen Mo, 23. Januar
25. **2.5** Basiswechsel, Transformationsformel Mi, 25. Januar
26. Elementarmatrizen, Faktorisierung, Berechnung der Inversen Mo, 30. Januar
27. Normalform für darstellende Matrix; **3.** Determinanten, I Mi, 1. Februar
28. Determinanten, II Mo, 6. Februar
29. Klausur Mi, 8. Februar
30. Gerd Fischer: Zur Geschichte Mo, 13. Februar
31. Zur Geometrie Mi, 15. Februar

0 Lineare Geometrie im n -dimensionalen reellen Raum

26. Oktober 2011

0.1 Der n -dimensionale reelle Raum

Lineare Algebra-Vorlesung – wir wollen trotzdem mit Geometrie anfangen, weil Geometrie etwas ist, was man unmittelbar vor Augen hat. Daher ist Geometrie auch Jahrtausende alt, Algebra aber eine Erfindung der Neuzeit.

EUKLID (300 vor Christus):

1. Ein *Punkt* ist, was keine Teile hat.
2. Eine *Linie* ist eine breitenlose Länge.

usw. Der formale, axiomatische Zugang ist unintuitiv, führt auf lauter merkwürdige Geometrie-Modelle. Schwierig, 1899 von DAVID HILBERT mit seinen *Grundlagen der Geometrie* perfektioniert.

Alternativ: nach RENÉ DESCARTES' (1637) "Discours de la methode" verwendet man "kartesische" *Koordinaten*, um Punkte im Raum durch *Zahlen* zu beschreiben.

0.1.1 Zahlen

Natürliche Zahlen $\mathbb{N} := \{0, 1, 2, 3, \dots\}$

Positive natürliche Zahlen $\mathbb{N}^* := \{0, 1, 2, 3, \dots\} = \mathbb{N} \setminus \{0\}$

Summe/Addition $m + n$, Produkt/Multiplikation $m \cdot n = mn$

Gleichung $m + x = n$ hat aber nicht immer eine Lösung: Erweiterung des Zahlbereichs

Ganze Zahlen $\mathbb{Z} := \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$

Addition (erweitert), Differenz/Subtraktion, Multiplikation (erweitert)

Gleichung $n \cdot x = m$ hat aber nicht immer eine Lösung: Erweiterung des Zahlbereichs

Rationale Zahlen (Brüche): $\mathbb{Q} = \{\frac{m}{n} : m, n \in \mathbb{Z}, n \neq 0\}$

— Gleichheit: $\frac{m}{n} = \frac{m'}{n'}$ genau dann wenn $m \cdot n' = m' \cdot n$ in \mathbb{Z} .

— Erweiterung: enthält die ganzen Zahlen: $m := \frac{m}{1}$, insbesondere $0 = \frac{0}{1} = \frac{0}{n}$, $1 = \frac{1}{1}$.

— Addition (erweitert), Subtraktion, Multiplikation (erweitert), Division (Nenner $\neq 0$).

— Inverse Zahlen: $r = \frac{m}{n}$ ergibt $-r := -\frac{m}{n}$ und $r^{-1} := \frac{n}{m}$ für $m \neq 0$.

Rechenregeln:

- A1** Assoziativität der Addition
- A2** Kommutativität der Addition
- A3** Neutrales Element der Addition
- A4** Inverse bzgl. Addition
- M1** Assoziativität der Multiplikation
- M2** Kommutativität der Multiplikation
- M3** Neutrales Element der Multiplikation
- M4** Inverse bzgl. Multiplikation
- D** Distributivgesetz(e)

Struktur, in der diese Regeln gelten, in denen wir also "wie mit Zahlen" rechnen können, heißt *Körper*.

In jedem Körper kann man lineare Gleichungen lösen: $ax + b = c$ hat die Lösung $(b + (-c)) \cdot a^{-1}$ für $a \neq 0$.

Beispiele für Körper: $\mathbb{Q}, \mathbb{R}, GF(2) := \{N, E\}$

Wiederholung: $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$. Rechenregeln charakterisieren Zahlbereich/“Körper”

Warum reichen uns (den alten Griechen) die Brüche/rationalen Zahlen nicht? Quadratische Gleichungen:

Lemma 0.1. *Es gibt keine rationale Zahl $r = \frac{m}{n}$ mit $r^2 = (\frac{m}{n})^2 = 2$*

Beweis. auf Widerspruch! □

Approximativ geht das aber sehr gut: $x_0 = 1, x_{n+1} = \frac{1}{2}(x_n + \frac{2}{x_n})$

$$x_0 = 1 \quad x_0^2 - 2 = -1$$

$$x_1 = \frac{3}{2} = 1,5 \quad x_1^2 - 2 = \frac{1}{4}$$

$$x_2 = \frac{17}{12} = 1,41\bar{6} \quad x_2^2 - 2 = \frac{1}{144}$$

$$x_3 = \frac{577}{408} = 1,4142156862745098039 \quad x_3^2 - 2 = \frac{1}{166464} \text{ etc.}$$

$$\sqrt{2} = 1,414213562\dots$$

Fragen: Fehler ist immer Stammbruch? Beliebiger Startwert? Beweisen, dass das konvergiert?

Dezimalentwicklung: natürliche Zahlen

$$n = z_N z_{N-1} \dots z_1 z_0 = z_N 10^N + z_{N-1} 10^{N-1} + \dots + z_1 10 + z_0 = \sum_{i=0}^N z_{N-i} 10^{N-i} = \sum_{j=0}^N z_j 10^j$$

mit $N \geq 0, z_i \in \{0, 1, \dots, 9\}, z_N \neq 0$.

Summen-Notation!

Beweis durch vollständige Induktion, Beispiel

$$\sum_{i=0}^n i = \frac{1}{2}n(n+1).$$

Induktionsanfang: Stimmt für $n = 0$

Induktionsschritt: Wenn das für einen Wert von n stimmt, so folgt es für $n + 1$.

Ganze Zahlen: genauso. Dezimaldarstellung ist *eindeutig* (wenn wir $z_N \neq 0$ fordern)

Rationale Zahlen: wiederholte Division mit Rest liefert

$$\frac{m}{n} = \pm z_N 10^N + z_{N-1} 10^{N-1} + \dots = \pm \sum_{i=0}^{\infty} z_{N-i} 10^{N-i}.$$

Eindeutig! Aber nicht jeder unendliche Dezimal“bruch” bildet eine rationale Zahl. Wir werden später sehen: Die Ziffernfolge z_i ist für jeden Bruch $\frac{m}{n}$ periodisch.

Aber auch wenn die Ziffernfolge nicht periodisch ist, liefert die unendliche Summe eine “reelle” Zahl. Aber dann gilt: Unterschiedliche Dezimalbrüche liefern nicht unbedingt dieselbe Zahl.

Die reellen Zahlen können aber auf unterschiedliche Weise eingeführt werden:

reelle Zahlen $\mathbb{R} = (??)$

- Dezimalbrüche (ohne unendliche Folge von Neunen!):

$$\mathbb{R} := \left\{ \pm \sum_{i=0}^{\infty} z_{N-i} 10^{N-i} : z_N \in \{1, \dots, n\}, z_{N-i} \in \{1, \dots, n\} \text{ für } i > 0 \right\} \cup \{0\}$$

- Dedekind-Schnitte

$$\mathbb{R} := \{A \subset \mathbb{Q} : A \neq \emptyset, A \neq \mathbb{Q}, \text{ nach unten abgeschlossen, ohne größtes Element}\}$$

- Äquivalenzklassen von Cauchy-Sequenzen

Zu zeigen ist, dass alle drei Modelle dasselbe beschreiben, dass sie wohldefiniert sind, und wie man mit ihnen rechnen kann.

Achtung: „Dezimalbrüche“ sind keine Brüche!

Zum Beispiel: Wann sind zwei reelle Zahlen gleich? Wie kann man sie addieren? Das ist alles nicht ganz trivial! Wir überlassen das der Analysis-Vorlesung. Uns reicht:

Rechenregeln:

- K** Körperaxiome (siehe oben)
- O1** Anordnung: jede Zahl ist entweder positiv ($x > 0$) oder 0 oder negativ ($x < 0$); wenn x positiv ist, ist das additive Inverse negativ.
- O2** Summen und Produkte von positiven Zahlen sind positiv
- Q** Quadratwurzeln aus positiven Zahlen existieren (eindeutig, wenn wir sie positiv wählen).

