

Geometrie I
Mitschrift der Vorlesung von Prof. Leißner im
Wintersemester 2002/03

Lars Hoegen

[homer.simpson@atomkraftwerk-springfield.de]

Version: 2,7

Letzte Änderung: 8. März 2003

Vorwort

Nachstehend findet sich eine Mitschrift, die auf Notizen aus der im Titel genannten Vorlesung basieren. Sie endet mit dem Datum 22.01.2003, dem Tag der Klausur und enthält alle bis dahin in der Vorlesung behandelten Abschnitte einschließlich Übungsaufgaben und Lösungen. Dabei orientierte ich mich am Tafelbild von Prof. Leißner und habe nur an wenigen Stellen ergänzt.

Dies ist eine *Mitschrift*, d.h. sie erhebt Anspruch auf Unvollständigkeit und Rechtschreibfehler sind Absicht.

Dieser Text ist auf jeden Fall verbesserungswürdig. Leider entwickelt man solchen Projekten eine gewisse Betriebsblindheit. Ich möchte Dich daher bitten, dieses Schriftstück in allen Aspekten (Inhalt, Layout, Ergänzungen, Streichungen etc.) zu kritisieren, am besten per Mail an

homer.simpson@atomkraftwerk-springfield.de

Danksagung

Mein Dank gilt Olga Scheid, Svenja Grundey, Beate Große Kracht, Robert Meyer, Christian Pankratius, Benjamin Rott und Patrick Henkel.

Ohne sie wäre diese Mitschrift nur unvollständig, da ich einige Male nicht an den Vorlesungen und Übungen wegen Parallelveranstaltungen oder Krankheit teilnehmen konnte. Sie haben mir dankenswerter Weise ihre Notizen zur Verfügung gestellt.

Korrekturen

Diese Dokument wird inhaltlich nicht mehr erweitert, daher versehe ich es mit einer Versionsnummer, die mit jeder Korrektur weiter gegen der Wert der Eulerschen Zahl konvergiert.

Alle Änderungen werden in einem entsprechenden Verzeichnis im Anhang protokolliert.

Abweichungen zur Vorlesung

Aus Gründen der Arbeitsergonomie binde ich mich in der Untergliederung der Abschnitte und Unterpunkte an die Vorgaben von $\text{\LaTeX} 2_{\epsilon}$. Dabei übernehme ich in den Überschriften der Abschnitte die von Prof. Leißner verwendeten Abkürzungen:

- (a) (D) steht für Definition,
- (b) (S) steht für Satz,
- (c) (M) soll eine Motivation für den kommenden Stoff sein,
- (d) (B) bezeichnet ein Beispiel und

(e) (A) kennzeichnet eine Aufgabe.

Prof. Leißner verwendet für Unterpunkte erster Ordnung kleine griechische Buchstaben α, β, γ etc. Ich ersetze diese durch kleine lateinische Buchstaben, da L^AT_EX 2_ε die griechische Indizierung nur sehr bedingt unterstützt¹. Ab zweiter Ordnung verwendet er arabische Zahlen, dort gehe ich mit ihm konform.

¹Auch wäre dabei die Kompatibilität zu PostScript-Schriften nicht vollständig sichergestellt, was zu Problemen im Druckbild führen würde.

Inhaltsverzeichnis

0	Algebraische Strukturen	7
1	Affine Euklidische Geometrie	49
2	Inzidenz- und affine Räume	85

Kapitel 0

Algebraische Strukturen

0.1 (D) Standardbezeichnungen für häufig vorkommende Mengen

$\{1, 2, 3, \dots\} =: \mathbb{N}$	Menge der natürlichen Zahlen
$\{0, 1, 2, \dots\} =: \mathbb{N}_0$	Menge der nicht-negativen ganzen Zahlen
$\{\dots, -2, -1, 0, 1, 2, \dots\} =: \mathbb{Z}$	Menge der ganzen Zahlen
$\{\frac{a}{b} \mid a, b \in \mathbb{Z} \text{ und } b \neq 0\} =: \mathbb{Q}$	Menge der rationalen Zahlen
$\{\alpha \mid \alpha \text{ ist reelle Zahl}\} =: \mathbb{R}$	Menge der reellen Zahlen
$\{\alpha + i\beta \mid \alpha, \beta \in \mathbb{R}, i^2 = -1\} =: \mathbb{C}$	Menge der komplexen Zahlen

Sind A, B beliebig vorgegebene Mengen, so wird das *kartesische Produkt* gesetzt als $\{(a, b) \mid a \in A \wedge b \in B\} =: A \times B$.

0.2 (D) Abbildung von A nach B

Sind A, B Mengen, so wird $\{\varphi \mid \varphi \text{ ist Abbildung von } A \text{ nach } B\} =: \text{Abb}(A, B)$ die *Abbildung von A nach B* genannt.

Eine *Bijektion von A nach B* setzt man als $\{\varphi \in \text{Abb}(A, B) \mid \varphi \text{ ist Bijektion}\} =: \text{Bij}(A, B)$.

Im Fall $A = B$ wird auch $\text{Abb}(A, B) =: \text{Abb}(A)$ und $\text{Bij}(A, B) =: \text{Bij}(A) =: \text{Sym}(A)$ gesetzt, wobei $\text{Sym}(A)$ die Menge aller Symmetrien bezeichnet.

0.3 (D)

Sind A, B, C Mengen und $\varphi \in \text{Abb}(A, B)$, $\psi \in \text{Abb}(B, C)$, so stellt die Hintereinanderausführung der Abbildungen – „erst φ , dann ψ “ – eine Abbildung von A nach C dar, die bei der *Funktionsschreibweise* in der Form

$$\gamma : \begin{cases} A \rightarrow C \\ a \mapsto \gamma(a) = \psi(\varphi(a)) =: \psi\varphi(a) \end{cases}$$

geschrieben wird, also $\gamma = \psi\varphi$. Die *Exponentialschreibweise*¹ verwendet die Form

$$\gamma : \begin{cases} A \rightarrow C \\ a \mapsto a^\gamma = (a\varphi)\psi =: a^{\varphi \cdot \psi} \end{cases}$$

also $\gamma = \varphi\psi$. Es gibt auch die *duale Schreibweise* in der Form

$$\gamma : \begin{cases} A \rightarrow C \\ a \mapsto a\gamma = (a\varphi)\psi =: a(\varphi\psi) \end{cases}$$

also $\gamma = \varphi\psi$.

0.4 (D)

- (a) Ist $G = \{a, b, \dots\}$ eine Menge und $a : \begin{cases} G \times G \rightarrow G \\ (a, b) \mapsto a \circ b \end{cases}$ eine Abbildung von $G \times G \rightarrow G$, so heißt das Paar (G, \circ) ein *Gruppoid*.
- (b) Eine Teilmenge $U \subset G$ eines Gruppoids (G, \circ) heißt genau dann *Untergruppoid von* (G, \circ) , wenn $\{u_1 \circ u_2 \mid (u_1, u_2) \in U \times U\} =: U \circ U \subset U$ bzw. auch genau dann, wenn (U, \circ) ebenfalls Gruppoid ist.
- (c) Zwei Gruppoiden $(G, \circ); (H, *)$ heißen *gleich* – in Zeichen $(G, \circ) = (H, *)$ – wenn gilt: Es ist $G = H$ und $g \circ h = g * h$ für alle $(g, h) \in G \times G$.

0.5 (B)

- (a) $(\mathbb{N}, +) =: (G, \circ)$ ist ein Gruppoid.
- (b) $(\mathbb{N}, \cdot) =: (H, *)$ ist ein Gruppoid.
- (c) $(G, \circ) \neq (H, *)$, denn:
Es ist zwar $G = \mathbb{N} = H$, aber z.B. $\left. \begin{matrix} 3 \circ 4 = 3 + 4 = 7 \\ 3 * 4 = 3 \cdot 4 = 12 \end{matrix} \right\} \rightsquigarrow 3 \circ 4 \neq 3 * 4$, also $(G, \circ) \neq (H, *)$.
- (d) Für $\{1, 3, 5, \dots\} =: U \subset \mathbb{N}$ gilt:
- (1) U ist ein Untergruppoid von (\mathbb{N}, \cdot) , denn $U \cdot U \subset U$.
 - (2) U ist kein Untergruppoid von $(\mathbb{N}, +)$, da z.B. $(3, 5) \in U \times U$, aber $3 + 5 \notin U$.

0.6 (D)

Ist (G, \circ) ein Gruppoid und $\begin{Bmatrix} n_\lambda \\ n_\rho \\ n \end{Bmatrix} \in G$, so heißt $\begin{Bmatrix} n_\lambda \text{ ein } \textit{linkseitig} \\ n_\rho \text{ ein } \textit{rechtsseitig} \\ n \text{ ein } [\textit{zweiseitig}] \end{Bmatrix}$ *neutrales Element* von (G, \circ) , wenn für alle $a \in G$ gilt $\begin{Bmatrix} n_\lambda \circ a = a \\ a \circ n_\rho = a \\ n \circ a = a = a \circ n \end{Bmatrix}$.

¹Prof. Leißner bevorzugt diese Darstellungsweise.

0.7 (A)

Man bestimme für jedes der vier Gruppoide

(a) $(\mathbb{N}, +)$

(b) (\mathbb{N}, \cdot)

(c) $(\mathbb{N}, \text{hoch})$ mit $\text{hoch} : \begin{cases} \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N} \\ (a, b) \mapsto a \text{ hoch } b := a^b \end{cases}$

(d) $(\mathbb{N}, \text{vergiss})$ mit $\text{vergiss} : \begin{cases} \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N} \\ (a, b) \mapsto a \text{ vergiss } b := a \end{cases}$

jeweils die Mengen aller linksseitig, rechtsseitig und zweiseitig neutralen Elemente.

Lösung

Sei (G, \circ) ein Gruppoid. Ich setze

$$\begin{aligned} \{n_\lambda \in G \mid n_\lambda \text{ ist ein linksseitig neutrales Element von } (G, \circ)\} &=: N_\lambda \\ \{n_\rho \in G \mid n_\rho \text{ ist ein rechtsseitig neutrales Element von } (G, \circ)\} &=: N_\rho \\ \{n \in G \mid n \text{ ist ein [zweiseitig] neutrales Element von } (G, \circ)\} &=: N \end{aligned}$$

Daraus folgt $N_\lambda \cap N_\rho = N$.

(a) Sei $n \in \mathbb{N}$ beliebig vorgegeben. Angenommen $n \in N_\rho$ oder $n \in N_\lambda$ oder $n \in N$, dann muß gelten $n+n = n$. Da in \mathbb{N} aber $n+n \neq n$, folgt $N_\lambda = \{\} = N_\rho = N$.

(b) Sei $n \in \mathbb{N}$ beliebig vorgegeben.

- Angenommen $n \in N_\lambda$. Ich suche in \mathbb{N} nach Elementen x , die die Gleichung $n = n \cdot x$ erfüllen. Dies gilt nur für $n = n \cdot 1 = 1$
- Damit ist $N_\lambda \subset \{1\}$, d.h. höchstens 1 ist linksseitig neutrales Element.
- Umgekehrt gilt für alle $a \in \mathbb{N} : 1 \cdot a = a \rightsquigarrow 1 \in N_\lambda \rightsquigarrow N_\lambda = \{1\}$.
- Analog zeigt man $N_\rho = \{1\}$.

Nach der Voraussetzung folgt $N = \{1\}$.

- (c)
- Sei $n_\lambda \in N_\lambda$ beliebig vorgegeben.
 - Dann gilt nach Definition $n_\lambda = n_\lambda^1 = 1$, da n_λ linksseitig neutrales Element. Damit ergibt sich $N_\lambda \subset \{1\}$.
 - Weiter ist $1^2 = 1 \cdot 1 \neq 2 \rightsquigarrow 1 \notin N_\lambda \rightsquigarrow N_\lambda = \{\}$. Damit hat man alle linksseitig neutralen Elemente.
 - Für die (zweiseitig) neutralen Elemente gilt somit $N = N_\lambda \cap N_\rho = \{\} \cap N_\rho = \{\}$.
 - Sei nun $n_\rho \in N_\rho$ beliebig vorgegeben.
 - Da $2^{n_\rho} = 2$ gelten soll, ergibt sich durch scharfes Hinschauen $n_\rho = 1 \rightsquigarrow N_\rho \subset \{1\}$.
 - Umgekehrt gilt für alle $a \in \mathbb{N} : a^1 = a \rightsquigarrow 1 \in N_\rho$. Somit ist die Menge der rechtsseitig neutralen Elemente bestimmt durch $N_\rho = \{1\}$.
- (d)
- Sei $n_\lambda \in N_\lambda$ beliebig vorgegeben.
 - Suche auch hier nach Elementen x , für die $n \text{ vergiss } x = n$ erfüllt ist.

- Man sieht leicht, daß $n_\lambda = n_\lambda$ vergiß $(n_\lambda + 1) = n_\lambda + 1$, da n_λ linksseitig neutrales Element ist.
- Dies ist ein Widerspruch, daher ist $N_\lambda = \{\}$ und weiter wie oben gezeigt $N = N_\lambda \cap N_\rho = \{\}$.
- Sei $n \in \mathbb{N}$ beliebig vorgegeben.
- Es gilt für alle $a \in \mathbb{N}$, daß a vergiß $n = a$, daher folgt $n \in N_\rho$, d.h. die Menge aller rechtsseitig neutralen Elemente ist gleich den natürlichen Zahlen: $N_\rho = \mathbb{N}$.

0.8 (S+D)

Ein Gruppoid (G, \circ) besitzt höchstens ein [zweiseitig] neutrales Element.

Besitzt ein Gruppoid (G, \circ) ein [zweiseitig] neutrales Element n , so heißt (G, \circ) ein *Gruppoid mit neutralem Element* und n heißt *das* neutrale Element von (G, \circ) .

Beweis Angenommen, n und n' sind neutrale Elemente von (G, \circ) . Nach (0.6) gilt:

$$\begin{aligned}\forall a \in G : n \circ a &= a = a \circ n \\ \forall a \in G : n' \circ a &= a = a \circ n'\end{aligned}$$

und es folgt, da $n \in G$

$$n = n' \circ n = n' = n \circ n'$$

also $n = n'$.

0.9 (A)

Es sei (G, \circ) ein Gruppoid mit neutralem Element n .

Beweise oder widerlege: Ist U ein Untergruppoid von (G, \circ) und besitzt (U, \circ) ebenfalls ein neutrales Element n' so gilt $n = n'$.

Lösung

Man findet ein Gegenbeispiel, welches die Behauptung widerlegt, wenn man $G = \mathbb{N}_0 \times \mathbb{N}_0$ mit der Verknüpfung

$$\circ \begin{cases} G \circ G \rightarrow G \\ (a, b), (c, d) \mapsto (a, b) \circ (c, d) := (ac, bd) \end{cases}$$

betrachtet. $(1, 1)$ ist neutrales Element von (G, \circ) . Betrachte

$$\begin{aligned}\mathbb{N}_0 \times \{0\} &= \{(a, 0) \mid a \in \mathbb{N}_0\} =: U \subset G \\ (a, 0) \circ (b, 0) &= (a \cdot b, 0 \cdot 0) \in U \quad \forall (a, 0), (b, 0) \in U\end{aligned}$$

Damit ist (U, \circ) Untergruppoid von (G, \circ) und $(1, 0)$ ist neutrales Element von (U, \circ) , aber $(1, 0) \neq (1, 1)$ stellt einen Widerspruch zur Aussage dar (es ist $(1, 1) \notin U$).

0.10 (A)

Es sei (G, \circ) ein Gruppoid. Beweise oder widerlege die folgenden Behauptungen:

- Besitzt (G, \circ) ein [zweiseitig] neutrales Element n , so ist dies auch das einzige linksseitig neutrale Element von (G, \circ) .
- Besitzt (G, \circ) wenigstens ein linksseitig neutrales Element n_λ und wenigstens ein rechtsseitig neutrales Element n_ρ , so ist (G, \circ) ein Gruppoid mit neutralem Element.
- Besitzt (G, \circ) genau ein rechtsseitig neutrales Element n_ρ , so ist (G, \circ) ein Gruppoid mit neutralem Element.
- Besitzt (G, \circ) mindestens zwei linksseitig neutrale Elemente n_λ, n'_λ mit $n_\lambda \neq n'_\lambda$, so ist (G, \circ) kein Gruppoid mit neutralem Element.

Lösung

- Beweis:* Sei $n_\lambda \in N_\lambda$ beliebig vorgegeben. Da n zweiseitig neutrales und n_λ linksseitig neutrales Element ist, gilt $n_\lambda = n_\lambda \circ n = n$ und weiter $N_\lambda \subset \{n\}$. Damit ergibt sich $N_\lambda = N$; analog verfährt man für $n_\rho \in N_\rho$.
- Beweis:* Angenommen $N_\lambda \neq \{\}$ und $N_\rho \neq \{\}$. Wähle ein $n_\lambda \in N_\lambda$ und ein $n_\rho \in N_\rho$, dann gilt nach Definition $n_\lambda = n_\lambda \circ n_\rho = n_\rho \rightsquigarrow N_\lambda = N_\rho = N$.
- Widerspruch:* Ein Gegenbeispiel zur Aussage findet sich in (0.7(c)), denn in $(\mathbb{N}, \text{hoch})$ gilt $N_\rho = \{1\}$ und $N_\lambda = \{\}$; dieses Gruppoid erfüllt die Voraussetzung der Aussage. Nun hat aber, wie oben gezeigt, das Gruppoid überhaupt kein (zweiseitig) neutrales Element.
- Man findet zwei Belege:* Im Fall $N_\lambda \neq \{\} \neq N_\rho$ gilt allgemein für ein Gruppoid $N_\lambda = \{n\} = N_\rho$.
Ist die Mächtigkeit der Menge der linksseitig neutralen Elemente größer Eins, also $|N_\lambda| > 1$, so gilt wegen obiger Feststellung $N_\lambda = \{\} = N_\rho$.
Gilt $|N_\rho| > 1$, so folgt aus obiger Feststellung $N_\lambda = \{\} = N_\rho$.
Dies belegt die Aussage.

0.11 (M)

$(\mathbb{Z}, -)$ ist ein Gruppoid, denn $\begin{cases} \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z} \\ (a, b) \mapsto a - b \end{cases}$ ist eindeutig definierte Abbildung von $\mathbb{Z} \times \mathbb{Z}$ nach \mathbb{Z} . Es ist z.B.

$$\begin{aligned} (2, 3) &\mapsto 2 - 3 = -1 \in \mathbb{Z} \\ (3, 4) &\mapsto 3 - 4 = -1 \in \mathbb{Z} \end{aligned}$$

eindeutig definiert.

Problem: Ist $(2, 3, 4) \mapsto 2 - 3 - 4 \in \mathbb{Z}$ definiert? Die Definition ist nur dann eindeutig, wenn man den Ausdruck $2 - 3 - 4$ eindeutig beklammert:

- Möglichkeit: $(2 - 3) - 4 = -1 - 4 = -5 \in \mathbb{Z}$
- Möglichkeit: $2 - (3 - 4) = 2 - (-1) = 3 \in \mathbb{Z}$

Resultat: Ist (G, \circ) ein Gruppoid, so ist für alle $a, b, c \in G$ zwar $a \circ b =: n \in G$ und $b \circ c =: v \in G$ definiert, aber $a \circ b \circ c$ ist nur dann definiert, wenn man den Ausdruck eindeutig beklammert. Es gibt genau zwei Möglichkeiten der Beklammerung:

- Möglichkeit: $(a \circ b) \circ c = n \circ c \in G$
- Möglichkeit: $a \circ (b \circ c) = a \circ v \in G$

0.12 (D)

Ein Gruppoid (G, \circ) heißt dann und nur dann *assoziativ* oder *Halbgruppe* (Semigruppe), wenn das *Assoziativgesetz* [Ass] : $(a \circ b) \circ c = a \circ (b \circ c)$ für alle $a, b, c \in G$ gilt.

0.13 (B)

- (a) $(\mathbb{N}, \text{hoch})$ ist keine Halbgruppe, denn es ist z.B.

$$\begin{aligned} (2 \text{ hoch } 3) \text{ hoch } 4 &= (2^3)^4 = 2^{12} = 2^2 \cdot 2^{10} = 4 \cdot 1024 = 4096 \\ 2 \text{ hoch } (3 \text{ hoch } 4) &= 2^{(3^4)} = 2^{81} = 2 \cdot (2^{10})^8 = 2 \cdot (1024)^8 > 2 \cdot 10^{24} \end{aligned}$$

- (b) $(\mathbb{N}, \text{vergiss})$ ist Halbgruppe, denn: Sei $a, b, c \in \mathbb{N}$ beliebig vorgegeben, dann ist

$$\begin{aligned} (a \text{ vergiss } b) \text{ vergiss } c &= a \text{ vergiss } c = a \\ a \text{ vergiss } (b \text{ vergiss } c) &= a \text{ vergiss } c = a \end{aligned}$$

- (c) Bei Halbgruppen ist auch $a \circ b \circ c \circ d$ unabhängig von der zur Berechnung notwendigen Beklammerung. Es sind die folgenden fünf Beklammerungen möglich:

$$\begin{aligned} ((a \circ b) \circ c) \circ d &=: a_1 \in G \\ (a \circ b) \circ (c \circ d) &=: a_2 \in G \\ (a \circ (b \circ c)) \circ d &=: a_3 \in G \\ a \circ ((b \circ c) \circ d) &=: a_4 \in G \\ a \circ (b \circ (c \circ d)) &=: a_5 \in G \end{aligned}$$

Wir zeigen $a_i = a_1$ für $i = 2, 3, 4, 5$:

- Setzte $a \circ b =: u \in G$.
- $a_2 = u \circ (c \circ d) \stackrel{[\text{Ass}]}{=} (u \circ c) \circ d = ((a \circ b) \circ c) \circ d = a_1$
- $a_3 = (a \circ (b \circ c)) \circ d \stackrel{[\text{Ass}]}{=} ((a \circ b) \circ c) \circ d = a_1$
- a_4 und a_5 analog.

0.14 Kam in der Vorlesung nicht vor.

0.15 (A)

Es seien (G, \circ) ein Gruppoid, $n \in \mathbb{N}$ und $a_1, a_2, \dots, a_n \in G$. Zeige:

- (a) Setzt man $A_1 = A_2 := 1$ und A_n für $n \geq 3$ als die Anzahl der möglichen verschiedenen eindeutigen Beklammerungen von $a_1 \circ a_2 \circ \dots \circ a_n$, so gilt

$$A_n = \sum_{i=1}^{n-1} A_{n-i} \cdot A_i$$

- (b) Ergänze die Tabelle
- | | | | | | | | | | | |
|-------|---|---|---|---|---|---|---|---|---|----|
| n | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| A_i | 1 | 1 | 2 | 5 | | | | | | |

Lösung

- (a) Beim Beweis von (0.16) wurde gezeigt: Eine beliebig vorgegebene Beklammerung von $a_1 \circ a_2 \circ \dots \circ a_n$ gehört zu einer der drei Typen

- (I) $a_1 \circ [a_2 \circ \dots \circ a_n]$,
 (II) $[a_1 \circ a_2 \circ \dots \circ a_{n-1}] \circ a_n$ oder
 (III) $[a_1 \circ a_2 \circ \dots \circ a_i] \circ [a_{i+1} \circ \dots \circ a_n]$

mit $2 < i < n$.

Nun kann man beim Typ (I) noch das Element a_1 mit Klammern versehen, beim Typ (II) ebenso das Element a_n .

Beim Typ (III) kann man die Schlußklammer des ersten Klammersausdrucks genau A_i mal verschieben, die Beginnklammer des zweiten Klammersausdrucks genau A_{n-i} mal verschieben. Damit sind beim Typ (III) $A_i \cdot A_{n-i}$ verschiedene Beklammerungen möglich:

$$A_n = A_1 \cdot A_{n-1} + A_2 \cdot A_{n-2} + \dots + A_{n-1} A_1 = \sum_{i=1}^{n-1} A_{n-i} \cdot A_i$$

- (b) Beispiel für den Fall $n = 8$:

$$A_1 A_7 + A_2 A_6 + A_3 A_5 + A_4 A_4 + A_5 A_3 + A_6 A_2 + A_7 A_1 = 2 \cdot (132 + 42 + 28) + 25 = 429$$

Damit ergibt sich die Tabelle wie folgt:

n	1	2	3	4	5	6	7	8	9	10
A_i	1	1	2	5	14	42	132	429	1430	4862

0.16 (S)

Ist (G, \circ) eine Halbgruppe, $n \in \mathbb{N}$, $a_1, a_2, \dots, a_n \in G$ und $\text{Kl}(a_1 \circ a_2 \circ \dots \circ a_n)$ eine beliebig vorgegebene Beklammerung von $a_1 \circ a_2 \circ \dots \circ a_n$, so gilt stets

$$\text{Kl}(a_1 \circ a_2 \circ \dots \circ a_n) = (\dots ((a_1 \circ a_2) \circ a_3) \dots) \circ a_n =: \text{St}(a_1 \circ a_2 \circ \dots \circ a_n)$$

Das durch die beliebig vorgegebene Beklammerung bestimmte Element aus G stimmt also stets mit dem durch die *Standardbeklammerung* $\text{St}(a_1 \circ a_2 \circ \dots \circ a_n)$ definierten Element aus G überein.

Die Klammern können bei einer Halbgruppe also weggelassen werden bzw. bei der zur Berechnung notwendigen Beklammerung beliebig eingefügt werden.

Beweis durch vollständige Induktion nach $n \in \mathbb{N}$.

- Setze $\{n \in \mathbb{N} \mid (\text{S } 0.16) \text{ ist wahr für alle } k \in \mathbb{N} \text{ mit } 1 \leq k \leq n\} =: T$
 $\leadsto 1, 2, 3 \in T$ (Induktionsverankerung).
- Sei $n \in T$ mit $n \geq 3$ beliebig vorgegeben. Sei $a_1, a_2, \dots, a_n \in G$ beliebig vorgegeben. Sei $\text{Kl}(a_1 \circ a_2 \circ \dots \circ a_n \circ a_{n+1})$ eine beliebig vorgegebene Beklammerung von $a_1 \circ a_2 \circ \dots \circ a_n \circ a_{n+1}$.
- Bezeichnet man die erste zu öffnende Klammer mit $[_1$ und die zugehörige schließende Klammer mit $]_1$, sowie die erste auf $]_1$ folgende Klammer – falls eine solche existiert – mit $[_2$ bzw. $]_2$, so liegt genau einer der folgenden drei Fälle vor:

- (I) $a_1 \circ [_1 a_2 \circ \dots \circ a_n \circ a_{n+1}]_1$,
 (II) $[_1 a_1 \circ a_2 \circ \dots \circ a_n]_1 \circ a_{n+1}$,
 (III) $[_1 a_1 \circ a_2 \circ \dots \circ a_i]_1 \circ [_2 a_{i+1} \circ \dots \circ a_n \circ a_{n+1}]_2$ mit $2 < i < n$.

- Im Fall (I) gilt

$$\begin{aligned}
& a_1 \circ [a_2 \circ \dots \circ a_n \circ a_{n+1}]_1 \\
&= a_1 \circ [\text{St}(a_2 \circ \dots \circ a_n) \circ a_{n+1}] \\
&\stackrel{[\text{Ass}]}{=} [a_1 \circ \text{St}(a_2 \circ \dots \circ a_n)] \circ a_{n+1} \\
&= \text{St}(a_1 \circ a_2 \circ \dots \circ a_n) \circ a_{n+1} \\
&= \text{St}(a_1 \circ a_2 \circ \dots \circ a_n \circ a_{n+1})
\end{aligned}$$

- Im Fall (II) gilt

$$\begin{aligned}
& [a_1 \circ a_2 \circ \dots \circ a_n] \circ a_{n+1} \\
&= \text{St}(a_1 \circ a_2 \circ \dots \circ a_n) \circ a_{n+1} \\
&= \text{St}(a_1 \circ a_2 \circ \dots \circ a_n \circ a_{n+1})
\end{aligned}$$

- Im Fall (III) gilt

$$\begin{aligned}
& [a_1 \circ a_2 \circ \dots \circ a_i] \circ [a_{i+1} \circ \dots \circ a_n \circ a_{n+1}] \\
&= \text{St}(a_1 \circ a_2 \circ \dots \circ a_i) \circ [\text{St}(a_{i+1} \circ \dots \circ a_n) \circ a_{n+1}] \\
&\stackrel{[\text{Ass}]}{=} [\text{St}(a_1 \circ a_2 \circ \dots \circ a_i) \circ \text{St}(a_{i+1} \circ \dots \circ a_n)] \circ a_{n+1} \\
&= \text{St}(a_1 \circ a_2 \circ \dots \circ a_n) \circ a_{n+1} \\
&= \text{St}(a_1 \circ a_2 \circ \dots \circ a_n \circ a_{n+1})
\end{aligned}$$

- \leadsto Für alle $n \in T$ gilt $n + 1 \in T$ (Induktionsschluß).

Nach dem Prinzip der vollständigen Induktion folgt $T = \mathbb{N}$.

0.17 (D)

Ein Gruppoid (G, \circ) heißt genau dann *kommutativ* oder *abelsch*, wenn das *Kommutativgesetz* [Komm] : $a \circ b = b \circ a$ für alle $a, b \in G$ gilt.

0.18 (B)

- (a) (\mathbb{N}, \cdot) ist abelsche Halbgruppe, denn $a \cdot b = b \cdot a$.
- (b) $(\mathbb{N}, \text{hoch})$ ist kein kommutativer Gruppoid, denn es ist z.B. $1 \text{ hoch } 3 = 1^3 = 1 \neq 3 = 3^1 = 3 \text{ hoch } 1$.

0.19 (S)

Ist (G, \circ) eine abelsche Halbgruppe und sind a_1, a_2, \dots, a_n endlich viele Elemente aus G , so gilt

$$a_{\nu 1} \circ a_{\nu 2} \circ \dots \circ a_{\nu n} = a_1 \circ a_2 \circ \dots \circ a_n$$

für jede Permutation (Umordnung) der Reihenfolge der Elemente a_1, a_2, \dots, a_n . Bei jeder abelschen Halbgruppe (G, \circ) ist das dem Term $a_1 \circ a_2 \circ \dots \circ a_n$ zugeordnete Element aus G unabhängig von der zur Berechnung notwendigen Reihenfolge der $a_i \in G$ und der Beklammerung von $a_1 \circ a_2 \circ \dots \circ a_n$.