0.1.2 Der Vektorraum \mathbb{R}^n

\mathbb{R} = Zahlengerade

$\mathbb{R}^2 := \{(x, y) : x, y \in \mathbb{R}\}$ Punkte der Zeichenebene werden über Koordinatensystem mit Paaren von reellen Zahlen identifiziert

$\mathbb{R}^3 := \{(x, y, z) : x, y, z \in \mathbb{R}\}$ dto.: 3-dimensionaler “Anschauungsraum”

$\mathbb{R}^n := \{(x_1, \dots, x_n) : x_1, \dots, x_n \in \mathbb{R}\}$ dto.: n -dimensionaler Raum. Die Punkte sind durch geordnete n -Tupel von reellen Zahlen gegeben.

$\mathbb{R}^n = \{(x_1, \dots, x_n) : x_1, \dots, x_n \in \mathbb{R}\}$ sind die Punkte des n -dimensionalen Raums.

Nullpunkt $o = (0, \dots, 0)$

Addition mit $v = (v_1, \dots, v_n)$ entspricht einer *Translation*, die den Punkt o in den Punkt v überführt.

Streckung mit $\lambda \in \mathbb{R}$ *Skalarmultiplikation*, die o festhält und v auf λv streckt. (Auch für $\lambda = 0$!)

“das Wichtigste in Kürze”:

Rechenregeln für einen “**Vektorraum**”:

- A1** Assoziativität der Addition
- A2** Kommutativität der Addition
- A3** Neutrales Element der Addition
- A4** Inverse bzgl. Addition
- S1** Assoziativität der Skalarmultiplikation
- A3** Neutrales Element der Skalarmultiplikation
- D1** Distributivität 1
- D2** Distributivität 2

0.1.3 Geraden, Ebenen etc.: innere und äußere Beschreibung

Geraden, innere Beschreibung, äußere Beschreibung durch $ax + by = c$ (für \mathbb{R}^2)

Lösungsmenge von $a_1x_1 + \dots + a_nx_n = c$ ist eine *Hyperebene* in \mathbb{R}^n wenn nicht $a_1 = \dots = a_n = 0$

Allgemeiner:

Definition. Ein *affiner Unterraum* ist eine Teilmenge des \mathbb{R}^n :

- (I) alle Affinkombinationen von einem Punkt und einer Menge von Vektoren, oder leer
- (A) alle Lösungen einer Menge von “linearen” Gleichungen

Beispiel:

innere Beschreibung: Gerade durch $(1, 1)$ und $(47, 0) \longleftrightarrow$ äußere Beschreibung: Gerade $\{(x, y) : 5x + 42y = 47\}$

Definition 0.2 (Affiner Unterraum). Ein *affiner Unterraum* ist eine Teilmenge des \mathbb{R}^n :

(I) alle Affinkombinationen von einem Punkt und einer Menge von Vektoren, oder leer:

$$\begin{aligned} U &= \{p_0 + \lambda_1(p_1 - p_0) + \cdots + \lambda_k(p_k - p_0) : \lambda_1, \dots, \lambda_k \in \mathbb{R}\} \\ &= \{\lambda_0 p_0 + \lambda_1 p_1 + \cdots + \lambda_k p_k : \lambda_0, \dots, \lambda_k \in \mathbb{R}, \lambda_0 + \cdots + \lambda_k = 1\} \end{aligned}$$

für $k \geq 0, p_0, \dots, p_k \in \mathbb{R}^n$.

(Ä) alle Lösungen einer Menge von "linearen" Gleichungen $Ax = b$ mit $A \in \mathbb{R}^{m \times n}, b \in \mathbb{R}^m$ (Matrix Notation), bzw. (äquivalent) als Schnitt von m Hyperebenen, die jeweils durch eine einzige lineare Gleichung definiert sind.

Proposition 0.3. Die beiden Definitionen (I) und (Ä) sind äquivalent.

Beweis. Beobachtung: Das Umrechnen von innerer Beschreibung auf äußere Beschreibung, und umgekehrt, führt jeweils auf die Lösung eines linearen Gleichungssystems. \square

Naive Regel: Dimension der Lösungsmenge = Anzahl Variablen – Anzahl Gleichungen.

Definition 0.4 (k -dimensionaler affiner Unterraum). Ein *k -dimensionaler affiner Unterraum* ist eine Teilmenge des \mathbb{R}^n :

- (I) alle Affinkombinationen von einem Punkt und einer Menge von k Vektoren, die aber nicht von $k - 1$ Vektoren aufgespannt wird, oder leer (im Fall $k = -1$)
- (A) Lösungsmenge eines Systems von $n - k$ "linearen" Gleichungen, die aber nicht durch weniger Gleichungen zu kriegen ist.

Definition 0.5 (Linearer Unterraum). *Linearer Unterraum:* affiner Unterraum, der o enthält.

0.1.4 Gleichungssysteme, Lösungsraum, Matrix-Darstellung, Gauß-Elimination

Lineares Gleichungssystem in Matrix-Notation.

Elementare Zeilenoperationen: Vertauschen, Multiplikation mit $\alpha \neq 0$, Addition eines Vielfachen zu einer anderen Gleichung.

Proposition 0.6. Jedes Gleichungssystem kann durch elementare Zeilenoperationen in Zeilenstufenform gebracht werden.

0.1.5 Geometrie: Skalarprodukt, Winkel, Abstände, Hesse-Nf.

\mathbb{Q} Körper: Axiome A1–A4, M1–M4, D

\mathbb{R} Körper, und zusätzlich O1, O2, Q

\mathbb{R}^n Vektorraum, A1–A4, S1, S3, D1, D2

— damit kann man Punkte, Geraden, Hyperebenen, affine Unterräume beschreiben, und zwar

(I) innere Beschreibung: Linearkombinationen

(Ä) äußere Beschreibung: lineare Gleichungssysteme

Beispiel “Scherung” $(x, y) \mapsto (x + y, y)$ bildet Geraden auf Geraden ab etc., aber verändert Längen, Winkel etc.

Skalarprodukt \longrightarrow Norm/Abstände \longrightarrow Winkel \longrightarrow Orthogonalität

Definition 0.7 (Skalarprodukt). Für $x, y \in \mathbb{R}^n$ definieren wir $\langle x, y \rangle := x_1y_1 + \cdots + x_ny_n$.

Rechenregeln:

(L) linear in x

(S) symmetrisch

(PD) positiv definit

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

Winkel: $\cos \alpha := \frac{\langle x, y \rangle}{|x||y|}$ (braucht Trigonometrie/Analysis)

Orthogonalität: $x \perp y$ wenn $\langle x, y \rangle = 0$

Polarisierungsgleichung: aus Normen lässt sich Skalarprodukt rekonstruieren

Parallelogrammgleichung

Pythagoras

Hesse-Normalform (nutzt Orthogonalität/Normalenvektor)

Beispiel für Rechnung: Ikosaeder.

1 Grundlagen

1.1 Mengen, Relationen, Abbildungen

1.1.1 Mengen und Teilmengen

Mengen: Elemente – unterscheidbar, Enthaltensein entscheidbar
endliche Menge

Mächtigkeit (Kardinalität) n ; leere Menge

Teilmenge $M' \subset M$

echte Teilmenge $M' \subsetneq M$

Ärger: “Menge aller Mengen” (Russel’sche Antinomie 1903)

Potenzmenge $\mathcal{P}(M)$

1.1.2 Operationen mit Mengen

Vereinigung

Schnitt

Differenz $M \setminus M'$

Rechenregeln: $M \setminus (N_1 \cup N_2) = \text{etc.}$

(direktes) *Produkt*: Menge der geordneten Paare bzw. n -Tupel M^n

1.1.3 Abbildungen

$f : M \rightarrow N, x \mapsto f(x)$

identische Abbildung $\text{id}_M : M \rightarrow M, x \mapsto x$

Bild eines Elements, einer Teilmenge

Einschränkung auf Teilmenge $M' \subset M$

Urbild eines Elements (“Faser”), einer Teilmenge

injektiv

surjektiv

Abbildung $f : M \rightarrow N$, mit Definitionsbereich M und Werten in N

injektiv, surjektiv, *bijektiv*

Bild eines Elements: $f(x)$ für $x \in M$

Bild $f(M)$, sowie $f(M')$ für $M' \subset M$

Urbild eines Elements: $f^{-1}(y) := \{x \in M : f(x) = y\}$

— ist eine Teilmenge!

— kann leer sein!

Urbild $f^{-1}(N')$ für $N' \subset N$

Einschränkung auf Teilmenge: $f|_{M'} : M' \rightarrow N$ für $M' \subset M$

Umkehrabbildung (einer bijektiven Abbildung), auch mit f^{-1} notiert.

Definition 1.1. Eine endliche Menge hat *Kardinalität* n , wenn es bijektive Abbildung auf $[n] := \{1, 2, \dots, n\}$ gibt.