Beweis

- Sei (G, \circ) eine abelsche Halbgruppe und sind $a_1, a_2, \dots, a_n \in G$ sowie $1 \leq i < n$ beliebig vorgegeben.
- Man kann umgruppieren:

$$\begin{aligned}
 & a_1 \circ a_2 \circ \dots \circ a_i \circ a_{i+1} \circ \dots \circ a_n \\
 & \stackrel{(0.16)}{=} a_1 \circ \dots \circ (a_i \circ a_{i+1}) \circ \dots \circ a_n \\
 & \stackrel{[\text{Komm}]}{=} a_1 \circ \dots \circ (a_{i+1} \circ a_i) \circ \dots \circ a_n \\
 & \stackrel{(0.16)}{=} a_1 \circ \dots \circ a_{i+1} \circ a_i \circ \dots \circ a_n
 \end{aligned}$$

- Bei einer abelschen Halbgruppe dürfen in $a_1 \circ \dots \circ a_i \in G$ zwei beliebig gewählte „Nachbarn“ vertauscht werden, ohne daß das Resultat sich ändert.
- Sei v_1, v_2, \dots, v_n eine beliebig vorgegebene Umordnung des n -Tupels $(1, 2, \dots, n)$. Dann kann der Ausdruck $a_{v_1} \circ a_{v_2} \circ \dots \circ a_{v_n}$ durch Nacheinanderausführung von endlich vielen „Nachbarvertauschungen“ in $a_1 \circ a_2 \circ \dots \circ a_n$ überführt werden. Man benötigt dafür höchstens $(n-1) + (n-2) + \dots + 2 + 1 = \frac{(n-1)n}{2}$ Schritte.
- $\leadsto a_{v_1} \circ a_{v_2} \circ \dots \circ a_{v_n} = a_1 \circ a_2 \circ \dots \circ a_n$

Bemerkung Die Sätze (0.16) und (0.19) ermöglichen oft Rechenvorteile. (\mathbb{N}, \cdot) ist abelsche Halbgruppe $\leadsto 2 \cdot 4 \cdot 5 \cdot 25 = (2 \cdot 5) \cdot (4 \cdot 25) = 10 \cdot 100 = 1000$

0.20 (D)

Eine Halbgruppe mit neutralem Element heißt *Monoid*.

0.21 (A)

Es sei $M =: \{a, b, \dots\}$ eine nichtleere Menge, $\text{Abb}(M) =: \{\alpha, \beta, \dots\}$ mit $a^{\alpha\beta} := (a^\alpha)^\beta$ für alle $(a, \alpha, \beta) \in M \times \text{Abb}(M) \times \text{Abb}(M)$.

Beweise oder widerlege:

- $(\text{Abb}(M), \cdot)$ ist stets ein Monoid.
- (M, \circ) mit $a \circ b := a$ für alle $a, b \in G$ ist stets (nie) ein Monoid.

Bemerkung In dieser Aufgabe findet die Schreibweise a^α Anwendung, die *nicht* als „ a hoch α “ zu lesen ist, sondern „Die Abbildungsvorschrift α wird angewendet auf a “ (vgl. Fußnote auf Seite 8).

Lösung

Definition Für zwei Abbildungen α, β einer Menge M in eine Menge S definiert man $\alpha = \beta \iff \forall m \in M : m^\alpha = m^\beta$

Beweis

- (a) Zu zeigen ist, daß $(\text{Abb}(M), \cdot)$ assoziativ, also Halbgruppe ist und ein neutrales Element besitzt.

Seien $(x, \alpha, \beta, \gamma) \in M \times \text{Abb}(M) \times \text{Abb}(M) \times \text{Abb}(M)$ beliebig vorgegeben.

- $\left. \begin{aligned} x^{(\alpha \cdot \beta) \cdot \gamma} &= (x^{\alpha \cdot \beta})^\gamma = ((x^\alpha)^\beta)^\gamma \\ x^{\alpha \cdot (\beta \cdot \gamma)} &= (x^\alpha)^{\beta \cdot \gamma} = ((x^\alpha)^\beta)^\gamma \end{aligned} \right\} \rightsquigarrow \forall x \in M : x^{(\alpha \cdot \beta) \cdot \gamma} = x^{\alpha \cdot (\beta \cdot \gamma)}$
- Damit ist für alle $\alpha, \beta, \gamma \in \text{Abb}(M) : (\alpha \beta) \gamma = \alpha (\beta \gamma)$
- Demnach ist $(\text{Abb}(M), \cdot)$ Halbgruppe.
- Setze $\text{id}_M : \begin{cases} M \rightarrow M \\ x \mapsto x^{\text{id}_M} := x \end{cases} \quad \forall x \in M.$
- Dann gilt $\text{id}_M \in \text{Abb}(M)$ und es ist $\left. \begin{aligned} x^{(\text{id}_M \cdot \alpha)} &= (x^{\text{id}_M})^\alpha = x^\alpha \\ x^{(\alpha \cdot \text{id}_M)} &= (x^\alpha)^{\text{id}_M} = x^\alpha \end{aligned} \right\} \forall (x, \alpha) \in M \times \text{Abb}(M).$
- $\text{id}_M \cdot \alpha = \alpha = \alpha \cdot \text{id}_M$, d.h. id_M ist neutrales Element von $\text{Abb}(M)$.

Damit ist $(\text{Abb}(M), \cdot)$ ein Monoid.

- (b)
- (M, \circ) mit $a \circ b := a$ für alle $a, b \in M$ ist stets eine Halbgruppe, denn für alle $u, v, w \in M$ gilt $(u \circ v) \circ w = u \circ v = u = u \circ (v \circ w)$.
 - Ist $|M| > 1$, so besitzt (M, \circ) kein neutrales Element, da $N_\rho = M \rightsquigarrow N = \{\}$.
 - Ist $|M| = 1$, so ist (M, \circ) ein Monoid mit neutralem Element a .

0.22 (D)

Sei (G, \circ) ein Monoid (mit neutralem Element n) und $a \in G$.

- (a) Ein Element $\begin{Bmatrix} a_\lambda^i \\ a_\rho^i \\ a^i \end{Bmatrix} \in G$ ist eine $\begin{Bmatrix} \text{links-} \\ \text{rechts-} \\ \text{zwei-} \end{Bmatrix}$ seitige Inverse von a , wenn
- gilt $\begin{Bmatrix} a_\lambda^i \circ a = n \\ a \circ a_\rho^i = n \\ a^i \circ a = n = a \circ a^i \end{Bmatrix}$. Die zweiseitigen Inversen von a werden oft auch einfach nur Inverse von a genannt.

- (b) a heißt *Einheit von* (G, \circ) , wenn a eine Inverse (von a) besitzt.

0.23 (A)

Bestimme für die Monoide $(\mathbb{Z}, +)$, (\mathbb{Z}, \cdot) und $(\text{Abb}(M), \cdot)$ gemäß (A 0.21) jeweils die Menge aller Elemente, die eine rechtsseitige Inverse, eine linksseitige Inverse und eine Inverse besitzen.

Lösung

Ist (G, \circ) ein Monoid, so werde

$$\begin{aligned} \{a \in G \mid a \text{ besitzt eine linksseitige Inverse}\} &=: U_\lambda \\ \{a \in G \mid a \text{ besitzt eine rechtsseitige Inverse}\} &=: U_\rho \\ \{a \in G \mid a \text{ besitzt eine Inverse}\} &=: U \end{aligned}$$

gesetzt.

- (a) $(\mathbb{Z}, +)$: Für jedes $a \in \mathbb{Z}$ ist $-a$ wegen $a + (-a) = 0 = (-a) + a$ eine zweiseitige Inverse, daher folgt $U_\lambda = U_\rho = U = \mathbb{Z}$.
- (b) (\mathbb{Z}, \cdot) :
- Da (\mathbb{Z}, \cdot) abelsch ist, gilt $U_\lambda = U_\rho = U$.
 - Sei $a \in U$ beliebig vorgegeben.
Dann gibt es ein $a' \in \mathbb{Z}$ mit $a \cdot a' = 1$.
 - Angenommen $0 \in \{a, a'\}$, dann wäre $a \cdot a' = 0 \neq 1$. Daher gilt $0 \notin \{a, a'\} \rightsquigarrow |a|, |a'| \geq 1$.
 - Aus $|a| \cdot |a'| = |a \cdot a'| = |1| = 1$ folgt weiter $|a| = \frac{1}{|a'|} \leq 1$.
 - Demnach ist $|a| = 1 \rightsquigarrow a \in \{+1, -1\}$ und man erhält $U \subset \{1, -1\}$.
 - Es ist $1 \cdot 1 = 1 = (-1) \cdot (-1) \rightsquigarrow 1, -1 \in U$
 - Die Menge der Inversen von (\mathbb{Z}, \cdot) ist also $U = \{1, -1\}$.
- (c) $(\text{Abb}(M), \cdot)$: Ist $\varphi \in \text{Abb}(A, B)$ und $b \in B$, so heißt $b^{\varphi^{-1}} := \{a \in A \mid a^\varphi = b\}$ die Urbildmenge bezüglich der Abbildung φ .

- Ich suche zunächst die rechtsseitigen Inversen:

- Sei $\alpha \in U_\rho$ beliebig vorgegeben.
- Dann existiert ein $\beta \in \text{Abb}(M)$, so daß $\alpha \cdot \beta = \text{id}_M$.
- Seien weiterhin $x_1, x_2 \in M$ beliebig vorgegeben.
- Aus $x_1^\alpha = x_2^\alpha =: y$ folgt

$$x_1 = x_1^{\text{id}_M} = x_1^{\alpha \cdot \beta} = (x_1^\alpha)^\beta = y^\beta = (x_2^\alpha)^\beta = x_2^{\alpha \cdot \beta} = x_2^{\text{id}_M} = x_2$$

- Demnach ist $\alpha \in \{\varphi \in \text{Abb}(M) \mid \varphi \text{ ist injektiv}\} =: I$.
- Damit ist $U_\rho \subset I$.
- Sei umgekehrt $\varphi \in I$ beliebig vorgegeben.
- Dann ist $(a^\varphi)^{\varphi^{-1}} = \{a\}$ für alle $a \in M$.
- Wähle ein $c \in M$ (möglich, da $M \neq \{\}$).

$$\text{– Setze } \psi_c : \begin{cases} M \rightarrow M \\ b \mapsto b^{\psi_c} : \begin{cases} a & \text{falls } b = a^\varphi \in M^\varphi \\ c & \text{sonst} \end{cases} \end{cases}$$

Dann ist $\psi_c \in \text{Abb}(M)$.

- Weiterhin ist $a^{\varphi \cdot \psi_c} = (a^\varphi)^{\psi_c} = a = a^{\text{id}_M}$ für alle $a \in M$.
- Damit folgt $\varphi \cdot \psi_c = \text{id}_M \rightsquigarrow \varphi \in U_\rho \rightsquigarrow I \subset U_\rho$.

Für die rechtsseitigen Inversen gilt also $U_\rho = I$.

- Betrachte nun die linksseitigen Inversen.

- Sei $\beta \in U$ beliebig vorgegeben.
- Dann existiert ein $\alpha \in \text{Abb}(M)$, so daß $\alpha \cdot \beta = \text{id}_M$.
- Sei weiterhin $b \in M$ beliebig vorgegeben.
- Für $b^\alpha =: a \in M$ gilt $a^\beta = (b^\alpha)^\beta = b^{\alpha \cdot \beta} = b^{\text{id}_M} = b$.
- Damit ist $\beta \in \{\psi \in \text{Abb}(M) \mid \psi \text{ ist surjektiv}\} =: S$.
- Damit ist $U_\lambda \subset S$.
- Sei umgekehrt $\varphi \in S$ beliebig vorgegeben.
- Wähle für jedes $a \in M$ ein $b_a \in a^{\varphi^{-1}}$ (gemäß dem nicht von allen Mathematikern anerkannten Auswahlaxiom von ca. 1920).

- Dann folgt $\varphi : \begin{cases} M \rightarrow M \\ a \mapsto a^\varphi := b_a \end{cases}$ ist Abbildung von M nach M mit $a^{\varphi \cdot \psi} = (a^\varphi)^\psi = b_a^\psi = a^{\text{id}_M}$ für alle $a \in M$.
- Demzufolge ist $\varphi \cdot \psi = \text{id}_M \rightsquigarrow \psi \in U_\lambda \rightsquigarrow S \subset U_\lambda$.

Resümee: $U_\lambda = S$.

- Nach Definition ist $U \subset U_\lambda$ und $U \subset U_\rho$, woraus sich hier folgendes ergibt:

$$U \subset U_\rho \cap U_\lambda = I \cap S = \text{Bij}(M)$$

- Zeige noch die andere Inklusion:
 - Sei ein $\varphi \in \text{Bij}(M)$ beliebig vorgegeben.
 - Dann ist $|a^{\varphi^{-1}}| = 1$ für alle $a \in M$.
 - Setze $\varphi' : \begin{cases} M \rightarrow M \\ a \mapsto a^{\varphi'} = b \end{cases} \Leftrightarrow b \in a^{\varphi^{-1}}$.
 - Da $(a^\varphi)^{\varphi'} = a \Leftrightarrow a \in (a^\varphi)^{\varphi^{-1}}$ folgt für alle $a \in M$

$$\left. \begin{array}{l} a^{\varphi \cdot \varphi'} = (a^\varphi)^{\varphi'} = a = a^{\text{id}_M} \\ a^{\varphi' \cdot \varphi} = (a^{\varphi'})^\varphi = a = a^{\text{id}_M} \end{array} \right\} \rightsquigarrow \varphi' \cdot \varphi = \varphi \cdot \varphi' = \text{id}_M$$
 - Damit ergibt sich $\varphi \in U$ und $\text{Bij}(M) \subset U$ und als Schlußfolgerung:

$$U = \text{Bij}(M) = U_\lambda \cap U_\rho$$

Ergänzung Für $(\text{Abb}(M), \cdot)$ gilt im Fall $|M| < \infty$:

- $\alpha \in U_\lambda \rightsquigarrow \alpha$ ist surjektiv $\rightsquigarrow \alpha$ ist injektiv, da $|M| < \infty$
 $\rightsquigarrow \alpha \in \text{Bij}(M) \rightsquigarrow \alpha \in U \rightsquigarrow U_\lambda = U$
- $\beta \in U_\rho \rightsquigarrow \beta$ ist injektiv $\rightsquigarrow \beta$ ist surjektiv, da $|M| < \infty$
 $\rightsquigarrow \beta \in \text{Bij}(M) \rightsquigarrow \beta \in U \rightsquigarrow U_\rho = U$

Demnach ist für $|M| < \infty$ stets $U_\lambda = U_\rho = U$.

Ergänzung Für $(\text{Abb}(M), \cdot)$ mit $M = \mathbb{N}$ sei $\varphi : \begin{cases} \mathbb{N} \rightarrow \mathbb{N} \\ n \mapsto n^\varphi =: 2n \end{cases}$. Dann ist φ injektiv, aber nicht surjektiv $\rightsquigarrow \varphi \in U_\lambda \setminus U_\rho$.

Weiterhin sei $\psi : \begin{cases} \mathbb{N} \rightarrow \mathbb{N} \\ n \mapsto n^\psi := \begin{cases} \frac{n}{2} & \text{falls } n \text{ gerade} \\ n & \text{falls } n \text{ ungerade} \end{cases} \end{cases}$. Dann ist ψ surjektiv, aber nicht injektiv $\rightsquigarrow \psi \in U_\rho \setminus U_\lambda$.

0.24 (S+D)

Jedes Element $a \in G$ eines Monoids (G, \circ) besitzt höchstens eine zweiseitige Inverse a^i in (G, \circ) und a^i heißt – falls es existiert, d.h. falls a eine Einheit von (G, \circ) ist – die Inverse von a .

Beweis Sei (G, \circ) ein Monoid (mit neutralem Element n), $a \in G$ und a^i eine zweiseitige Inverse von a . Ist $a' \in G$ ebenfalls eine Inverse von a , so gilt

$$a' = a' \circ n \stackrel{(0.22)}{=} a' \circ (a \circ a^i) \stackrel{[\text{Ass}]}{=} (a' \circ a) \circ a^i \stackrel{(0.22)}{=} n \circ a^i = a^i$$

0.25 (A)

Sei (G, \circ) ein Monoid (mit neutralem Element n) und $a \in G$. Beweise oder widerlege die folgenden Behauptungen:

- (a) Besitzt a eine zweiseitige Inverse a^i , so ist a^i auch die einzige linksseitige und die einzige rechtsseitige Inverse von a .
- (b) Besitzt a mindestens eine rechtsseitige und mindestens eine linksseitige Inverse, so ist a eine Einheit.
- (c) Besitzt a (genau) eine rechtsseitige Inverse, so ist a eine Einheit.

Lösung

- (a) Angenommen a' ist ebenfalls eine linksseitige Inverse von a . Dann wäre

$$a' = a' \circ n = a' \circ (a \circ a^i) = (a' \circ a) \circ a^i = n \circ a^i = a^i$$

also ist $a' = a^i$.

- (b) Angenommen a^* ist ebenfalls eine rechtsseitige Inverse von a . Dann wäre

$$a^* = n \circ a^* = (a^i \circ a) \circ a^* = a^i \circ (a \circ a^*) = a^i \circ n = a^i$$

also ist $a^* = a^i$.

- (c) Sei $\left\{ \begin{array}{l} a_\lambda^i \text{ eine linksseitige} \\ a_\rho^i \text{ eine rechtsseitige} \end{array} \right\}$ Inverse von a . Dann folgt:

$$a_\lambda^i = a_\lambda^i \circ n = a_\lambda^i \circ (a \circ a_\rho^i) = (a_\lambda^i \circ a) \circ a_\rho^i = n \circ a_\rho^i = a_\rho^i =: a^i$$

a^i ist demnach zweiseitige Inverse von a .

0.26 (S)

Ist (G, \circ) ein Monoid (mit neutralem Element n) und U die Menge aller Einheiten von (G, \circ) , so gilt:

- (a) $n \in U$
- (b) $a^i \in U$ für alle $a \in U$ und $(a^i)^i = a$
- (c) $a_1 \circ a_2 \circ \dots \circ a_n \in U$ für alle $a_1, a_2, \dots, a_n \in U$ und

$$(a_1 \circ a_2 \circ \dots \circ a_{n-1} \circ a_n)^i = a_n^i \circ a_{n-1}^i \circ \dots \circ a_2^i \circ a_1^i$$

d.h. die Reihenfolge der Elemente kehrt sich um.

Beweis

- (a) Setze $n =: n^i \rightsquigarrow n^i \circ n = n \circ n = n = n \circ n = n \circ n^i$
 $\rightsquigarrow n^i$ ist zweiseitige Inverse von n .
- (b) Sei $a \in U$ beliebig vorgegeben. $\xrightarrow{(0.22)}$ Zu a existiert ein $a^i \in G$ mit $a \circ a^i =$
 $n = a^i \circ a \xrightarrow{(0.22)} a$ ist zweiseitige Inverse von $a^i \xrightarrow[(0.24)]{(0.22)} a^i \in U$ und $(a^i)^i = a$.

- (c) • Setze $\{n \in \mathbb{N} \mid \text{Für alle } a_1, a_2, a_n \in U \text{ gilt } a_1 \circ a_2 \circ \dots \circ a_n \in U \text{ und } (a_1 \circ a_2 \circ \dots \circ a_{n-1} \circ a_n)^i = a_n^i \circ a_{n-1}^i \circ \dots \circ a_2^i \circ a_1^i\} =: S$.
- Dann ist $1 \in S$ (Induktionsanfang).
- Seien $n \in S$ und $a_1, a_2, \dots, a_n, a_{n+1} \in U$ beliebig vorgegeben.
Setze $a_1 \circ a_2 \circ \dots \circ a_n =: b \in U$ und $b^i := a_n^i \circ a_{n-1}^i \circ \dots \circ a_2^i \circ a_1^i$ (Induktionsannahme).
- $\leadsto a_1 \circ \dots \circ a_{n-1} \circ a_n \circ a_{n+1} = b \circ a_{n+1}$
- Setze $a_{n+1}^i \circ b^i =: c \quad (\in G)$.

$$\begin{aligned}
& (a_1 \circ a_2 \circ \dots \circ a_n \circ a_{n+1}) \circ c \\
&= (b \circ a_{n+1}) \circ (a_{n+1}^i \circ b^i) \\
&\stackrel{[\text{Ass}]}{=} b \circ (a_{n+1} \circ a_{n+1}^i) \circ b^i \\
&= b \circ n \circ b^i = b \circ b^i = n,
\end{aligned}$$

c ist also rechtsseitige Inverse.

$$\begin{aligned}
& c \circ (a_1 \circ a_2 \circ \dots \circ a_n \circ a_{n+1}) \\
&= (a_{n+1}^i \circ b^i) \circ (b \circ a_{n+1}) \\
&= a_{n+1}^i \circ (b \circ b^i) \circ a_{n+1} \\
&= a_{n+1}^i \circ n \circ a_{n+1} = a_{n+1}^i \circ a_{n+1} = n,
\end{aligned}$$

c ist also linksseitige Inverse.

- c ist demnach zweiseitige Inverse von $a_1 \circ a_2 \circ \dots \circ a_n \circ a_{n+1}$.
- Damit ist auch $a_1 \circ a_2 \circ \dots \circ a_n \circ a_{n+1} \in U$ und

$$\begin{aligned}
& (a_1 \circ a_2 \circ \dots \circ a_n \circ a_{n+1})^i = c \\
&= a_{n+1}^i \circ b^i \\
&= a_{n+1}^i \circ (a_n^i \circ \dots \circ a_2^i \circ a_1^i) \\
&= a_{n+1}^i \circ a_n^i \circ \dots \circ a_2^i \circ a_1^i
\end{aligned}$$

- Für alle $n \in S$ gilt $n+1 \in S$ (Induktionsschluß).

Nach dem Prinzip der vollständigen Induktion folgt weiter $S = \mathbb{N}$.

0.27 (S+D)

- (a) Jede Halbgruppe (G, \circ) mit $G \neq \{\}$ besitzt entweder keine oder alle der folgenden Eigenschaften:

- (1) (G, \circ) ist Monoid und jedes $a \in G$ ist Einheit.
- (2) Die Gleichungen $\begin{cases} a \circ x = b \\ y \circ a = b \end{cases}$ sind für beliebig vorgegebene

$a, b \in G$ stets eindeutig lösbar, d.h. es gibt genau ein $\begin{cases} x_0 \in G \\ y_0 \in G \end{cases}$ mit

$$\begin{cases} a \circ x_0 = b \\ y_0 \circ a = b \end{cases}.$$

- (3) Die Gleichungen $\begin{cases} a \circ x = b \\ y \circ a = b \end{cases}$ sind für beliebig vorgegebene $a, b \in G$ stets eindeutig lösbar, d.h. es gibt mindestens ein $\begin{cases} x_0 \in G \\ y_0 \in G \end{cases}$ mit $\begin{cases} a \circ x_0 = b \\ y_0 \circ a = b \end{cases}$.
- (4) (G, \circ) besitzt ein rechtsseitig neutrales Element n_ρ mit der Eigenschaft: Zu jedem $a \in G$ existiert (mindestens) ein $\bar{a} \in G$ mit $a \circ \bar{a} = n_\rho$.
- (5) (G, \circ) besitzt ein linksseitig neutrales Element n_λ mit der Eigenschaft: Zu jedem $a \in G$ existiert (mindestens) ein $a' \in G$ mit $a' \circ a = n_\lambda$.
- (b) Gilt eine und daher – laut (a) – jede der fünf oben genannten Eigenschaften, so heißt (G, \circ) eine *Gruppe*.

Beweis Als Beweismethode ziehen wir den Ringbeweis, auch Beweismühle genannt, heran, d.h. wir zeigen $(1) \rightsquigarrow (2) \rightsquigarrow (3) \rightsquigarrow (4) \rightsquigarrow (5) \rightsquigarrow (1)$.

(a) $(1) \rightsquigarrow (2)$:

- Es gelte (G, \circ) ist ein Monoid und jedes $a \in G$ ist Einheit. Dann besitzt (G, \circ) genau ein neutrales Element und jedes $a \in G$ besitzt genau eine Inverse a^i .
- Seien $a, b \in G$ beliebig vorgegeben.
- Angenommen $\begin{cases} x_0 \in G \\ y_0 \in G \end{cases}$ ist eine Lösung der Gleichung $\begin{cases} a \circ x = b \\ y \circ a = b \end{cases}$. Damit folgt

$$\begin{cases} x_0 = n \circ x_0 = (a^i \circ a) \circ x_0 = a^i \circ (a \circ x_0) = a^i \circ b \\ y_0 = y_0 \circ n = y_0 \circ (a \circ a^i) = (y_0 \circ a) \circ a^i = b \circ a^i \end{cases}$$
- Damit sind höchstens die nach Voraussetzung eindeutig bestimmten Elemente $\begin{cases} a^i \circ b =: x_0 \in G \\ b \circ a^i =: y_0 \in G \end{cases}$ Lösungen der Gleichung $\begin{cases} a \circ x = b \\ y \circ a = b \end{cases}$ (Eindeutigkeit der Lösungen).
- Umgekehrt gilt für diese Elemente $\begin{cases} x_0 \in G \\ y_0 \in G \end{cases}$ aber auch tatsächlich

$$\begin{cases} x_0 = n \circ x_0 = (a^i \circ a) \circ x_0 = a^i \circ (a \circ x_0) = a^i \circ b \\ y_0 = y_0 \circ n = y_0 \circ (a \circ a^i) = (y_0 \circ a) \circ a^i = b \circ a^i \end{cases}$$

(Existenz der Lösungen).

$(2) \rightsquigarrow (3)$:

- Es gelte die Behauptung (2).
- Die Gleichungen $\begin{cases} a \circ x = b \\ y \circ a = b \end{cases}$ besitzen für beliebig vorgegebene $a, b \in G$ stets genau eine Lösung $\begin{cases} x_0 \\ y_0 \end{cases}$.
- Damit folgt Aussage (3) als Abschwächung der Aussage (2).

$(3) \rightsquigarrow (4)$:

- Wähle ein $b \in G$ (möglich, da $G \neq \{\}$). Wähle eine Lösung n_ρ der Gleichung $b \circ x = b \rightsquigarrow b \circ n_\rho = b$.
- Sei $a \in G$ beliebig vorgegeben. Wähle eine Lösung der Gleichung $y \circ a = b \rightsquigarrow y_0 \circ b = a$.

- Es ist $a \circ n_\rho = (y_0 \circ b) \circ n_\rho = y_0 \circ (b \circ n_\rho) = y_0 \circ b = a$. Damit ist n_ρ rechtsseitig neutrales Element von (G, \circ) .
- Sei \bar{a} eine Lösung der Gleichung $a \circ x = n_\rho$. Dann existiert zu jedem $a \in G$ ein $\bar{a} \in G$ mit $a \circ \bar{a} = n_\rho$.
- Somit besitzt (G, \circ) die Eigenschaft (4).

(4) \leadsto (5):

- (G, \circ) besitzt ein rechtsseitig neutrales Element n_ρ mit der Eigenschaft aus (4): Zu jedem $a \in G$ existiert (mindestens) ein $\bar{a} \in G$ mit $a \circ \bar{a} = n_\rho$.
- Sei $a \in G$ beliebig vorgegeben. Dann existiert ein $\bar{a} \in G$ mit $a \circ \bar{a} = n_\rho$.
- Nach (4) gilt dann weiterhin $\bar{a} \in G$ mit $\bar{a} \circ \bar{\bar{a}} = n_\rho$.
- Es ist

$$\bar{a} \circ a \circ \bar{a} \circ \bar{\bar{a}} = \begin{cases} (\bar{a} \circ a) \circ (\bar{a} \circ \bar{\bar{a}}) = (\bar{a} \circ a) \circ n_\rho = \bar{a} \circ a \\ (\bar{a} \circ (a \circ \bar{\bar{a}})) \circ \bar{\bar{a}} = (\bar{a} \circ n_\rho) \circ \bar{\bar{a}} = \bar{a} \circ \bar{\bar{a}} = n_\rho \end{cases}$$

also $\bar{a} \circ a = n_\rho$.

- $n_\rho \circ a = (a \circ \bar{a}) \circ a = a \circ (\bar{a} \circ a) = a \circ n_\rho = a$
- Nenne $n_\rho = n_\lambda$, $a = a'$ und es folgt die Behauptung (5).

(5) \leadsto (1):

- Es gelte die Behauptung (5).
- Sei $a \in G$ beliebig vorgegeben. Dann existiert ein $a' \in G$ mit $a' \circ a = n_\lambda \leadsto \exists a'' \circ a' = n_\lambda$.
- Es ist

$$a'' \circ a' \circ a \circ a' = \begin{cases} (a'' \circ a') \circ (a \circ a') = n_\lambda \circ (a \circ a') = a \circ a' \\ a'' \circ ((a' \circ a) \circ a') = a'' \circ (n_\lambda \circ a') = a'' \circ a' = n_\lambda \end{cases}$$

also $a \circ a' = n_\lambda$.

- $a \circ n_\lambda = a \circ (a' \circ a) = (a \circ a') \circ a = n_\lambda \circ a = a$ und n_λ ist ein zweiseitig neutrales Element von (G, \circ) , d.h. (G, \circ) ist ein Monoid.
- Damit ist a' für jedes $a \in G$ eine zweiseitige Inverse, d.h. jedes $a \in G$ ist Einheit.

0.28 (A)

Es sei (G, \circ) eine Gruppe mit dem neutralen Element n und (U, \circ) ein Untergruppoid von (G, \circ) .

Zeige: Besitzt (U, \circ) ebenfalls ein neutrales Element n' , so gilt $n = n'$.

Lösung

Beweis Seien (G, \circ) eine Gruppe mit neutralem Element n , (U, \circ) ein Untergruppoid mit neutralem Element n' .

Betrachte die Gleichung $n' \circ x = n'$. Im (G, \circ) ist n die Lösung dieser Gleichung. Im (U, \circ) ist n' die Lösung dieser Gleichung.

Da (U, \circ) Untergruppoid von (G, \circ) ist, sind n, n' Lösungen dieser Gleichung in (G, \circ) . Folglich ist $n = n'$, damit ist (U, \circ) ebenfalls eine Gruppe gemäß Satz 0.27.