Dirichlet's *Schubfachprinzip*: Für $m < n$ gibt es keine injektive Abbildung $[n] \rightarrow [m]$

Lemma 1.2. Wenn M, N endlich sind und dieselbe Kardinalität haben, dann sind äquivalent

- (i) $f : M \rightarrow N$ injektiv,
- (ii) $f : M \rightarrow N$ surjektiv,
- (iii) $f : M \rightarrow N$ bijektiv.

Komposition (Hintereinanderausführung) von Abbildungen:

$f : M \rightarrow N$ und $g : N \rightarrow L$ so ist $g \circ f : M \rightarrow L$ die Abbildung "g nach f", die durch $(g \circ f)(x) := g(f(x))$ definiert ist.

Hintereinanderausführung ist assoziativ, aber nicht kommutativ (das ist nicht nur falsch, sondern macht keinen Sinn)!

Lemma 1.3. Seien M, N Mengen, $M \neq \emptyset$.

$f : M \rightarrow N$ ist injektiv \iff es gibt $g : N \rightarrow M$ mit $g \circ f = \text{id}_M$.

$f : M \rightarrow N$ ist surjektiv \iff es gibt $g : N \rightarrow M$ mit $f \circ g = \text{id}_N$.

abzählbare Menge M wenn es $f : \mathbb{N} \rightarrow M$ surjektiv gibt.

abzählbar-unendliche Menge M wenn es $f : \mathbb{N} \rightarrow M$ bijektiv gibt (also abzählbar und nicht endlich)

überabzählbare Menge: nicht abzählbar

Satz 1.4 (Cantor 1878). \mathbb{Q} ist abzählbar

Beweis. nach Calkin & Wilf (2000)

□

Satz 1.5. \mathbb{R} ist nicht abzählbar

Beweis. Cantorsches Diagonalverfahren

□

1.2 Gruppen

1.2.1 Verknüpfungen

Verknüpfung: $* : M \times M \rightarrow M$

(A1) heißt *assoziativ* wenn ...

(A2) heißt *kommutativ* wenn ...

(A3) hat ein *neutrales Element* $e \in M$ wenn $e * a = a = a * e$ für alle $a \in M$

(A4) hat ein *neutrales Element und inverse Elemente* wenn es ein neutrales Element e gibt und zu jedem a ein $a' \in M$ gibt mit $a * a' = e = a' * a$.

1.2.2 Gruppen

Definition 1.6 (Gruppe). Eine *Gruppe* ist ein Paar $(G, *)$ bestehend aus einer Menge G und einer Verknüpfung $* : G \times G \rightarrow G$ mit

(A1) assoziativ

(A3) *neutrales Element*

(A4) ... und inverse Elemente

Die Gruppe heißt *kommutativ* oder *abelsch* falls die Verknüpfung (A2) erfüllt, also abelsch ist.

Lemma 1.7.

(i) *Das neutrale Element ist eindeutig*

(ii) *Die inversen Elemente sind eindeutig*

Additive Notation (nur verwenden im kommutativen Fall!):

Verknüpfung $+$, neutrales Element 0 , inverses Element zu a ist $-a$

Multiplikative Notation:

Verknüpfung \cdot , neutrales Element 1 , inverses Element zu a ist a^{-1}

Beispiele:

- $(\mathbb{Z}, +)$
- $(\mathbb{Q}, +)$
- (\mathbb{Q}^+, \cdot)
- $(\mathbb{Q} \setminus \{0\}, \cdot)$
- $(\mathbb{Z}^n, +)$
- $(\mathcal{S}(X), \circ)$ (“symmetrische Gruppe” der bijektiven Abbildungen)

Wiederholung Gruppe. Weitere Beispiel. “Abstrakt”

1.3 Ringe und Körper

Definition 1.8. Ein *Ring* ist ein Tripel $(R, +, \cdot)$ bestehend aus einer Menge R und zwei Verknüpfungen $+ : R \times R \rightarrow R$ (die “Addition”) und $\cdot : R \times R \rightarrow R$ (die “Multiplikation”) mit den folgenden

Rechenregeln:

- A1** Assoziativität der Addition
- A2** Kommutativität der Addition
- A3** Neutrales Element 0 der Addition
- A4** Inverse $-a$ bzgl. Addition
- M1** Assoziativität der Multiplikation
- M2** Kommutativität der Multiplikation
- M3** Neutrales Element 1 der Multiplikation
- D** Distributivgesetz(e)

Der Ring heißt *kommutativ* wenn die Multiplikation kommutativ ist.

Bemerkung: nicht ganz einheitlich normiert. Alle unsere Ringe haben multiplikative Einheit “1”

Beispiele:

- \mathbb{Z}
- Polynomringe in einer und in mehreren Variablen
- Funktionenringe
- \mathbb{Z}/k
- Körper

Definition 1.9. Ein *Körper* ist ein Tripel $(K, +, \cdot)$ bestehend aus einer Menge K und zwei Verknüpfungen $+ : K \times K \rightarrow K$ (die “Addition”) und $\cdot : K \times K \rightarrow K$ (die “Multiplikation”) mit den folgenden **Rechenregeln:**

- A1** Assoziativität der Addition
- A2** Kommutativität der Addition
- A3** Neutrales Element 0 der Addition
- A4** Inverse $-a$ bzgl. Addition
- M1** Assoziativität der Multiplikation
- M2** Kommutativität der Multiplikation
- M3** Neutrales Element 1 der Multiplikation
- M4** Inverse bzgl. Multiplikation
- D** Distributivgesetz(e)

Beispiele:

- \mathbb{Q}
- \mathbb{R}
- Körper $\mathbb{R} = \mathbb{R}(t)$ der rationalen Funktionen
- $\mathbb{Z}/2, \mathbb{Z}/m$

Proposition 1.10. *Der Ring \mathbb{Z}/p ist ein Körper dann und nur dann, wenn p eine Primzahl ist*

Beweis: “nur dann”

Wiederholung Ringe, Körper; insbesondere: keine Nullteiler!

Beweis der Proposition: "dann"

Beispiel endliche Körper:

- Körper in 4 Elementen: Verknüpfungstabellen!

Charakteristik eines Körpers;

Proposition 1.11. *Charakteristik eines endlichen Körpers ist eine Primzahl*

Komplexe Zahlen:

Definition auf $\mathbb{R} \times \mathbb{R}$, Körper-Axiome

Komplexe Zahlen (Fortsetzung)

Realteil $\operatorname{re} z$, Imaginärteil $\operatorname{im} z$

konjugierte Zahl \bar{z} ; Regeln $\overline{\bar{z}} = z$, $\overline{x + y} = \bar{x} + \bar{y}$, $\overline{x \cdot y} = \bar{x} \cdot \bar{y}$,

Norm $|z| := \sqrt{z\bar{z}} = \sqrt{x^2 + y^2}$

Darstellung in der Gauß'schen Zahlenebene;

Norm ist Länge; Addition ist Vektoraddition

Darstellung in Polarkoordinaten als $z = x + iy = r(\cos \varphi + i \sin \varphi)$;

Multiplikation ist Multiplikation der Beträge, Addition der Winkel

1.4 Polynome, Fundamentalsatz der Algebra, Polynomdivision mit Rest

Definition 1.12 (Ring der Polynome). Sei F ein Körper. Der *Ring der Polynome* $F[X]$ ist die Menge der formalen Ausdrücke $f(X) = a_0 + a_1X + \dots + a_n$ ($n \geq 0$, $a_0, a_1, \dots, a_n \in F$). wobei zwei Polynome *gleich* heißen, wenn die Koeffizienten vor jeder Potenz X^i gleich sind.

Addition

Multiplikation

Grad eines Polynoms: das größte i mit $a_i \neq 0$. Definiere $\deg 0 = -\infty$

Polynome und Polynomfunktionen. "Einsetzungshomomorphismus".

Wenn zwei Polynomfunktionen gleich sind, müssen dann die Polynome gleich sein? (Ja, wenn der Körper nicht endlich ist)

Lemma 1.13. $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$ (mit Gleichheit, wenn die Polynome nicht gleichen Grad haben)

$\deg(fg) = \deg(f) + \deg(g)$

Proposition 1.14. *Der Ring der Polynome ist ein Ring, nullteilerfrei, Kürzungsregel*

Proposition 1.15. *Polynomdivision mit Rest, eindeutig*

Korollar 1.16. *Nullstelle eines Polynoms impliziert Linearfaktor*

Korollar 1.17. *Ein Polynom $p \in F[X]$ vom Grad $n \geq 0$ hat höchstens n verschiedene Nullstellen in F .*

Satz 1.18 („Fundamentalsatz der Algebra“). *Jedes komplexe Polynom $p \in \mathbb{C}[X]$ vom Grad $n \geq 1$ hat eine Nullstelle.*

Jedes komplexe Polynom $p \in \mathbb{C}[X]$ vom Grad $n \geq 0$ zerfällt in Linearfaktoren:

$$p(X) = c(X - \lambda_1)^{n_1} \dots (X - \lambda_k)^{n_k}$$

mit $c \in \mathbb{C} \setminus \{0\}$, $k \geq 1$, $\lambda_1, \dots, \lambda_k$ sind die verschiedenen Nullstellen von p und $n_1, \dots, n_k \geq 1$ sind ihre Vielfachheiten, mit $n_1 + \dots + n_k = n$.

Die Darstellung ist eindeutig bis auf Reihenfolge.

Wdh.: Fundamentalsatz der Algebra

Beweis. Wir beweisen nicht die erste Aussage, für die man Analysis/Topologie braucht. (Siehe: BUCH der Beweise [1, Kapitel 19])

Alles weitere folgt. □

Satz 1.19 („reeller Fundamentalsatz der Algebra“). *Jedes reelle Polynom $p \in \mathbb{R}[X]$ vom Grad $n \geq 1$ hat eine Nullstelle, oder einen irreduziblen Teiler vom Grad 2, oder beides.*

Jedes reelle Polynom $p \in \mathbb{R}[X]$ vom Grad $n \geq 0$ zerfällt in lineare und quadratische Faktoren:

$$p(X) = c(X - \lambda_1)^{n_1} \cdots (X - \lambda_k)^{n_k} (X^2 + b_1X + c_1) \cdots (X^2 + b_\ell X + c_\ell)$$

mit $c \in \mathbb{R} \setminus \{0\}$, $k, \ell \geq 0$, $\lambda_1, \dots, \lambda_k \in \mathbb{R}$ sind die verschiedenen reellen Nullstellen von p , die reellen Zahlen $b_1, \dots, b_\ell, c_1, \dots, c_\ell \in \mathbb{R}$ erfüllen $b_i^2 - 4c_i < 0$, und $n_1, \dots, n_k \geq 1$ sind Vielfachheiten mit $n_1 + \dots + n_k + \ell = n$.

Die Darstellung ist eindeutig bis auf Reihenfolge.

Beweis. Induktion über den Grad n , wobei $n = 0, 1$ klar ist. Unter Verwendung der komplexen Version, die hier gleich kommt.

Beachte:

für $\mu_i \in \mathbb{C}$ sind $\mu_i + \bar{\mu}_i = 2\operatorname{Re}(\mu_i)$ und $\mu_i \bar{\mu}_i = |\mu_i|^2$ reell, und insbesondere ist $(X - \mu_i)(X - \bar{\mu}_i)$ ein Polynom mit reellen Koeffizienten! □

(Man versuche, das ohne komplexe Zahlen zu beweisen!?!)

Satz 1.20 („Komplexe Version des reellen Fundamentalsatzes der Algebra“). *Jedes reelle Polynom $p \in \mathbb{R}[X]$ vom Grad $n \geq 0$ zerfällt in Linearfaktoren, wobei die nicht-reellen Nullstellen in Konjugationspaaren auftreten:*

$$p(X) = c(X - \lambda_1) \cdots (X - \lambda_k)(X - \mu_1)(X - \bar{\mu}_1) \cdots (X - \mu_\ell)(X - \bar{\mu}_\ell)$$

mit $c \in \mathbb{R} \setminus \{0\}$, $k, \ell \geq 0$, $\lambda_1, \dots, \lambda_k \in \mathbb{R}$ sind die verschiedenen reellen Nullstellen von p , $\mu_1, \dots, \mu_\ell \in \mathbb{C} \setminus \mathbb{R}$, mit $k + 2\ell = n$.

Die Darstellung ist eindeutig bis auf Reihenfolge.

Beweis. Induktion über den Grad n , wobei $n = 0, 1$ klar ist. Unter Verwendung der Komplexen Version, die jetzt erst kommt.

Wenn p eine reelle Nullstelle λ hat, sind wir fertig nach Induktion.

Wenn p eine echt-komplexe Nullstelle $\lambda \in \mathbb{C} \setminus \mathbb{R}$ hat, so ist auch $\bar{\lambda}$ eine Nullstelle (mit $\lambda \neq \bar{\lambda}$), denn es gilt $p(\bar{\lambda}) = \overline{p(\lambda)}$. Damit ist p teilbar durch

$$(X - \lambda)(X - \bar{\lambda}) = X^2 - (\lambda + \bar{\lambda})X + \lambda\bar{\lambda}$$

und das ist ein reeller Faktor vom Grad 2. □

2 Vektorräume

2.1 Grundlagen

Definition 2.1 (*K*-Vektorraum). Sei *K* ein Körper. Ein *Vektorraum über K* (auch *K*-Vektorraum genannt) ist eine Menge *V* zusammen mit

- einer Verknüpfung $+: V \times V \rightarrow V$, genannt *Addition*, und
- einer Abbildung $\bullet: K \times V \rightarrow V$, genannt *Skalarmultiplikation*

so dass

V1 $(V, +)$ ist eine abelsche Gruppe (mit neutralem Element $\mathbf{0}$, dem *Nullvektor*, und additiven Inversen $-v$ für $v \in V$)

V2 Rechenregeln für Skalarmultiplikation:

$$(S1) \quad (\lambda \cdot \mu) \bullet v = \lambda \bullet (\mu \bullet v)$$

$$(S3) \quad 1 \bullet v = v$$

$$(D) \quad (\lambda + \mu) \bullet v = (\lambda \bullet v) + (\mu \bullet v)$$

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

für alle $v, w \in V, \lambda, \mu \in K$.

Beispiele:

- \mathbb{R}^n ist \mathbb{R} -Vektorraum
- K^n ist K -Vektorraum, $n \geq 0$
- $\{0\}$ ist K -Vektorraum
- K ist K -Vektorraum
- \mathbb{R} ist \mathbb{Q} -Vektorraum
- \mathbb{C} ist \mathbb{R} -Vektorraum
- $\mathbb{R}[X]$ ist \mathbb{R} -Vektorraum
- ...

Wdh. Definition Vektorraum

Rechenregeln:

- $0 \bullet v = \mathbf{0}$
- $\lambda \bullet \mathbf{0} = \mathbf{0}$
- $\lambda \bullet v = \mathbf{0} \Rightarrow v = \mathbf{0}$ oder $\lambda = 0$
- $(-\lambda) \bullet v = \lambda \bullet (-v)$, insbesondere für $\lambda = 1$.

Definition 2.2 (Untervektorraum). nicht-leer, abgeschlossen unter Addition und Skalarmultiplikation

Lemma 2.3. *Jeder Untervektorraum ist ein Vektorraum*

Beispiele:

- Polynome vom Grad höchstens d
- beschränkte, stetige, differenzierbare, polynomiale Funktionen

Definition 2.4 (linear unabhängig). Sei V ein K -Vektorraum. Eine Teilmenge $M \subset V$ ist *linear unabhängig*, wenn alle (endlichen) Linearkombinationen unterschiedliche Ergebnisse geben.

Lemma 2.5. *äquivalent:*

- *linear unabhängig*
- *jede lineare Abhängigkeit ist trivial*
- *kein Vektor lässt sich aus den anderen kombinieren*

Definition 2.6 (Erzeugendensystem). Sei V ein K -Vektorraum. Eine Teilmenge $M \subset V$ ist ein *Erzeugendensystem*, wenn alle Vektoren als (endliche) Linearkombinationen erhalten werden können.

Wdh. Definition Vektorraum V über einem Körper K , Beispiele

Wdh. Definition Untervektorraum

Wdh. Lemma: Jeder Untervektorraum ist ein Vektorraum

Definition 2.7. Eine *Familie* von Vektoren eines Vektorraums: $(v_i)_{i \in I}$: die Vektoren sind

- nicht notwendig unterschiedlich,
- nicht geordnet,
- nicht unbedingt endlich viele.

Der *Spann* einer Familie $v_1, \dots, v_k \in V$ ist $\text{span}(v_1, \dots, v_k) = \dots$

Lemma 2.8. Der Spann $\text{span}(v_1, \dots, v_k)$ einer Folge $v_1, \dots, v_k \in V$ von Vektoren ist ein Untervektorraum. Er ist der kleinste Untervektorraum von V , der alle v_i enthält.

Definition 2.9. Definiere Matrix $A \in K^{m \times n}$ (m Zeilen, n Spalten),

Schreibe K^m für den Vektorraum der Spaltenvektoren der Länge m ,

$(K^n)^*$ für den Vektorraum der Zeilenvektoren der Länge n

Matrixprodukt $Av \in K^m$ für $v \in K^n$.