0.29 (D)

- (a) Wird bei einem Gruppoid (anstatt \circ) das Symbol $\left\{ \begin{smallmatrix} + \\ \cdot \end{smallmatrix} \right\}$ verwendet, so heißt
- $$\left\{ \begin{array}{l} (G, +) \text{ ein } \textit{additiv} \\ (G, \cdot) \text{ ein } \textit{multiplikativ} \end{array} \right\} \text{ geschriebenes Gruppoid.}$$
- (b) Ist $\left\{ \begin{array}{l} (G, +) \\ (G, \cdot) \end{array} \right\}$ eine Halbgruppe, so wird für alle $(a, n) \in G \times \mathbb{N}$ abkürzend
- $$\left\{ \begin{array}{l} \overbrace{a + a + \dots + a}^{n \text{ Summanden}} = n \cdot a \\ \underbrace{a \cdot a \cdot \dots \cdot a}_{n \text{ Faktoren}} = a^n \end{array} \right\} \text{ geschrieben.}$$
- (c) Ist $\left\{ \begin{array}{l} (G, +) \\ (G, \cdot) \end{array} \right\}$ ein Monoid, so wird das neutrale Element $\left\{ \begin{array}{l} \textit{Nullement} \\ \textit{Einselement} \end{array} \right\}$ genannt und mit $\left\{ \begin{array}{l} 0, \text{ genauer } 0_G \\ 1, \text{ genauer } 1_G \end{array} \right\}$ bezeichnet.
- (d) Ist $a \in G$ eine Einheit, so wird das inverse Element a' im Fall $\left\{ \begin{array}{l} (G, +) \\ (G, \cdot) \end{array} \right\}$ mit $\left\{ \begin{array}{l} -a \\ a^{-1} \end{array} \right\}$ bezeichnet.

0.30 (S)

Ist (G, \cdot) ein Halbgruppe, so gelten für alle $(a, m, n) \in G \times \mathbb{N} \times \mathbb{N}$ die folgenden Regeln:

- (a) $a^m \cdot a^n = a^{m+n}$
 (b) $(a^m)^n = a^{m \cdot n}$

Beweis Seien $(a, m, n) \in G \times \mathbb{N} \times \mathbb{N}$ beliebig vorgegeben.

- (a) $a^m \cdot a^n = \underbrace{(a \cdot \dots \cdot a)}_{m \text{ Faktoren}} \cdot \underbrace{(a \cdot \dots \cdot a)}_{n \text{ Faktoren}} = \underbrace{a \cdot \dots \cdot a \cdot a \cdot \dots \cdot a}_{m+n \text{ Faktoren}} = a^{m+n}$
- (b) $(a^m)^n = \underbrace{a^m \cdot \dots \cdot a^m}_{n \text{ Terme}} = \underbrace{(a \cdot \dots \cdot a)}_{m \text{ Faktoren}} \cdot \dots \cdot \underbrace{(a \cdot \dots \cdot a)}_{m \text{ Faktoren}} = \underbrace{a \cdot \dots \cdot a}_{n \text{ Klammerterme}} = a^{m \cdot n}$

0.31 (S+D)

Ist (G, \cdot) ein Monoid, so gilt:

- (a) (U, \cdot) mit $U := \{a \in G \mid a \text{ ist Einheit}\}$ ist eine Gruppe und U heißt die *Einheitengruppe* von (G, \cdot) .
- (b) $(a^n)^{-1} = (a^{-1})^n =: a^{-n} \in U$ für alle $(a, n) \in U \times \mathbb{N}$
 Setzt man noch $a^0 := 1_G$, so stellt $\gamma: \begin{cases} U \times \mathbb{Z} \rightarrow U \\ (a, \gamma) \mapsto a^\gamma \end{cases}$ eine eindeutige Abbildung von $U \times \mathbb{Z}$ nach U dar.
- (c) Für alle $(a, \gamma, \delta) \in U \times \mathbb{Z} \times \mathbb{Z}$ gelten die Potenzregeln:

- (1) $a^\gamma \cdot a^\delta = a^{\gamma+\delta}$
- (2) $(a^\gamma)^\delta = a^{\gamma\delta}$

Beweis Sei (G, \cdot) ein Monoid.

- (a) • Setze $\{a \in G \mid a \text{ ist Einheit}\} =: U$, dann ist $1_G \in U$ und $U \neq \{\}$. Seien $a, b \in U$ beliebig vorgegeben.
- $a \cdot b \in U \rightsquigarrow U$ ist Untergruppoid.
- Seien $a, b, c \in U$ beliebig vorgegeben, dann sind auch $a, b, c \in G$. Da (G, \cdot) Halbgruppe ist, folgt somit $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, weswegen (U, \cdot) Halbgruppe ist.
- Demnach ist (U, \cdot) ein Monoid.
- Sei nun $a \in U$ beliebig vorgegeben. Dann ist auch $a^{-1} \in U$ und, da $a^{-1}a = 1_G = aa^{-1}$, jedes $a \in U$ ist Einheit von (U, \cdot) .

Damit ist (U, \cdot) eine Gruppe.

- (b) • Sei $(a, n) \in U \times \mathbb{N}$ beliebig vorgegeben.
- Dann ist $a^n = \underbrace{a \cdot \dots \cdot a}_{n \text{ Faktoren}} \in U \rightsquigarrow (a^n)^{-1} \in U$.
- Weiter ist $(a^n)^{-1} = (a \cdot \dots \cdot a)^{-1} = a^{-1} \cdot \dots \cdot a^{-1} = (a^{-1})^n =: a^{-n} \in U$.
- Also sind $a^n, a^{-n} \in U \forall n \in \mathbb{N} \rightsquigarrow a^\gamma \in U$ für alle $(a, \gamma) \in U \times \mathbb{Z}$.
- (c) (1) • Sei $a \in U$ beliebig, dann aber fest vorgegeben.
Setze $\{n \in \mathbb{N}_0 \mid a^\gamma \cdot a^n = a^{\gamma+n} \text{ für alle } \gamma \in \mathbb{Z}\} =: S$.
- Wegen $a^\gamma \cdot a^0 = a^\gamma \cdot 1_G = a^\gamma = a^{\gamma+0}$ ist $0 \in S$.
Sei $n \in S$ beliebig vorgegeben.
 $a^\gamma a^n = a^{\gamma+n} =: a^\sigma$ mit $\gamma + n = \sigma$.
- Es ist $a^\gamma a^{n+1} = a^\gamma (a^n a) = (a^\gamma a^n) a = a^\sigma a$.
Unterscheide drei Fälle:
(I) $\sigma \in \mathbb{N} \rightsquigarrow a^\sigma a = (a \cdot \dots \cdot a) \cdot a = a^{\sigma+1}$
(II) $\sigma = 0 \rightsquigarrow a^\sigma a = a^0 a = 1_G a = a = a^1 = a^{\sigma+1}$
(III) $\sigma < 0 \rightsquigarrow \sigma =: -m$ für ein $m \in \mathbb{N}$.
- Man kann umformen:

$$\begin{aligned}
 & \underbrace{(a^{-1} \cdot \dots \cdot a^{-1})}_{m \text{ Faktoren}} \cdot a \\
 &= (a^{-1} \cdot \dots \cdot a^{-1}) \cdot (a^{-1} \cdot a) \\
 &= \underbrace{a^{-1} \cdot \dots \cdot a^{-1}}_{m-1 \text{ Faktoren}} \\
 &= (a^{-1})^{m-1} = a^{-(m-1)} = a^{(-m)+1} \\
 &= a^{\sigma+1}
 \end{aligned}$$

$$\text{also } a^\gamma \cdot a^{n+1} = a^\sigma \cdot a = a^{\sigma+(n+1)}.$$

- Damit hat man nach dem Prinzip der vollständigen Induktion gezeigt, daß $n+1 \in S \rightsquigarrow a^\gamma \cdot a^n = a^{\gamma+n}$ für alle $(\gamma, n) \in \mathbb{Z} \times \mathbb{Z}_0$.
- Analog zeigt man $a^n \cdot a^\delta = a^{n+\delta}$ für alle $(n, \delta) \in \mathbb{Z} \times \mathbb{Z}_0$.
Folglich ist $a^\gamma \cdot a^\delta = a^{\gamma+\delta}$, falls $\gamma \geq 0$ oder falls $\delta \geq 0$.

- Im Fall $\gamma < 0$ und $\delta < 0$ gilt $-\gamma =: m \in \mathbb{N}$ und $-\delta =: n \in \mathbb{N}$, und mit $a^{-1} =: b \in U$ erhält man:

$$\begin{aligned} a^{\gamma\delta} &= (a^{-1})^m (a^{-1})^n = b^m b^n = b^{m+n} = (a^{-1})^{m+n} \\ &= (a^{-1})^{-\gamma-\delta} = a^{\gamma+\delta} \end{aligned}$$

(2) Diene der geneigten Leserin bzw. dem geneigten Leser als Aufgabe.

0.32 (A)

Beweise (0.32) (S+D)(c)(2)!

Lösung

- Seien $(a, \gamma) \in U \times \mathbb{Z}$ beliebig vorgegeben.
- Setze $a^\gamma := b \in U$ und $\{n \in \mathbb{N}_0 \mid (a^\gamma)^n = a^{\gamma \cdot n}\} =: S$.
- Es ist $(a^\gamma)^0 = b^0 = 1_G = a^0 = a^{\gamma \cdot 0}$, damit ist $0 \in S$.
- Sei ein $n \in S$ beliebig vorgegeben, dann ist $b^n = (a^\gamma)^n = a^{\gamma \cdot n}$.
- Es ist $(a^\gamma)^{n+1} = b^{n+1} = b^n \cdot b = a^{\gamma \cdot n} \cdot a^\gamma = a^{\gamma \cdot n + \gamma} = a^{\gamma(n+1)}$.
- Damit ist $n+1 \in S$ für alle $n \in S$ und nach dem Prinzip der vollständigen Induktion folgt $(a^\gamma)^n = a^{\gamma \cdot n}$ für alle $n \in \mathbb{N}_0$.
- Für $\gamma \in \mathbb{Z}$ gilt
 - im Fall $\gamma > 0$: $\gamma =: n \in \mathbb{N} \rightsquigarrow (a^\gamma)^{-1} = (a^n)^{-1} = a^{-n} = a^{-\gamma}$
 - im Fall $\gamma = 0$: $(a^\gamma)^{-1} = (a^0)^{-1} = 1_G^{-1} = 1_G = a^0 = a^{-0} = a^{-\gamma}$
 - Im Fall $\gamma < 0$: Setze $j = -n$ mit einem $n \in \mathbb{N}$. Dann ist $(a^\gamma)^{-1} = (a^{-n})^{-1} = ((a^n)^{-1})^{-1} = a^n = a^{-\gamma}$
- Es ist also stets $(a^\gamma)^{-1} = a^{-\gamma}$.
- Für $\delta \in \mathbb{Z}$ mit $\delta < 0$ gilt $\delta =: -n$ mit einem $n \in \mathbb{N}$.
- Dann ist $(a^\gamma)^\delta = b^\delta = b^{-n} = (b^{-1})^n = ((a^\gamma)^{-1})^n = a^{(-\gamma) \cdot n} = a^{\gamma \cdot (-n)} = a^{\gamma \cdot \delta}$.

0.33 (D)

Es sei (G, \cdot) eine Gruppe. Ein Untergruppoid U heißt *Untergruppe von* (G, \cdot) , wenn (U, \cdot) eine Gruppe ist.

0.34 (S) Untergruppenkriterium

Für eine Teilmenge $U \subset G$ eine Gruppe (G, \cdot) sind äquivalent:

- U ist eine Untergruppe von (G, \cdot) .
- Es gilt $U \neq \{\}$ und $a \cdot b^{-1} \in U$ für alle $a, b \in U$.

Beweis(a) \leadsto (b):

- Sei U eine Untergruppe von (G, \cdot) . Dann ist (U, \cdot) eine Gruppe, $U \neq \{\}$ und U besitzt ein neutrales Element 1_U .
- Die Gleichung $1_U \cdot x = 1_U$ besitzt in U die Lösung $x = 1_U$ und in (G, \cdot) wegen $G \supset U$ die Lösung $x = 1_G$. Wegen $1_G \in U \subset G$ besitzt die Gleichung in (G, \cdot) also die Lösungen 1_G und 1_U . Folglich ist $1_U = 1_G \in U$.
- Sei $b \in U$ beliebig vorgegeben. Dann besitzt die Gleichung $b \cdot x = 1_G$ in U genau eine Lösung $b' \in U$. Wegen $U \subset G$ ist $b' \in G$ auch eine Lösung von $b \cdot x = 1_G$ in G . Da es nach (0.27) aber nur eine Lösung gibt, muß $b' = b^{-1} \in U$, d.h. für alle $b \in U$ gilt $b^{-1} \in U$.
- Seien $a, b \in U$ beliebig vorgegeben, dann sind auch $a, b^{-1} \in U$. Da (U, \cdot) Untergruppoid, folgt $a \cdot b^{-1} \in U$ für alle $a, b \in U$, was die Behauptung aus (b) ist.

(b) \leadsto (a):

- Es sei $U \neq \{\}$ und $ab^{-1} \in U$ für alle $a, b \in U$.
- Wähle ein $a \in U$ (möglich, da $U \neq \{\}$), dann sind $a, a \in U$ und weiter $aa^{-1} = 1_G \in U$.
- Sei $b \in U$ beliebig vorgegeben, dann sind $1_G, b \in U$, weshalb auch $1_G b^{-1} = b^{-1} \in U$ ist für alle $a, b \in U$.
- Seien $a, b \in U$ beliebig vorgegeben, dann sind $a, b^{-1} \in U$ und $a(b^{-1})^{-1} = ab \in U$.
- Damit ist (U, \cdot) Untergruppoid von (G, \cdot) . Da weiterhin (G, \cdot) Halbgruppe ist, ist auch (U, \cdot) Halbgruppe, somit ist (U, \cdot) ein Monoid.
- Sei $a \in U$ beliebig vorgegeben. Dann ist auch $a^{-1} \in U$ und a besitzt in (U, \cdot) eine zweiseitige Inverse (nämlich a^{-1}), d.h. jedes $a \in U$ ist Einheit in (U, \cdot) .
- Das zeigt die Behauptung aus (a), daß (U, \cdot) eine Gruppe ist.

0.35 (A)

Beweise oder widerlege:

$$\{U \in \mathbb{Z} \mid U \text{ ist Untergruppe von } (\mathbb{Z}, +)\} = \{\mathbb{Z}_n \mid n \in \mathbb{N}\}$$

mit $\mathbb{Z}_n := \{\gamma_n \mid \gamma \in \mathbb{Z}\}$.**Lösung****Beweis**

- Sei $n \in \mathbb{N}_0$ beliebig vorgegeben, dann ist $\mathbb{Z}_n \neq \{\}$. Seien weiterhin $a =: \gamma n, b =: \delta n \in \mathbb{Z}_n$ beliebig vorgegeben.
- $a - b = \gamma n - \delta n = (\gamma - \delta)n \in \mathbb{Z}_n$, da $(\gamma - \delta) \in \mathbb{Z}$. Nach dem Untergruppenkriterium folgt daraus $\{\mathbb{Z}_n \mid n \in \mathbb{N}_0\} \subset \{U \in \mathbb{Z} \mid U \text{ ist Untergruppe von } (\mathbb{Z}, +)\}$.
- Sei eine Untergruppe U von $(\mathbb{Z}, +)$ beliebig vorgegeben, dann ist $0 \in U$ und weiterhin

- 1. Fall $U = 0$: $U = \mathbb{Z}_0 = \{\gamma \cdot 0 \mid \gamma \in \mathbb{Z}\}$
- 2. Fall $\exists a \in U \setminus \{0\} \rightsquigarrow \{a, -a\} \subset U \rightsquigarrow U \cap \mathbb{N} \neq \{\}$
- Setze $(*) \min\{x \in U \cap \mathbb{N}\} =: n$.
Dann sind $n + n = 2 \cdot n \in U$, $(n + n) + n = 3 \cdot n \in U$, ... und es folgt $U \supset \mathbb{N} \cdot n =: \{v \cdot n \mid v \in \mathbb{N}\}$.
- Sei ein $v \in \mathbb{N}$ beliebig vorgegeben.
 $v \cdot n \in U \rightsquigarrow -(v \cdot n) = (-v) \cdot n \in U \rightsquigarrow U \supset \mathbb{Z}_n$.
- Sei $a \in U$ beliebig vorgegeben, dann existiert ein $\gamma \in \mathbb{Z}$: $\gamma n \leq a < (\gamma + 1)n$.
Damit ist $0 \leq \overbrace{a}^{\in U} - \underbrace{\gamma \cdot n}_{\in U} < n$. Wegen $(*)$ ergibt sich $a - \gamma n = 0 \rightsquigarrow$
 $a = \gamma n \in \mathbb{Z}_n$ und es ist $U \subset \mathbb{Z}_n$.