Also ist Av eine Linearkombination der Spalten von A

Definition 2.10. Sei $A \in K^{m \times n}$ eine Matrix.

- Spaltenraum $\text{SR}(A) := \{Av : v \in K^n\} \subset K^m$: die Menge aller Linearkombinationen von Spalten
- Zeilenraum $\text{ZR}(A) \subset (K^n)^*$: die Menge aller Linearkombinationen von Zeilen von A
- Kern $\ker(A) := \{v \in K^n : Av = 0\}$

Der Kern ist damit die Lösungsmenge eines homogenen linearen Gleichungssystems.

Proposition 2.11. Für jede Matrix $A \in K^{m \times n}$ ist

- der Spaltenraum $\text{SR}(A)$ ein Untervektorraum von K^m ,
- der Zeilenraum $\text{ZR}(A)$ ein Untervektorraum von $(K^n)^*$,
- der Kern $\ker(A)$ ein Untervektorraum von K^n ,

Wdh. $v_1, \dots, v_k \in V$ linear unabhängig (“alle Linearkombinationen unterschiedlich”)

Lemma 2.12. Für $v_1, \dots, v_k \in V$ sind die folgenden Bedingungen äquivalent:

- (i) v_1, \dots, v_k linear unabhängig (“alle Linearkombinationen unterschiedlich”).
- (ii) Jedes $w \in \text{span}(v_1, \dots, v_k)$ eine eindeutige Darstellung $w = \lambda_1 v_1 + \dots + \lambda_k v_k$.
- (iii) Die Abbildung $f : K^k \rightarrow V, \lambda \mapsto \lambda_1 v_1 + \dots + \lambda_k v_k$ ist injektiv.

Lemma 2.13. Für $v_1, \dots, v_k \in V$ sind die folgenden Bedingungen äquivalent:

- (i) v_1, \dots, v_k linear abhängig (“nicht alle Linearkombinationen unterschiedlich”).
- (ii) Es gibt eine nicht-triviale lineare Abhängigkeit $\lambda_1 v_1 + \dots + \lambda_k v_k = 0$ mit $(\lambda_1, \dots, \lambda_k) \neq (0, \dots, 0)$,
- (iii) Mindestens einer der Vektoren lässt sich als Linearkombination der anderen darstellen: es gibt ein i , $1 \leq i \leq k$, und $\mu_1, \dots, \widehat{\mu}_i, \dots, \mu_k \in K$ mit $v_i = \mu_1 v_1 + \dots + \widehat{\mu}_i v_i + \dots + \mu_k v_k$.

Lemma 2.14 (Steinitz’ Austauschlemma). Wenn v_1, \dots, v_k linear unabhängig sind, aber v_1, \dots, v_k, w nicht, mit $w \neq 0$, dann gibt es ein i_0 so dass $v_1, \dots, \widehat{v}_{i_0}, \dots, v_k, w$ linear unabhängig sind.

Die Familien v_1, \dots, v_k und $v_1, \dots, \widehat{v}_{i_0}, \dots, v_k, w$ haben dann denselben Spann.

Genauer: in dieser Situation liegt w im Spann, mit $w = \lambda_1 v_1 + \dots + \lambda_k v_k$.

Nicht alle λ_i sind gleich 0, weil sonst $w = 0$ wäre.

Für i_0 können wir genau diejenigen i nehmen, für die $\lambda_i \neq 0$ ist.

Proposition 2.15 (Steinitz’ Austauschlemma, II). Seien v_1, \dots, v_k und w_1, \dots, w_ℓ linear unabhängig, mit $k \geq \ell$. Dann gibt es $1 \leq i_1 < i_2 < \dots < i_{k-\ell} \leq k$ so dass

$$w_1, \dots, w_\ell, v_{i_1}, \dots, v_{k-\ell}$$

linear unabhängig ist.

Beweis. Die Vektoren w_1, \dots, w_ℓ können nacheinander in dieser Reihenfolge “reingetauscht” werden, jeweils unter Verwendung der “genaueren” Version von Lemma 2.14. □

Definition 2.16. Sei V ein K -Vektorraum. Eine Familie von Vektoren $(v_i)_{i \in I}$ ist ein *Erzeugendensystem* von V , wenn ihr Spann V ist.

Eine Familie von Vektoren $v_1, \dots, v_k \in V$ ist ein *endliches Erzeugendensystem* von V , wenn

$$\text{span}(v_1, \dots, v_k) = V.$$

Ein Vektorraum ist *endlich erzeugt* wenn er ein endliches Erzeugendensystem hat.

Beispiele

- \mathbb{R}^n ist endlich erzeugt
- $\mathbb{R}[x]$ ist nicht endlich erzeugt

2.2 Basis und Dimension

Definition 2.17. Eine *Basis* eines Vektorraums V ist ein linear unabhängiges Erzeugendensystem.

Lemma 2.18. Sei V ein K -Vektorraum, und $v_1, \dots, v_k \in V$. Dann sind äquivalent

- (i) (v_1, \dots, v_k) ist eine *Basis*.
- (ii) (v_1, \dots, v_k) ist *maximal linear unabhängig*.
- (iii) (v_1, \dots, v_k) ist ein *minimales Erzeugendensystem*.
- (iv) Jedes $v \in V$ lässt sich *eindeutig* als $v = \lambda_1 v_1 + \dots + \lambda_k v_k$ mit $\lambda_1, \dots, \lambda_k \in K$ darstellen.
- (v) Die Abbildung $\varphi : K^n \rightarrow V$, $(\lambda_1, \dots, \lambda_k)^T \mapsto \lambda_1 v_1 + \dots + \lambda_k v_k$ ist *bijektiv*.

Beweis. Just do it. □

Proposition 2.19. Wenn ein Vektorraum V eine *endliche Basis* v_1, \dots, v_r hat, dann sind alle Basen *endlich*, und haben *dieselbe Länge* r .

Beweis. Klar aus Proposition 2.15. □

Definition 2.20. Wenn ein Vektorraum eine *endliche Basis* v_1, \dots, v_r hat, dann hat er die *Dimension* r . Wir schreiben dann $\dim V = r$. Insbesondere nennen wir ihn dann *endlich-dimensional*.

Wenn ein Vektorraum keine *endliche Basis* hat, dann heißt er *unendlich-dimensional*. Wir schreiben dann $\dim V = \infty$.

Bemerkung. Das ist wohldefiniert, wegen Proposition 2.19.

Wir sehen auch: wenn V unendlich-dimensional ist, dann gibt es für jedes $n \geq 0$ eine linear unabhängige Familie v_1, \dots, v_n . Diese kann nämlich mit $v_{n+1} \in V \setminus \text{span}(v_1, \dots, v_n)$ konstruiert werden.

Korollar 2.21. Ein Vektorraum ist *genau dann endlich-dimensional*, wenn er *endlich erzeugt* ist. Insbesondere hat jeder endlich-erzeugte Vektorraum eine *Basis*.

Korollar 2.22. In einem endlich-erzeugten Vektorraum enthält jedes Erzeugendensystem eine *Basis*. In einem endlich-erzeugten Vektorraum ist jede *unabhängige Menge* in einer *Basis* enthalten.

Korollar 2.23. Wenn V ein endlich-dimensionaler Vektorraum ist und $U \subset V$ ein Untervektorraum, so gilt $\dim U \leq \dim V$, mit Gleichheit nur für $U = V$.

Beweis. Wir nehmen an, dass $\dim U \geq \dim V$ und betrachten eine *Basis* von U . Diese ist *unabhängig* in V , also eine *Basis* in V . □

2.3 Lineare Abbildungen

Definition 2.24 (lineare Abbildung). Seien V, W Vektorräume über demselben Körper K . Eine Abbildung $F : V \rightarrow W$ ist *linear* wenn

- $F(v + v') = F(v) + F(v')$ für alle $v, v' \in V$,
- $F(\lambda v) = \lambda F(v)$ für alle $v \in V, \lambda \in K$.

Lemma 2.25. Eine Abbildung $F : V \rightarrow W$ zwischen K -Vektorräumen ist genau dann linear, wenn

$$F(\lambda_1 v_1 + \dots + \lambda_k v_k) = \lambda_1 F(v_1) + \dots + \lambda_k F(v_k) \quad \text{für alle } k \geq 0, v_1, \dots, v_k \in V, \lambda_1, \dots, \lambda_k \in K.$$

Beweis. \implies : Vollständige Induktion über k .