Da beide Inklusionen gezeigt sind, gilt $U = \mathbb{Z}_n$.

0.36 (A)

Beweise oder widerlege die folgenden Aussagen:

Sind U, V Untergruppen eine Gruppe (G, \cdot) , so ist auch stets

- (a) $U \cap V$ ein Untergruppe von (G, \cdot) ,
- (b) $U \cup V$ ein Untergruppe von (G, \cdot) .

Lösung

- (a) • Seien U, V Untergruppen einer Gruppe (G, \circ) . Da $1_G \in U$ und $1_G \in V$, ist $1_G \in U \cap V$ und weiter $U \cap V =: D \neq \{\}$.
• Seien $a, b \in D$ beliebig vorgegeben.
• Dann sind $\left\{ \begin{array}{l} a, b \in U \rightsquigarrow a \cdot b^{-1} \in U \\ a, b \in V \rightsquigarrow a \cdot b^{-1} \in V \end{array} \right\}$ (jeweils nach dem Untergruppenkriterium), also $a \cdot b^{-1} \in D$ für alle $a, b \in D$.
• Nach dem Untergruppenkriterium ist D somit Untergruppe von (G, \circ) .
- (b) • $\mathbb{Z}_2, \mathbb{Z}_3$ sind Untergruppen von $(\mathbb{Z}, +)$. Es sind $3, 2 \in \mathbb{Z}_2 \cup \mathbb{Z}_3 =: V$.
• Angenommen V wäre Untergruppe von $(\mathbb{Z}, +)$, dann müßte gelten $3 - 2 = 1 \in V$.
• Es ist aber $1 \notin \mathbb{Z}_2 \cup \mathbb{Z}_3 = \{\gamma \cdot 2 \mid \gamma \in \mathbb{Z}\} \cup \{\delta \cdot 3 \mid \delta \in \mathbb{Z}\}$.
• Widerspruch!

0.37 (A)

Es sei $U \neq \{\}$ ein Untergruppoid einer Gruppe (G, \cdot) . Beweise oder widerlege:

- (a) Ist $|U| < \infty$, so ist U stets eine Untergruppe von (G, \cdot) .
- (b) Ist $|U| = \infty$, so ist U stets eine Untergruppe von (G, \cdot) .

Lösung

- (a)
- Sei $b \in U$ beliebig vorgegeben.
 - Da U Untergruppoid ist, läßt sich sagen $U \supset \{b, b^2, \dots, b^n, \dots, b^m, \dots\}$.
 - Da weiterhin nach Voraussetzung $|U| < \infty$, existieren $0 < n < m$ mit $b^n = b^m$. Damit ist $b^{n-n} = b^{m-n} = b^k = 1_G$ mit $k := m - n, 0 < k$.
 - Falls nun $k = 1 \rightsquigarrow b^1 = 1_G \rightsquigarrow b^{-1} = 1_G^{-1} = 1_G \in U$.
 - Falls hingegen $k > 0 \rightsquigarrow b^{k-1} \cdot b = b^k = 1_G \rightsquigarrow b^{-1} = b^{k-1} \in U$.
 - Es folgt aus beiden Fällen, daß $b^{-1} \in U$ für alle $b \in U$.
- Seien $a, b \in U$ beliebig vorgegeben, dann ist, wie eben festgelegt, $a, b^{-1} \in U$ und, da (U, \cdot) Untergruppoid, $ab^{-1} \in U$.
 - Es ist n.V. $U \neq \{\}$, daher folgt nach dem Untergruppenkriterium, daß U Untergruppe von (G, \circ) ist.
- (b) *Widerspruch*: \mathbb{N} ist Untergruppoid von $(\mathbb{Z}, +)$. Angenommen \mathbb{N} sei Untergruppe von $(\mathbb{Z}, +)$, dann müßte, da $2 \in \mathbb{N}$, auch $-2 \in \mathbb{N}$ sein, was einen Widerspruch darstellt.

0.38 (D)

Ist $(G, +)$ eine additiv geschriebene Gruppe und sind $a, b \in G$, so ist $a - b$ bzw. $-a + b$ eine abkürzende Schreibweise für $a + (-b)$ bzw. $(-a) + b$.

0.39 (D)

- (a) Es seien $(L, +), (R, +), (A, +)$ – L wie links, R wie rechts und A wie abelsch – drei nicht notwendig verschiedene abelsche Gruppen mit den Nullelementen $0_L, 0_R$ und 0_A und $\cdot : \begin{cases} L \times R \rightarrow A \\ (l, r) \mapsto l \cdot r \end{cases}$ eine Abbildung von $L \times R$ nach A .
- Das Quadrupel $((L, +), (R, +), (A, +), \cdot)$ heißt genau dann *distributive Verknüpfung abelscher Gruppen (DVAG)*, wenn für alle $l_1, l_2, l \in L$ und für alle $r_1, r_2, r \in R$ die *Distributivgesetzte* gelten:

$$[\text{Dist}]_L : \underbrace{(l_1 + l_2) \cdot r}_{\in A} = \underbrace{l_1 r}_{\in A} + \underbrace{l_2 r}_{\in A}$$

$$[\text{Dist}]_R : l \cdot (r_1 + r_2) = lr_1 + lr_2$$

- (b) Gilt $(L, +) = (R, +) = (A, +)$ so heißt die DVAG $((L, +), (R, +), (A, +), \cdot) =: (A, +, \cdot)$ ein *verallgemeinerter Ring*.
- (c) Ein verallgemeinerter Ring $(R, +, \cdot)$ heißt *Ring*, wenn (R, \cdot) eine Halbgruppe ist.
 Er heißt *Ring mit Einselement*, wenn (R, \cdot) Monoid ist.
 Er heißt *Körper*, wenn $((R \setminus \{0\}), \cdot)$ eine Gruppe ist.
- (d) (*Klammereinsparregel*). Fehlen bei einer DVAG bei einem Term (z.B. $3 \cdot 4 + 5$) die Klammern, so gilt die Konvention *Punktrechnung* $(\cdot, \circ, *)$ verknüpft stärker als *Strichrechnung* $(+, -)$ [in der Schule lapidar als „Punktrechnung geht vor Strichrechnung“ bezeichnet].

0.40 (B)

- (a) $(\mathbb{Z}, +, \cdot)$ ist ein Ring mit Einselement (der *Ring der ganzen Zahlen*).
 (b) $(\mathbb{R}, +, \cdot)$ ist ein Körper (der *Körper der reellen Zahlen*).

0.41 (A)

Ist $(\mathbb{R}, +)$ die additive Gruppe der reellen Zahlen und $n \in \mathbb{N}$, so wird für alle $(\alpha_1, \alpha_2, \dots, \alpha_n) =: a$ $(\beta_1, \beta_2, \dots, \beta_n) =: b \in \mathbb{R}^n$

$$a + b := (\alpha_1 + \beta_1, \alpha_2 + \beta_2, \dots, \alpha_n + \beta_n)$$

gesetzt. Damit sind $(\mathbb{R}, +)$ und $(\mathbb{R}^n, +)$ abelsche Gruppen.

Wir definieren die Abbildungen:

$$\begin{aligned} \cdot & : \begin{cases} \mathbb{R} \times \mathbb{R}^n \rightarrow \mathbb{R}^n \\ (\alpha, a) \mapsto \alpha \cdot a := (\alpha\alpha_1, \alpha\alpha_2, \dots, \alpha\alpha_n) \end{cases} \\ \circ & : \begin{cases} \mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R} \\ (a, b) \mapsto a \circ b := (\alpha_1 \cdot \beta_1 + \alpha_2 \cdot \beta_2 + \dots + \alpha_n \cdot \beta_n) \end{cases} \\ * & : \begin{cases} \mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}^n \\ (a, b) \mapsto a * b := (\alpha_1 \cdot \beta_1, \alpha_2 \cdot \beta_2, \dots, \alpha_n \cdot \beta_n) \end{cases} \end{aligned}$$

Beweise oder widerlege: Das Quadrupel

- (a) $((\mathbb{R}, +), (\mathbb{R}^n, +), (\mathbb{R}^n, +), \cdot)$ ist eine DVAG.
 (b) $((\mathbb{R}^n, +), (\mathbb{R}^n, +), (\mathbb{R}, +), \circ)$ ist eine DVAG.
 (c) $((\mathbb{R}^n, +), (\mathbb{R}^n, +), (\mathbb{R}^n, +), *)$ ist $\begin{cases} \text{eine DVAG} \\ \text{ein Ring mit Einselement} \\ \text{ein Körper} \end{cases}$.

Lösung

Zeige zunächst, daß $(\mathbb{R}^n, +)$ mit der Voraussetzung $a + b := (\alpha_1 + \beta_1, \alpha_2 + \beta_2, \dots, \alpha_n + \beta_n)$ abelsche Gruppe ist.

- $(\mathbb{R}^n, +)$ ist ein abelsches Gruppoid, denn
 $a + b = (\alpha_1 + \beta_1, \alpha_2 + \beta_2, \dots, \alpha_n + \beta_n) = (\beta_1 + \alpha_1, \beta_2 + \alpha_2, \dots, \beta_n + \alpha_n) = b + a$.
- Setze $(0, \dots, 0) = 0_{\mathbb{R}^n}$. Dann ist $a + 0_{\mathbb{R}^n} = (\alpha_1 + 0, \alpha_2 + 0, \dots, \alpha_n + 0) = (\alpha_1, \alpha_2, \dots, \alpha_n) = a$ und $0_{\mathbb{R}^n}$ ist neutrales Element von $(\mathbb{R}^n, +)$.
- Es gilt das Assoziativgesetz:

$$\begin{aligned} (a + b) + c &= (\alpha_1 + \beta_1, \alpha_2 + \beta_2, \dots, \alpha_n + \beta_n) + (\gamma_1, \gamma_2, \dots, \gamma_n) \\ &= ((\alpha_1 + \beta_1) + \gamma_1, \dots, (\alpha_n + \beta_n) + \gamma_n) \\ &= (\alpha_1 + (\beta_1 + \gamma_1), \dots, \alpha_n + (\beta_n + \gamma_n)) \quad \text{da } (\mathbb{R}^n, +) \text{ ass.} \\ &= (\alpha_1, \alpha_2, \dots, \alpha_n) + ((\beta_1, \beta_2, \dots, \beta_n) + (\gamma_1, \gamma_2, \dots, \gamma_n)) \\ &= a + (b + c) \end{aligned}$$

Damit ist $(\mathbb{R}^n, +)$ abelsches Monoid.

- Setze $(-\alpha_1, -\alpha_2, \dots, -\alpha_n) =: x$. Dann ist $a+x = (\alpha_1+(-\alpha_1), \alpha_2+(-\alpha_2), \dots, \alpha_n+(-\alpha_n)) = (0, 0, \dots, 0) = 0_{\mathbb{R}^n}$ und x ist Inverse zu a in $(\mathbb{R}^n, +)$.
- Wir haben somit gezeigt, daß $(\mathbb{R}^n, +)$ abelsche Gruppe ist.

Zeige nun die drei Behauptungen:

- (a) Zeige: $((\mathbb{R}, +), (\mathbb{R}^n, +), (\mathbb{R}^n, +), \cdot)$ ist mit $\alpha \cdot a := (\alpha\alpha_1, \alpha\alpha_2, \dots, \alpha\alpha_n)$ für alle $(\alpha, a) \in \mathbb{R} \times \mathbb{R}^n$ eine DVAG.
- $\text{ad } [\text{Dist}]_L$:
 - $(\alpha + \beta) \cdot a = ((\alpha + \beta)\beta_1, (\alpha + \beta)\beta_2, \dots, (\alpha + \beta)\beta_n)$
 - Da in $(\mathbb{R}, +, \cdot)$ stets das linke Distributivgesetz gilt, folgt weiter $(\alpha + \beta) \cdot a = (\alpha\beta_1 + \beta\beta_1, \alpha\beta_2 + \beta\beta_2, \dots, \alpha\beta_n + \beta\beta_n) = (\alpha\beta_1, \alpha\beta_2, \dots, \alpha\beta_n) + (\beta\beta_1, \beta\beta_2, \dots, \beta\beta_n) = \alpha \cdot a + \beta \cdot a$.
 - $\text{ad } [\text{Dist}]_R$: Wurde nicht fortgesetzt.

0.42 (S) Dualitätsprinzip

Ist $((L, +), (R, +), (A, +), \cdot)$ eine DVAG, so ist $((R, +), (L, +), (A, +), \circ)$ mit

$$\circ : \begin{cases} R \times L \rightarrow A \\ (r, l) \mapsto r \circ l =: l \cdot r \end{cases}$$

ebenfalls eine DVAG.

$((R, +), (L, +), (A, +), \circ)$ heißt die zur $((L, +), (R, +), (A, +), \cdot)$ *duale DVAG*.

Beweis Wir müssen zeigen, daß für $((L, +), (R, +), (A, +), \circ)$ ebenfalls die beiden Distributivgesetze gelten.

Seien $r_1, r_2, r \in R$ und $l_1, l_2, l \in L$ beliebig vorgegeben.

$$\begin{aligned} [\text{Dist}]_L : \quad (r_1 + r_2) \circ l &= l \cdot (r_1 + r_2) = l \cdot r_1 + l \cdot r_2 = r_1 \circ l + r_2 \circ l \\ [\text{Dist}]_R : \quad r \circ (l_1 + l_2) &= (l_1 + l_2) \cdot r = l_1 \cdot r + l_2 \cdot r = r \circ l_1 + r \circ l_2 \end{aligned}$$

0.43 (S) Rechenregeln für DVAG's

Ist $((L, +), (R, +), (A, +), \cdot)$ eine DVAG, so gelten für alle $l, l_1, \dots, l_n \in L$ und alle $r, r_1, \dots, r_m \in R$ mit $n, m \in \mathbb{N}$ die folgenden Rechenregeln:

- $0_L \cdot r = 0_A$
- $l \cdot 0_r = 0_a$
- $(-l) \cdot r = -l \cdot r$
- $l \cdot (-r) = -l \cdot r$
- $(-l) \cdot (-r) = l \cdot r$
- $l \cdot (r_1 - r_2) = l \cdot r_1 - l \cdot r_2$
- $(l_1 - l_2) \cdot r = l_1 \cdot r - l_2 \cdot r$
- $(\sum_{i=1}^n l_i) \cdot r = \sum_{i=1}^n l_i \cdot r$
- $l \cdot (\sum_{i=1}^m r_i) = \sum_{i=1}^m (l \cdot r_i)$
- $(\sum_{i=1}^n l_i) \cdot (\sum_{j=1}^m r_j) = \sum_{i=1, \dots, n} \sum_{j=1, \dots, m} l_i \cdot r_j$

Nach dem Dualitätsprinzip folgt dabei (b) aus (a), (d) aus (c) und (i) aus (h).

Beweis

(a) Für $0_L \cdot r =: a \in A$ gilt

$$a + a = 0_L \cdot r + 0_L \cdot r = (0_L + 0_L) \cdot r = 0_L \cdot r = a,$$

also $a + a = a$, daher ist

$$a = a + 0_A = a + (a + (-a)) = (a + a) + (-a) = a + (-a) = 0_A$$

(b) Es ist $l \cdot 0_R = 0_R \circ l = 0_A$

(c) Es ist $l \cdot r + (-l) \cdot r = (l + (-l)) \cdot r \stackrel{(a)}{=} 0_L \cdot r = 0_A$.

Damit ist $(-l) \cdot r$ in $(A, +)$ die Lösung der Gleichung $(l \cdot r) + x = 0_A$

$$\leadsto (-l) \cdot r = -(l \cdot r)$$

(d) $l \cdot (-r) = (-r) \circ l = -(r \circ l) = -(l \cdot r)$

$$(e) \quad (-l) \cdot (-r) \stackrel{(a)}{=} -(l \cdot (-r)) \stackrel{(c)}{=} -(-(r \cdot l)) = r \cdot l$$

$$(f) \quad l \cdot (r_1 - r_2) = l \cdot (r_1 + (-r_2)) = l \cdot r_1 + l \cdot (-r_2) = l \cdot r_1 + (-(l \cdot r_2)) = l \cdot r_1 - l \cdot r_2$$

$$(g) \quad (l_1 - l_2)r = (l_1 + (-l_2)) \cdot r = l_1 \cdot r + (-l_2) \cdot r = l_1 \cdot r + (-(l_2 \cdot r)) = l_1 \cdot r - l_2 \cdot r$$

- (h) • Setze $\{n \in \mathbb{N} \mid (\sum_{i=1}^n l_i) \cdot r = \sum_{i=1}^n (l_i \cdot r) \text{ für alle } l_1, \dots, l_n \in L \text{ und } r \in R\} =: S$
- Dann ist $1 \in S$.
 - Sei ein $n \in S$, $l_1, \dots, l_n, l_{n+1} \in L$ und ein $r \in R$ beliebig vorgegeben.
 - Damit ist:

$$\begin{aligned} & (l_1 + l_2 + \dots + l_n + l_{n+1}) \cdot r \\ &= ((l_1 + l_2 + \dots + l_n) + l_{n+1}) \cdot r \\ &= (l_1 + l_2 + \dots + l_n) \cdot r + l_{n+1} \cdot r \\ &= (l_1 \cdot r + l_2 \cdot r + \dots + l_n \cdot r) + l_{n+1} \cdot r \\ &= l_1 \cdot r + l_2 \cdot r + \dots + l_n \cdot r + l_{n+1} \cdot r \end{aligned}$$

- Für alle $n \in S$ gilt $n + 1 \in S$, nach dem Prinzip der vollständigen Induktion folgt $S = \mathbb{N}$.

(i) Seien $m \in \mathbb{N}, l \in L$ und $r_1, \dots, r_m \in R$ beliebig vorgegeben. Dann ist $l \cdot (r_1 + \dots + r_m) = (r_1 + \dots + r_m) \circ l \stackrel{(h)}{=} r_1 \circ l + \dots + r_m \circ l = l \cdot r_1 + \dots + l \cdot r_m$.

- (j) • Seien $l_1, \dots, l_n \in L$ und $r_1, \dots, r_m \in R$ beliebig vorgegeben.
- Setze $l_1 + l_2 + \dots + l_n =: l \in L$ und $r_1 + r_2 + \dots + r_m =: r \in R$.
 - Damit ist

$$\begin{aligned} & (l_1 + \dots + l_n) \cdot (r_1 + \dots + r_m) \\ &= l \cdot (r_1 + \dots + r_m) \\ &= l \cdot r_1 + \dots + l \cdot r_m \\ &= (l_1 + \dots + l_n) \cdot r_1 + \dots + (l_1 + \dots + l_n) \cdot r_m \\ &= l_1 \cdot r_1 + l_2 \cdot r_1 + \dots + l_n \cdot r_1 + \dots + l_1 \cdot r_m + \dots + l_n \cdot r_m \\ &= \sum_{\substack{i=1, \dots, n \\ j=1, \dots, m}} l_i \cdot r_j \end{aligned}$$

0.44 (D)

Eine DVAG $((L, +), (R, +), (A, +), \cdot)$ heißt

- (a) *nullteilerfrei*, wenn aus $l \cdot r = 0_a$ stets $\{l, r\} \cap \{0_L, 0_R\} \neq \{\}$ folgt.
- (b) *kommutativ oder abelsch*, wenn $(L, +) = (R, +)$ und für alle $a, b \in R$ $ab = ba$ gilt.

0.45 (B)

- (a) Jeder Körper $(K, +, \cdot)$ ist ein nullteilerfreier Ring mit Einselement.

Beweis $(K, +, \cdot)$ ist ein Körper, dann ist $((K \setminus 0_K), \cdot)$ eine Gruppe und es folgt

- (1) Für alle $a, b \in K \setminus \{0\}$ gilt $ab \in K \setminus \{0\}$, d.h. $(K, +, \cdot)$ ist nullteilerfrei.
 - (2) $(K \setminus \{0\}, \cdot)$ besitzt ein Einselement 1_K , d.h. es gilt $1_K \cdot a = a = a \cdot 1_K$ für alle $a \in K \setminus \{0\}$ und für alle $a = 0_K$ gilt ebenfalls $1_K \cdot 0_K = 0_K = 0_K \cdot 1_K$, also gilt $1_K \cdot a = a = a \cdot 1_K$ für alle $a \in K$, damit ist 1_K Einselement von $(K, +, \cdot)$.
 - (3) $(ab)c = a(bc)$ für alle $a, b, c \in K \setminus \{0\}$ und im Fall $0_K \in \{a, b, c\}$ gilt $a(bc) = 0_K = (ab)c$; somit ist (K, \cdot) eine Halbgruppe, damit ist $(K, +, \cdot)$ nach Definition ein Ring.
- (b) $(\mathbb{Z}, +, \cdot)$ ist ein nullteilerfreier Ring mit Einselement, aber *kein* Körper.
- (c) Im Ring $(\mathbb{R}^{2 \times 2}, +, \cdot)$ der 2×2 -Matrizen gilt $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, aber $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$, d.h. $(\mathbb{R}^{2 \times 2}, +, \cdot)$ ist nicht nullteilerfrei.

0.46 (A)

Beweise: Jeder *endliche, nullteilerfreie* Ring ist ein Körper.

Lösung

- – Sei $(R, +, \cdot)$ ein endlicher, nullteilerfreier Ring.
 - Sei $R \setminus \{0\} := \{a_1, a_2, \dots, a_n\} =: R^x$. Dann ist $(R \setminus \{0\}, \cdot) =: (R^x, \cdot)$ eine Gruppe.
 - Da $(R, +, \cdot)$ nullteilerfrei ist, folgt $a \cdot b \in R^x$ für alle $a, b \in R^x$, d.h. (R^x, \cdot) ist Untergruppoid von (R, \cdot) .
 - Weiter ist $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ für alle $a, b \in R$, somit auch für alle $a, b \in R^x$. Es folgt, daß (R^x, \cdot) Halbgruppe ist.
- Seien $a, b \in R^x$ beliebig, dann aber fest vorgeben.
- Betrachte die Abbildung $\varphi_a : \begin{cases} R^x \rightarrow R^x \\ a_i \mapsto \varphi_a(a_i) := a \cdot a_i \end{cases}$.
- Angenommen, unter der Voraussetzung $a \neq 0$ sei $a \cdot a_i = a \cdot a_j$, dann ist $a \cdot (a_i - a_j) = a \cdot a_i - a \cdot a_j = 0 \rightsquigarrow a_i - a_j = 0 \rightsquigarrow a_i = a_j$, d.h. φ_a ist injektiv.

- Da $|R^x| = n < \infty$, muss φ_a auch surjektiv sein, d.h. $\exists a_i \in R^x : a \cdot a_i = b$, womit die Gleichung $a \cdot x = b$ in (R^x, \cdot) lösbar ist.
- Analog gilt: Die Abbildung $\psi_a : \begin{cases} R^x \rightarrow R^x \\ a_i \mapsto \psi_a(a_i) := a_i \cdot a \end{cases}$ ist injektiv, wegen $|R^x| = n < \infty$ auch surjektiv, d.h. die Gleichung $y \cdot a = b$ ebenfalls in (R^x, \cdot) lösbar.

Damit ist (R^x, \cdot) eine Gruppe.

0.47 (S)

Ist $((R, +), (R, +), (A, +), \cdot)$ eine abelsche DVAG, so gilt für alle $a, b \in R$ die Formel $(a + b)^2 = a^2 + 2ab + b^2$.

Beweis Ist $((R, +), (R, +), (A, +), \cdot)$ eine abelsche DVAG, so gilt für alle $a, b \in R$

$$a + b =: n \in R$$

und

$$\begin{aligned} (a + b)^2 &= (a + b)(a + b) = n(a + b) = na + nb \\ &= (a + b)a + (a + b)b = (aa + ba) + (ab + bb) \\ &= a^2 + (ba + ab) + b^2 = a^2 + 2ab + b^2 \end{aligned}$$

0.48 (A)

Zeige: Sei $(R, +, \cdot)$ ein kommutativer Ring. Setze $a^n b^0 := a^n$ und $a^0 b^n := b^n$, dann gilt für alle $(a, b, n) \in R \times R \times \mathbb{N}$ die *binomische Formel*

$$(*) \quad (a + b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k \quad \text{mit} \quad \binom{n}{k} := \frac{n \cdot (n-1) \cdot \dots \cdot (n-k+1)}{1 \cdot 2 \cdot \dots \cdot k}$$

für alle $k > 0$ und $\binom{n}{0} := 1$.

Lösung

Vorüberlegung Für alle $n \in \mathbb{N}$ gilt:

$$(a) \quad \binom{n}{0} = 1 = \binom{n+1}{0} \quad \text{und} \quad \binom{n}{n} = 1 = \binom{n+1}{n+1}$$

$$(b) \quad \binom{n}{1} + \binom{n}{0} = n + 1 = \binom{n+1}{1}$$

(c) Für $k > 1$ gilt

$$\begin{aligned} &\binom{n}{k} + \binom{n}{k-1} \\ &= \frac{n(n-1) \dots (n-k+1)}{k!} + \frac{n(n-1) \dots (n-k+2)}{(k-1)!} \\ &= \frac{n(n-1) \dots (n-k+2)[(n-k+1) + k]}{k!} \\ &= \frac{(n+a)((n+1)-1)((n+1)-2) \dots ((n+1)-k+1)}{k!} \\ &= \binom{n+1}{k} \end{aligned}$$

Beweis

- Setze $\{n \in \mathbb{N} \mid \text{Für alle } a, b \in \mathbb{R} \text{ gilt } (*)\} =: S$.
Dann ist $(a+b)^1 = a+b = \binom{1}{0}a^{1-0}b^0 + \binom{1}{1}a^{1-1}b^1$ und es folgt $1 \in S$.
- Sei ein $n \in S$ beliebig vorgegeben. Dann ist

$$\begin{aligned}
& (a+b)^{n+1} \\
&= (a+b)^n(a+b) \\
&= \left(\sum_{k=0}^n \binom{n}{k} a^{n-k} b^k \right) (a+b) \\
&= \binom{n}{0} a^{n+1} b^0 + \binom{n}{1} a^n b^1 + \binom{n}{2} a^{n-1} b^2 + \dots + \binom{n}{n-1} a^2 b^{n-1} \\
&\quad + \binom{n}{n} a^1 b^n + \binom{n}{0} a^n b^1 + \binom{n}{1} a^{n-1} b^2 + \dots \\
&\quad + \binom{n}{n-2} a^2 b^{n-1} + \binom{n}{n-1} a^1 b^n + \binom{n}{n} a^0 b^{n+1} \\
&= \binom{n}{0} a^{n+1} b^0 + \left(\binom{n}{1} + \binom{n}{0} \right) a^n b^1 + \left(\binom{n}{2} + \binom{n}{1} \right) a^{n-1} b^2 \\
&\quad + \dots + \left(\binom{n}{n-1} + \binom{n}{n-2} \right) a^2 b^{n-1} \\
&\quad + \left(\binom{n}{n} + \binom{n}{n-1} \right) a^1 b^n + \binom{n}{n} a^0 b^{n+1} \\
&= \binom{n+1}{0} a^{(n+1)-0} b^0 + \binom{n+1}{n} a^{(n+1)-1} b^1 + \binom{n+1}{2} a^{(n+1)-2} b^2 \\
&\quad + \dots + \binom{n+1}{n-1} a^{(n+1)-(n-1)} b^{n-1} + \binom{n+1}{n} a^{(n+1)-n} b^n \\
&\quad + \binom{n+1}{n+1} a^{(n+1)-(n+1)} b^{n+1} \\
&= \sum_{k=0}^{n+1} \binom{n+1}{k} a^{(n+1)-k} b^k
\end{aligned}$$

Damit ist $n+1 \in S$ für alle $n \in S$

Nach dem Prinzip der vollständigen Induktion folgt $S = \mathbb{N}$.

0.49 (D)

Es seien S eine Menge und $m, n \in \mathbb{N}$.

- (a) Dann heißt jedes in der Form von m Zeilen und n Spalten angeordnete System

$$\begin{pmatrix} S_{11} & \dots & S_{1j} & \dots & S_{1n} \\ \vdots & & \vdots & & \vdots \\ S_{i1} & \dots & S_{ij} & \dots & S_{in} \\ \vdots & & \vdots & & \vdots \\ S_{m1} & \dots & S_{mj} & \dots & S_{mn} \end{pmatrix}$$

von $m \cdot n$ vielen Elementen aus S eine $m \times n$ -Matrix über S .

Die Gesamtheit aller $m \times n$ -Matrizen über S wir mit $S^{m \times n}$ bezeichnet.

Für $S^{1 \times n}$ wird auch kürzer $S^{1 \times n} := S^n : \{(S_1 \dots S_n) \mid S_1, S_2, \dots, S_n \in S\}$ geschrieben.

(b) Ist $\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} =: A \in S^{m \times n}$, so heißt $\begin{pmatrix} b_{11} & \dots & b_{1n} \\ \vdots & & \vdots \\ b_{m1} & \dots & b_{mn} \end{pmatrix} =: B \in S^{m \times n}$ mit $b_{ij} = a_{ji}$ für alle $(i, j) \in m \times n := \{(i, j) \mid 1 \leq i \leq n \text{ und } 1 \leq j \leq m\}$ die zu A transponierte Matrix – in Zeichen $B =: A^t$.

(c) Zwei Matrizen $A, B \in S^{m \times n}$ heißen gleich – in Zeichen $A = B$, wenn für alle $(i, j) \in m \times n$ gilt $a_{ij} = b_{ij}$.