\impliedby : Spezialisierung für $k = 2$ bzw. $k = 1$. □

Beispiele:

- $F(v) = 0$
- $\text{id} : V \rightarrow V$
- Drehungen und Spiegelungen in der Ebene \mathbb{R}^2 ; Scherungen
- Projektionen, z.B. $\pi : \mathbb{R}^n \rightarrow \mathbb{R}^{n-1}$ "letzte Koordinate weglassen"
- $F_A : K^n \rightarrow K^m, x \mapsto Ax$ für $A \in K^{m \times n}$
- $F : \mathbb{R}[x] \rightarrow \mathbb{R}[x], p \mapsto p'$
- Auswertungen wie $i : \mathbb{R}[x] \rightarrow \mathbb{R}, p(x) \mapsto p(42)$.

Proposition 2.26. Sei $F : V \rightarrow W$ eine lineare Abbildung.

- (i) $F(0) = 0, F(v - v') = F(v) - F(v')$
- (ii) $F(\lambda_1 v_1 + \dots + \lambda_k v_k) = \lambda_1 F(v_1) + \dots + \lambda_k F(v_k)$
- (iii) Der Kern $\ker(F)$ ist ein Untervektorraum von V .
- (iv) Das Bild $F(V)$ ist ein Untervektorraum von W .
- (v) $F(\text{span}(v_1, \dots, v_k)) = \text{span}(F(v_1), \dots, F(v_k))$
- (vi) Für v_1, \dots, v_k linear abhängig sind auch $F(v_1), \dots, F(v_k)$ linear abhängig.
- (vii) Für $F(v_1), \dots, F(v_k)$ linear unabhängig sind auch v_1, \dots, v_k linear unabhängig.
- (viii) Ist F injektiv und v_1, \dots, v_k linear unabhängig, dann ist auch $F(v_1), \dots, F(v_k)$ linear unabhängig.
- (ix) Für v_1, \dots, v_k Erzeugendensystem von V ist $F(v_1), \dots, F(v_k)$ Erzeugendensystem von $F(V)$.
- (x) $\dim F(V) \leq \dim V$ und $\dim F(V) \leq \dim W$.

Satz 2.27 (Dimensionsformel). Sei $F : V \rightarrow W$ linear, so gilt

$$\dim V = \dim \ker(F) + \dim F(V).$$

Beweis. Wenn $\ker(V)$ oder $F(V)$ unendlich-dimensional ist, dann auch V .

Wenn $\ker(V)$ und $F(V)$ endlich-dimensional sind, wähle Basen v_1, \dots, v_k bzw. w_1, \dots, w_r , sowie $u_1, \dots, u_r \in V$ mit $F(u_i) = w_i$.

Behauptung: $v_1, \dots, v_k, u_1, \dots, u_r$ ist Basis von V . □

2.4 Lineare Abbildungen und Matrizen

Proposition 2.28. Seien V, W Vektorräume über K , mit V endlich-dimensional.

- (i) Sind $v_1, \dots, v_k \in V$ linear unabhängig und $w_1, \dots, w_k \in W$ beliebig, dann gibt es mindestens eine lineare Abbildung $F : V \rightarrow W$ mit $F(v_i) = w_i$ für all i .
 (“ F ist auf linear-unabhängiger Menge beliebig vorschreibbar.”)
- (ii) Ist $v_1, \dots, v_k \in V$ Erzeugendensystem und $w_1, \dots, w_k \in W$ beliebig, dann gibt es höchstens eine lineare Abbildung $F : V \rightarrow W$ mit $F(v_i) = w_i$ für all i .
 (“ F ist durch die Werte auf Erzeugendensystem eindeutig festgelegt.”)
- (iii) Ist $v_1, \dots, v_k \in V$ eine Basis und $w_1, \dots, w_k \in W$ beliebig, dann gibt es genau eine lineare Abbildung $F : V \rightarrow W$ mit $F(v_i) = w_i$ für all i .
 (“ F ist durch die Werte auf Basis eindeutig festlegbar und festgelegt.”)

Definition 2.29 (Darstellende Matrix). Seien V, W Vektorräume über K , seien $\mathcal{B} = (v_1, \dots, v_n)$ und $\mathcal{C} = (w_1, \dots, w_m)$ geordnete (!) Basen von V bzw. von W und sei $F : V \rightarrow W$ linear.

Die darstellende Matrix für F bezüglich der Basen \mathcal{B} und \mathcal{C} ist die Matrix

$$M_{\mathcal{C}, \mathcal{B}}(F) = (a_{ij})_{1 \leq i \leq m, 1 \leq j \leq n} \in K^{m \times n},$$

deren j -te Spalte die Koeffizienten des Bildes des j -ten Basisvektors in V bezüglich der Basis in W enthält, das heißt mit

$$F(v_j) = a_{1j}w_1 + \dots + a_{mj}w_m.$$

Nach Proposition 2.28 hat jede lineare Abbildung zwischen endlich-dimensionalen Vektorräumen genau eine darstellende Matrix — die aber von vorheriger Wahl der Basen abhängt! Die Darstellende Matrix legt auch die lineare Abbildung fest — wenn man die Basen kennt.

Beispiele 2.30. für darstellende Matrizen:

1. eine Projektion $\pi : \mathbb{R}^3 \rightarrow \mathbb{R}^2$
2. eine Drehung $D_\alpha : \mathbb{R}^2 \rightarrow \mathbb{R}^2$

Lemma 2.31. Wenn man eine Abbildung $f : K^n \rightarrow K^m$ bezüglich der Standardbasen darstellt, so steht in der darstellenden Matrix $A = (A_1, \dots, A_n)$ einfach die Bilder der Basisvektoren des K^n .

Die Abbildung ist dann durch das Matrix-Vektor-Produkt $x \mapsto Ax$ gegeben.

Definition 2.32. Sei V ein Vektorraum mit geordneter Basis $\mathcal{B} = (v_1, \dots, v_n)$ und sei $\mathcal{E} = (e_1, \dots, e_n)$ die Standardbasis in K^n . Das zugehörige Koordinatensystem ist die bijektive lineare Abbildung

$$\Phi_{\mathcal{B}} : K^n \rightarrow V, \quad e_i \mapsto v_i \quad (1 \leq i \leq n).$$

Satz 2.33 (Darstellungssatz). Seien V, W Vektorräume über K , sei $\mathcal{B} = (v_1, \dots, v_n)$ eine Basis von V und $\mathcal{C} = (w_1, \dots, w_m)$ eine Basis von W und sei $F : V \rightarrow W$ linear.

Sei $A := M_{\mathcal{C}, \mathcal{B}}(F) \in K^{m \times n}$ die zugehörige darstellende Matrix, und $f_A : K^n \rightarrow K^m$ die lineare Abbildung, die durch $x \mapsto Ax$ gegeben ist.

Dann gilt

$$F = \Phi_{\mathcal{C}} \circ f_A \circ \Phi_{\mathcal{B}}^{-1}.$$

Äquivalent: Das folgende Diagramm aus endlich-dimensionalen Vektorräumen und linearen Abbildungen ist “kommutativ”:

$$\begin{array}{ccc} F : V & \longrightarrow & W \\ \Phi_{\mathcal{B}} \uparrow & & \uparrow \Phi_{\mathcal{C}} \\ K^n & \longrightarrow & K^m. \end{array}$$

Komposition von linearen Abbildungen ist linear: Übungsaufgabe!

Definition 2.34 (Matrixmultiplikation). Sind $A \in K^{m \times n}$ und $B \in K^{n \times r}$ Matrizen über K so dass die Spaltenanzahl von A gleich der Zeilenanzahl von B ist, dann ist $AB \in K^{m \times r}$ definiert durch

$$(a_{i1}b_{1k} + \cdots + a_{in}b_{nk})_{1 \leq i \leq m, 1 \leq k \leq r}.$$

(“(i, k)-Eintrag ergibt sich aus i -te Zeile mal k -te Spalte”)

Satz 2.35 (Darstellende Matrix einer Komposition von linearen Abbildungen). Sind U, V und W K -Vektorräume der Dimension r, m bzw. n , sind $\mathcal{A}, \mathcal{B}, \mathcal{C}$ Basen für U, V, W und sind die Abbildungen $F : V \rightarrow W$ und $G : U \rightarrow V$ linear, so gilt

$$M_{\mathcal{C}, \mathcal{A}}(F \circ G) = M_{\mathcal{C}, \mathcal{B}}(F) \cdot M_{\mathcal{B}, \mathcal{A}}(G).$$

Beweis. Nachrechnen! □

Anders gesagt: Matrizenmultiplikation ist genau so definiert, dass $(AB)x = A(Bx)$, für alle x .

Definition 2.36. Sei $A \in K^{m \times n}$ eine Matrix.

Die Dimension des Spaltenraums $\dim \text{SR}(A)$ heißt der *Spaltenrang* von A .

Die Dimension des Zeilenraums $\dim \text{ZR}(A)$ heißt der *Zeilenrang* von A .

Die Dimension des Bildes der linearen Abbildung $f_A : K^n \rightarrow K^m$, $x \mapsto Ax$ heißt der *Rang* von A .

Bemerkung. “Spaltenrang = Rang” ist klar nach Definition

Definition 2.37 (Elementare Zeilenoperationen). Sei $A \in K^{m \times n}$ eine Matrix. Die folgenden Schritte heißen *elementare Zeilenoperationen*:

- (a) Multiplikation einer Zeile mit einem Faktor $\lambda \in K$, $\lambda \neq 0$
- (b) Addition einer Zeile zu einer anderen.
- (1) Vertauschung von zwei Zeilen.
- (2) Addition eines Vielfachen einer Zeile zu einer anderen Zeile.

Lemma 2.38. *Jede elementare Zeilenoperation kann man mit elementaren Zeilenoperationen rückgängig machen.*

Operationen vom Typ (a) und (b) reichen aus, um auch Operationen vom Typ (1) und (2) zu erhalten.

Beweis. Übung! □

Satz 2.39 (Gauß-Verfahren). *Elementare Zeilenoperationen*

- ändern den Zeilenraum nicht,
- ändern den Kern nicht, und
- ändern die Dimension des Spaltenraums nicht.

Jede Matrix kann mit elementaren Zeilenoperationen in Zeilenstufenform gebracht werden.

Beweis. verwendet Dimensionssatz! □

Korollar 2.40. *Für jede Matrix $A \in K^{m \times n}$ gilt “Zeilenrang = Spaltenrang = Rang”.*

Beweis. verwendet, dass Vektoren mit “Dreiecksmatrixstruktur” linear unabhängig sind. □

Definition 2.41. Lineare Gleichungssysteme, zugehöriges homogenes System, Lösungsraum $\text{Lös}(A, b)$

Satz 2.42. Sei $Ax = b$ ein lineares Gleichungssystem mit $A \in K^{m \times n}$, $b \in K^m$ (also bestehend aus m Gleichungen mit n Variablen) mit $\text{rank } A = r$.

Der Lösungsraum des homogenen Systems $Ax = 0$ ist dann ein Untervektorraum der Dimension $n - \text{rank } A$.

Der Lösungsraum des inhomogenen Systems $Ax = b$ ist entweder leer (das ist genau dann, wenn $\text{rank}(A, b) > \text{rank } A$), oder er ist $\text{Lös}(A, b) = \text{Lös}(A, 0) + x^*$, also ein affiner Unterraum der Dimension $n - \text{rank } A$.

Beweis. Dimensionsformel.

Nehme eine Lösung x^* mit $Ax_0 = b$. Dann gilt $Ax = b \Leftrightarrow A(x - x^*) = 0$ □

Satz 2.43. Bestimme den Lösungsraum für lineare Gleichungssysteme $Ax = b$:

1. Bringe das System in Zeilenstufenform (das verändert den Lösungsraum nicht).
2. Falls $\text{rank}(A, b) > \text{rank } A$ ist $\text{Lös}(A, b) = \emptyset$.
3. Andernfalls finde eine Lösung x_0 (aus Zeilenstufenform: setze alle Nichtpivotvariable auf Null; berechne die Pivotvariablen von rechts nach links, also in der Reihenfolge x_{j_r}, \dots, x_{j_1} .)
4. parametrisiere den Lösungsraum von $\text{Lös}(A, 0)$ (in Zeilenstufenform: in Abhängigkeit von den Nichtpivotvariablen)

2.5 Basiswechsel

Definition 2.44 (Basiswechselmatrix). Sei V Vektorraum über K , seien $\mathcal{B} = (v_1, \dots, v_n)$ und $\mathcal{B}' := (v'_1, \dots, v'_n)$ Basen von V . Die Matrix

$$T_{\mathcal{B}', \mathcal{B}} := M_{\mathcal{B}', \mathcal{B}}(\text{id}) \in K^{n \times n}$$

heißt dann *Basiswechselmatrix*.

Lemma 2.45.

$$T_{\mathcal{B}', \mathcal{B}} = T_{\mathcal{B}, \mathcal{B}'}^{-1}.$$

Dazu Definition der *inversen Matrix* A^{-1} durch $AA^{-1} = A^{-1}A = E_n$ für $A \in K^{n \times n}$ wenn sie existiert.

Beweis. Satz 2.35. □

Satz 2.46 (Transformationsformel). Seien $\mathcal{B}, \mathcal{B}'$ Basen für V und $\mathcal{C}, \mathcal{C}'$ Basen für W und $F : V \rightarrow W$ linear. Dann gilt

$$M_{\mathcal{C}', \mathcal{B}'}(F) = T_{\mathcal{C}', \mathcal{C}} \cdot M_{\mathcal{C}, \mathcal{B}}(F) \cdot T_{\mathcal{B}, \mathcal{B}'}$$

Beweis. Das folgende Diagramm aus endlich-dimensionalen Vektorräumen und linearen Abbildungen ist "kommutativ":

$$\begin{array}{ccccccc}
 & \text{id} & & F & & \text{id} & \\
 V & = & V & \longrightarrow & W & = & W \\
 \Phi_{\mathcal{B}'} \uparrow & & \uparrow \Phi_{\mathcal{B}} & & \Phi_{\mathcal{C}} \uparrow & & \uparrow \Phi_{\mathcal{C}'} \\
 K^n & \longrightarrow & K^n & \longrightarrow & K^m & \longrightarrow & K^m \\
 T_{\mathcal{B}, \mathcal{B}'} & & & M_{\mathcal{C}, \mathcal{B}}(F) & & & T_{\mathcal{C}', \mathcal{C}}
 \end{array}$$

Verwende Satz 2.35. □

Lemma 2.47. Seien $A \in K^{m \times n}$, $B \in K^{n \times r}$ und $C \in K^{r \times s}$. Dann ist $(AB)C = A(BC)$.

Beweis. Beweis 1: Wilde Rechnerei.

Beweis 2: Komposition von Abbildungen ist offenbar assoziativ, also $(f_A \circ f_B) \circ f_C = f_A \circ (f_B \circ f_C)$.

Wir hatten Matrixmultiplikation so *definiert*, dass $f_A \circ f_B = f_{AB}$ usw.

Gleichheit von $f_{(AB)C} = f_{A(BC)}$ impliziert $(AB)C = A(BC)$. □

Lemma 2.48. Wenn V, W endlich-dimensional sind und dieselbe Dimension haben, dann sind äquivalent:

- (i) $f : V \rightarrow W$ injektiv,
- (ii) $f : V \rightarrow W$ surjektiv,
- (iii) $f : V \rightarrow W$ bijektiv.

Beweis. Dimensionssatz! □

Vergleiche Lemma 1.2 — “dasselbe” für endliche Mengen!

Lemma 2.49. Für eine quadratische Matrix $A \in K^{n \times n}$ sind äquivalent:

- (i) $f_A : K^n \rightarrow K^n$ ist invertierbar,
- (ii) A ist invertierbar,
- (iii) A hat “vollen Rang”: $\text{rank } A = n$,
- (iv) A kann durch elementare Zeilenoperationen in die Einheitsmatrix E_n transformiert werden.

Beweis. (i) \Leftrightarrow (ii) aus Eigenschaften der darstellenden Matrix, mit Kompositionssatz 2.35;

(ii) \Leftrightarrow (iii) \Leftrightarrow (iv) aus Zeilenoperationen, die A in Zeilenstufenform bringen. □

Definition 2.50. Elementarmatrizen $S_i(\lambda), Q_{ij}, P_{ij}, Q_{ij}(\lambda)$

Lemma 2.51. Elementare Zeilenoperationen lassen sich durch “Multiplikation von links mit Elementarmatrizen” $S_i(\lambda)$ und Q_{ij} darstellen ($i \neq j, \lambda \neq 0$).

Korollar 2.52. Wenn eine quadratische Matrix $A \in K^{n \times n}$ vollen Rang hat, dann kann sie als Produkt von Elementarmatrizen geschrieben werden ... und A^{-1} auch.

Beweis. Zeige erst, dass die Inversen von Elementarmatrizen auch Elementarmatrizen sind. □

Korollar 2.53. Die inverse Matrix A^{-1} kann (faktoriert oder nicht) berechnet werden, indem man die Matrix $(A|E_n)$ durch Zeilenoperationen in Normalform $(E_n|A^{-1})$ bringt.

Definition 2.54 (Transposition). *Transposition* A^t

Lemma 2.55. Für beliebige “passende” Matrizen $A \in K^{m \times n}$, $B \in K^{n \times r}$ gilt: $(AB)^t = B^t A^t$.
Für beliebige quadratische Matrizen gleicher Größe $A, B \in K^{n \times n}$ gilt: $(A^{-1})^t = (A^t)^{-1}$.

Transposition vertauscht Zeilen und Spalten, also auch Zeilenoperationen mit Spaltenoperationen.

Satz 2.56 (Normalform). Für jede lineare Abbildung $f : V \rightarrow W$ mit $\dim V = n$, $\dim W = m$ gibt es Basen $\mathcal{B} = (v_1, \dots, v_n)$ in V und $\mathcal{C} = (w_1, \dots, w_m)$ in W mit $f(v_i) = w_i$ für $1 \leq i \leq r$ und $f(v_i) = 0$ für $r < i \leq n$, also

$$M_{\mathcal{C}, \mathcal{B}}(f) = \begin{pmatrix} E_r & O \\ O & O \end{pmatrix}$$

Für $A \in K^{m \times n}$ gibt es invertierbare Matrizen $B \in K^{n \times n}$ und $C \in K^{m \times m}$ mit

$$CAB = \begin{pmatrix} E_r & O \\ O & O \end{pmatrix}.$$

Beweis. Erste Aussage: siehe Beweis des Dimensionssatzes!

Zweite Aussage: “invertierbare Matrix von rechts” = “elementare Spaltenoperationen” □

Definition 2.57 (Allgemeine lineare Gruppe). Die *allgemeine lineare Gruppe* (der Ordnung n über dem Körper K) ist

$$GL(n, K) = \{A \in K^{n \times n} : A \text{ invertierbar}\}$$

mit der Matrizenmultiplikation als Verknüpfung.

Lemma 2.58. Die allgemeine lineare Gruppe ist eine Gruppe. Für $n \geq 2$ ist sie nicht kommutativ:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}.$$

3 Determinanten

Satz 3.1 (Existenz und Eindeutigkeit der Determinantenfunktion). *Es gibt eine Funktion*

$$\det : K^{n \times n} \longrightarrow K$$

mit den folgenden Eigenschaften:

- (i) $\det A \neq 0$ genau dann, wenn A nicht invertierbar ist
- (ii) $\det(AB) = \det A \det B$
- (iii) $\det A$ ist ein Polynom in den Einträgen a_{ij} der Matrix A
- (iv) $\det A$ ist linear in den Zeilen von A
- (v) $\det A = 0$ wenn A eine Nullzeile hat
- (vi) $\det A = 0$ wenn zwei Zeilen von A gleich sind
- (vii) $\det A = 0$ wenn die Zeilen von A linear abhängig sind
- (viii) $\det A' = -\det A$ wenn A' aus A durch Vertauschung von zwei Zeilen entsteht
- (ix) $\det E_n = 1$
- (x) $\det A^t = \det A$ — also gelten (iv)–(x) auch für “Spalten” statt “Zeilen”
- (xi) *Leibniz-Formel:* $\det A = \sum_{\sigma} \operatorname{sgn}(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \dots a_{n\sigma(n)}$

Die Determinantenfunktion ist durch (iv)+(vi)+(ix) schon eindeutig festgelegt.

Satz 3.2 (Existenz und Eindeutigkeit der Determinantenfunktion). *Es gibt eine Funktion*

$$\det : K^{n \times n} \longrightarrow K$$

mit den folgenden Eigenschaften:

- (i) $\det A \neq 0$ genau dann, wenn A nicht invertierbar ist
- (ii) $\det(AB) = \det A \det B$
- (iii) $\det A$ ist ein Polynom in den Einträgen a_{ij} der Matrix A
- (iv) **[Axiom D1]** $\det A$ ist linear in den Zeilen von A
- (v) $\det A = 0$ wenn A eine Nullzeile hat
- (vi) **[Axiom D2]** $\det A = 0$ wenn zwei Zeilen von A gleich sind
- (vii) $\det A = 0$ wenn die Zeilen von A linear abhängig sind
- (viii) $\det A' = -\det A$ wenn A' aus A durch Vertauschung von zwei Zeilen entsteht
- (ix) **[Axiom D3]** $\det E_n = 1$
- (x) $\det A' = \det A$ wenn A' durch Addition des eines Vielfachen einer Zeile zu einer anderen entsteht.
- (xi) $\det A^t = \det A$ — also gelten (ii)–(v) auch für “Spalten” statt “Zeilen”
- (xii) **Leibniz-Formel:** $\det A = \sum_{\sigma} \operatorname{sgn}(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)}$
- (xiii) **Laplace-Entwicklung**
- (xiv) **Determinante einer oberen Blockmatrix**
- (xv) $\det(B^{-1}AB) = \det A$
— daraus folgt, dass die Determinante eines Endomorphismus $f : V \rightarrow V$ wohldefiniert ist, also nicht von der Basis abhängt.

Die Determinantenfunktion ist durch (iv)+(vi)+(ix) schon eindeutig festgelegt.

Beweis. Wir nehmen (iv)=(D1), (vi)=(D2), (ix)=(D3) als Axiome.

Aus (D1) folgt (v): Nullzeile gleich null mal Nullzeile.

Aus (D1) folgt (iii): $\det A$ ist ein homogenes Polynom vom Grad n in den n^2 Variablen a_{ij} .

Aus (D1) und (D2) folgt (x) — elementare Zeilenoperationen vom Typ (2) verändern die Determinante nicht.

Aus (D1), (D2) und (x) folgt (viii) — elementare Zeilenoperationen vom Typ (1) verändern das Vorzeichen.

Aus (D1), (viii) und (x) sehen wir, dass sich unter elementaren Zeilenoperationen nicht ändert, ob die Determinante gleich 0 ist. Wir können damit aber die Matrix entweder auf die Einheitsmatrix bringen, dann ist die Determinante nicht 0 nach (D3), oder wir erhalten eine Nullzeile, dann ist die Determinante 0 nach (v). Damit ist (i) gezeigt, aber auch (vii).

Um (ii) zu zeigen: A hat entweder vollen Rang, dann faktorisieren wir in Elementarmatrizen, und sehen, dass (ii) für Elementarmatrizen A gilt. Oder A hat nicht vollen Rang, dann auch AB nicht, also $\det A = \det AB = 0$ nach (i). Also gilt (ii).

Damit sind (i)-(x) gezeigt. Wir sehen aus dem Beweis für (iii), dass

$$\det A = \sum_{\sigma: \{1, \dots, n\} \rightarrow \{1, \dots, n\}} \det \begin{pmatrix} - & e_{\sigma(1)}^t & - \\ - & e_{\sigma(2)}^t & - \\ & \vdots & \\ - & e_{\sigma(n)}^t & - \end{pmatrix} a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)}.$$

Dabei geht die Summe über alle n^n Abbildungen σ , aber wenn die Abbildung nicht injektiv ist, dann wird die Determinante gleich 0 nach (D2). Also brauchen wir nur die σ betrachten, die injektiv sind, und diese sind bijektiv nach Lemma 1.2. Also summieren wir nur über alle $n!$ Permutationen σ . Die Determinante

der Matrix, die zu σ gehört, heißt das *Signum* der Permutation, und kann auf verschiedenste Weisen interpretiert werden:

$$\operatorname{sgn} \sigma = \det P_\sigma := \det \begin{pmatrix} -e_{\sigma(1)}^t & - \\ -e_{\sigma(2)}^t & - \\ \vdots & \\ -e_{\sigma(n)}^t & - \end{pmatrix} = (-1)^{\operatorname{inv}(\sigma)} = (-1)^{\operatorname{cross}(\sigma)},$$

wobei $\operatorname{inv}(\sigma)$ die Anzahl der *Fehlstände* von σ bezeichnet, also die Anzahl der Paare $i < j$ mit $\sigma(i) > \sigma(j)$, und $\operatorname{cross}(\sigma)$ die Anzahl der *Kreuzungen* in einem beliebigen Zopfdiagramm für σ .

Daran sehen wir die Gültigkeit der Leibniz-Formel (xii), und damit die Eindeutigkeit von \det

Andererseits überprüft man leicht, dass die durch die Leibniz-Formel (xii) definierte Funktion die Axiome (D1)–(D3) erfüllt. Damit haben wir die Existenz der Determinante.

Schließlich ist $(P_\sigma)^t$ die Matrix, die der inversen Permutation σ^{-1} entspricht. Und es gilt $(-1)^{\operatorname{inv}(\sigma)} = (-1)^{\operatorname{inv}\sigma^{-1}}$. Daraus folgt (xi).

Und so weiter. □

Literatur

- [1] Martin Aigner and Günter M. Ziegler. *Das BUCH der Beweise*. Springer-Verlag, Heidelberg Berlin, third edition, 2009.