0.50 (S)

Ist $(S, +)$ eine abelsche Gruppe, so ist auch $(S^{m \times n}, +)$ mit

$$A + B := \begin{pmatrix} a_{11} + b_{11} & \dots & a_{1n} + b_{1n} \\ \vdots & & \vdots \\ a_{m1} + b_{m1} & \dots & a_{mn} + b_{mn} \end{pmatrix} \in S^{m \times n}$$

ebenfalls eine abelsche Gruppe mit $\begin{pmatrix} 0 & \dots & 0 \\ \vdots & & \vdots \\ 0 & \dots & 0 \end{pmatrix} \in S^{m \times n}$ als neutralem Element

und $\begin{pmatrix} -a_{11} & \dots & -a_{1n} \\ \vdots & & \vdots \\ -a_{m1} & \dots & -a_{mn} \end{pmatrix} =: A^{-1}$ als der Inversen zu $\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} =: A \in S^{m \times n}$.

Beweis Seien $A := \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$ und $B := \begin{pmatrix} b_{11} & \dots & b_{1n} \\ \vdots & & \vdots \\ b_{m1} & \dots & b_{mn} \end{pmatrix} \in S^{m \times n}$

beliebig vorgegeben.

• $A + B = \begin{pmatrix} d_{11} & \dots & d_{1n} \\ \vdots & & \vdots \\ d_{m1} & \dots & d_{mn} \end{pmatrix} \in S^{m \times n}$ mit $d_{ij} = a_{ij} + b_{ij}$ ist für alle $(i, j) \in m \times n$ eindeutig definiert, d.h. $(S^{m \times n}, +)$ ist Gruppoid.

• $B + A = \begin{pmatrix} e_{11} & \dots & e_{1n} \\ \vdots & & \vdots \\ e_{m1} & \dots & e_{mn} \end{pmatrix} \in S^{m \times n}$ mit $e_{ij} = b_{ij} + a_{ij} = a_{ij} + b_{ij}$ ($(S, +)$ ist abelsch) für alle $(i, j) \in m \times n$.

• $\rightsquigarrow A + B = B + A \rightsquigarrow (S^{m \times n}, +)$ ist abelsch.

0.51 (S+D)

Seien $((L, +), (R, +), (A, +), \cdot)$ eine DVAG, $m, n, k \in \mathbb{N}$

und $\begin{pmatrix} l_{11} & \dots & l_{1n} \\ \vdots & & \vdots \\ l_{m1} & \dots & l_{mn} \end{pmatrix} =: U \in L^{m \times n}$, $\begin{pmatrix} r_{11} & \dots & r_{1k} \\ \vdots & & \vdots \\ r_{n1} & \dots & r_{nk} \end{pmatrix} =: V \in R^{n \times k}$.

Setzt man für alle $(i, k) \in m \times k$

$$a_{ij} = \sum_{\nu=1}^n l_{i\nu} r_{\nu j}$$

so gilt²

$$UV = \begin{pmatrix} a_{11} & \dots & a_{1k} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mk} \end{pmatrix} \in A^{m \times k}$$

und es ist $((L^{m \times n}, +), (R^{n \times k}, +), (A^{m \times k}, +), \cdot)$ ebenfalls eine DVAG.

$((L^{m \times n}, +), (R^{n \times k}, +), (A^{m \times k}, +), \cdot)$ heißt die *Matrizen-DVAG vom Typ (m, n, k) über der DVAG $((L, +), (R, +), (A, +), \cdot)$* .

Beweis Seien eine DVAG $((L, +), (R, +), (A, +), \cdot)$ und $m, n, k \in \mathbb{N}$ beliebig vorgegeben. Dann sind nach (0.50) $((L^{m \times n}, +), (R^{n \times k}, +), (A^{m \times k}, +), \cdot)$ abelsche Gruppen.

- Seien $\begin{pmatrix} l_{11} & \dots & l_{1n} \\ \vdots & & \vdots \\ l_{m1} & \dots & l_{mn} \end{pmatrix} =: U \in L^{m \times n}$, $\begin{pmatrix} r_{11} & \dots & r_{1k} \\ \vdots & & \vdots \\ r_{n1} & \dots & r_{nk} \end{pmatrix} =: V \in R^{n \times k}$ und $(i, j) \in m \times k$ beliebig, dann aber fest vorgegeben.
- Es gilt $l_{i\nu} r_{\nu j} \in A$ für $\nu = 1, 2, \dots, n$ und es folgt, da $(A, +)$ abelsche Gruppe ist

$$a_{ij} = \sum_{\nu=1}^n l_{i\nu} r_{\nu j} \in A$$

für alle $(i, j) \in m \times k$.

- Damit ist $UV = \begin{pmatrix} a_{11} & \dots & a_{1k} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mk} \end{pmatrix} \in A^{m \times k}$ eindeutig definiert.
- $\cdot : \begin{cases} L^{m \times n} \times R^{n \times k} \rightarrow A^{m \times k} \\ (U, V) \mapsto UV =: W \end{cases}$ mit

$$w_{ij} = \sum_{\nu=1}^n l_{i\nu} r_{\nu j} \quad \text{für alle } (i, j) \in m \times k$$

ist eindeutig definierte Abbildung von $L^{m \times n} \times R^{n \times k}$ nach $A^{m \times k}$.

Um zu beweisen, daß die o.g. Vorschrift eine DVAG bestimmt, muß man nun die beiden Distributivgesetze aus (0.39) (a) gelten. Wir zeigen zunächst $[\text{Dist}]_L$:

²Merkregel: Man sagt auch „ a_{ij} = i-te Zeile von U mal j-te Spalte von V“.

- Seien $\begin{pmatrix} l_{11} & \dots & l_{1n} \\ \vdots & & \vdots \\ l_{m1} & \dots & l_{mn} \end{pmatrix} =: U$, $\begin{pmatrix} l'_{11} & \dots & l'_{1n} \\ \vdots & & \vdots \\ l'_{m1} & \dots & l'_{mn} \end{pmatrix} =: U' \in L^{m \times n}$ und $\begin{pmatrix} r_{11} & \dots & r_{1k} \\ \vdots & & \vdots \\ r_{n1} & \dots & r_{nk} \end{pmatrix} =: V \in R^{n \times k}$ beliebig vorgegeben.

- $UV := X = \begin{pmatrix} x_{11} & \dots & x_{1k} \\ \vdots & & \vdots \\ x_{m1} & \dots & x_{mk} \end{pmatrix} \in A^{m \times k}$ mit $x_{ij} = \sum_{\nu=1}^n l_{i\nu} r_{\nu j}$ für alle $(i, j) \in m \times k$

- $U'V := X' = \begin{pmatrix} x'_{11} & \dots & x'_{1k} \\ \vdots & & \vdots \\ x'_{m1} & \dots & x'_{mk} \end{pmatrix} \in A^{m \times k}$ mit $x'_{ij} = \sum_{\nu=1}^n l'_{i\nu} r_{\nu j}$ für alle $(i, j) \in m \times k$

- $X + X' := W = \begin{pmatrix} w_{11} & \dots & w_{1k} \\ \vdots & & \vdots \\ w_{m1} & \dots & w_{mk} \end{pmatrix} \in A^{m \times k}$ mit

$$\begin{aligned} w_{ij} &= x_{ij} + x'_{ij} = \left(\sum_{\nu=1}^n l_{i\nu} r_{\nu j} \right) + \left(\sum_{\nu=1}^n l'_{i\nu} r_{\nu j} \right) \\ &= \sum_{\nu=1}^n (l_{i\nu} r_{\nu j} + l'_{i\nu} r_{\nu j}) = \sum_{\nu=1}^n (l_{i\nu} + l'_{i\nu}) r_{\nu j} \end{aligned}$$

für alle $(i, j) \in m \times k$.

- Nach (0.50) ist $U + U' =: Y = \begin{pmatrix} y_{11} & \dots & y_{1n} \\ \vdots & & \vdots \\ y_{m1} & \dots & y_{mn} \end{pmatrix} \in L^{m \times n}$ mit $y_{i\nu} = l_{i\nu} + l'_{i\nu}$ für alle $(i, j) \in m \times n$.

- Es ist $YV =: Z = \begin{pmatrix} z_{11} & \dots & z_{1k} \\ \vdots & & \vdots \\ z_{m1} & \dots & z_{mk} \end{pmatrix} \in A^{m \times k}$ mit

$$z_{ij} = \sum_{\nu=1}^n y_{i\nu} r_{\nu j} = \sum_{\nu=1}^n (l_{i\nu} + l'_{i\nu}) r_{\nu j} = w_{ij}$$

für alle $(i, j) \in m \times k$.

- Damit folgt $Z = W$.
- Resümee $(U + U')V = YV = Z = W = X + x' = UV + U'V$.

In $((L^{m \times n}, +), (R^{n \times k}, +), (A^{m \times k}, +), \cdot)$ gilt $[\text{Dist}]_L$.

Analog zeigt man, daß auch $[\text{Dist}]_R$ gilt, damit ist $((L^{m \times n}, +), (R^{n \times k}, +), (A^{m \times k}, +), \cdot)$ ebenfalls eine DVAG.

0.52 (S)

Ist $(R, +, \cdot)$ ein verallgemeinerter Ring, und $n \in \mathbb{N}$, so ist

$$((R^{n \times n}, +), (R^{n \times n}, +), (R^{n \times n}, +), \cdot) =: (R^{n \times n}, +, \cdot)$$

ebenfalls ein verallgemeinerter Ring.

Beweis Dieser Satz ist ein Korollar von (0.51) für $m = n = k$ und $(L, +) = (R, +) = (A, +)$.

0.53 (S)

Ist $(R, +, \cdot)$ ein Ring, so gilt für alle $k, l, m, n \in \mathbb{N}$ und alle $U = \begin{pmatrix} u_{11} & \dots & u_{1l} \\ \vdots & & \vdots \\ u_{kl} & \dots & u_{kl} \end{pmatrix} \in R^{k \times l}$, $V = \begin{pmatrix} v_{11} & \dots & v_{1m} \\ \vdots & & \vdots \\ v_{l1} & \dots & v_{lm} \end{pmatrix} \in R^{l \times m}$, $W = \begin{pmatrix} w_{11} & \dots & w_{1n} \\ \vdots & & \vdots \\ w_{m1} & \dots & w_{mn} \end{pmatrix} \in R^{m \times n}$:

$$(UV)W = U(VW)$$

Beweis

- Laut (0.51) ist $UV := X = \begin{pmatrix} x_{11} & \dots & x_{1m} \\ \vdots & & \vdots \\ x_{kl} & \dots & x_{km} \end{pmatrix} \in R^{k \times m}$ mit $x_{i\mu} = \sum_{\lambda=1}^l u_{i\lambda} v_{\lambda\mu}$ für alle $(i, \mu) \in k \times m$.

- $XW =: Y = \begin{pmatrix} y_{11} & \dots & y_{1n} \\ \vdots & & \vdots \\ y_{kl} & \dots & y_{kn} \end{pmatrix} \in R^{k \times n}$ mit

$$\begin{aligned} y_{ij} &= \sum_{\mu=1}^m x_{i\mu} w_{\mu j} = \sum_{\mu=1}^m \left(\sum_{\lambda=1}^l u_{i\lambda} v_{\lambda\mu} \right) w_{\mu j} \\ &= \sum_{\substack{\lambda=1, \dots, l \\ \mu=1, \dots, m}} u_{i\lambda} v_{\lambda\mu} w_{\mu j} \end{aligned}$$

für alle $(i, j) \in k \times n$.

- Es ist $VW =: Z = \begin{pmatrix} z_{11} & \dots & z_{1n} \\ \vdots & & \vdots \\ z_{l1} & \dots & z_{ln} \end{pmatrix} \in R^{l \times n}$ mit $z_{\lambda j} = \sum_{\mu=1}^m v_{\lambda\mu} w_{\mu j}$ für alle $(\lambda, j) \in l \times n$.

$$\begin{aligned}
\bullet \quad UZ &=: T = \begin{pmatrix} t_{11} & \dots & t_{1n} \\ \vdots & & \vdots \\ t_{k1} & \dots & t_{kn} \end{pmatrix} \in R^{k \times n} \text{ mit} \\
t_{ij} &= \sum_{\lambda=1}^l u_{i\lambda} z_{\lambda j} = \sum_{\lambda=1}^l u_{i\lambda} \left(\sum_{\mu=1}^m v_{\lambda\mu} w_{\mu j} \right) \\
&= \sum_{\substack{\lambda=1, \dots, l \\ \mu=1, \dots, m}} u_{i\lambda} (v_{\lambda\mu} w_{\mu j}) = \sum_{\substack{\lambda=1, \dots, l \\ \mu=1, \dots, m}} u_{i\lambda} v_{\lambda\mu} w_{\mu j} = y_{ij}
\end{aligned}$$

für alle $(i, j) \in k \times n$.

Damit haben wir: $Y = T \rightsquigarrow (UV)W = XW = Y = T = UZ = U(VW)$.

0.54 (B)

Für $(1\ 2\ 3) =: a \in \mathbb{R}^{1 \times 3}$, $\begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix} =: b \in \mathbb{R}^{3 \times 1}$, $(2) =: c \in \mathbb{R}^{1 \times 1}$ und

$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} =: d \in \mathbb{R}^{3 \times 3}$ gilt:

(a) $ab = 1 \cdot 4 + 2 \cdot 5 + 3 \cdot 6 = (32) \in \mathbb{R}^{1 \times 1}$

(b) $ba = (1\ 2\ 3) \begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix} = \begin{pmatrix} 4 & 8 & 12 \\ 5 & 10 & 15 \\ 6 & 12 & 18 \end{pmatrix} \in \mathbb{R}^{3 \times 3}$

(c) $(ab)c = (32)(2) = (64) \in \mathbb{R}^{1 \times 1}$

(d) $a(bc) = (1\ 2\ 3) \left(\begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix} (2) \right) = (1\ 2\ 3) \begin{pmatrix} 8 \\ 10 \\ 12 \end{pmatrix} = 8 + 20 + 36 = (64) \in \mathbb{R}^{1 \times 1}$

0.55 (S)

Ist $((K, +), (K, +), (A, +), \cdot)$ eine kommutative DVAG und $((K^{l \times m}, +), (K^{m \times n}, +), (A^{l \times n}, +), \cdot)$ die zugehörige Matrizen-DVAG vom Typ (l, m, n) ,

so gilt für alle $U := \begin{pmatrix} u_{11} & \dots & u_{1m} \\ \vdots & & \vdots \\ u_{l1} & \dots & u_{lm} \end{pmatrix} \in K^{l \times m}$ und $V := \begin{pmatrix} v_{11} & \dots & v_{1n} \\ \vdots & & \vdots \\ v_{m1} & \dots & v_{mn} \end{pmatrix} \in K^{m \times n}$:

$$(U \cdot V)^t = V^t \cdot U^t$$

Beweis

• Laut (0.51) gilt $U \cdot V =: C = \begin{pmatrix} c_{11} & \dots & c_{1n} \\ \vdots & & \vdots \\ c_{l1} & \dots & c_{ln} \end{pmatrix} \in A^{l \times n}$ mit

$$c_{ji} = \sum_{\mu=1}^m u_{i\mu} v_{\mu j}$$

für alle $(j, i) \in l \times n$.

- Laut (0.49)(b) gilt $(U \cdot V)^t =: D = \begin{pmatrix} d_{11} & \dots & d_{1l} \\ \vdots & & \vdots \\ d_{n1} & \dots & d_{nl} \end{pmatrix} \in A^{n \times l}$ mit $d_{ij} = c_{ji}$ für alle $(i, j) \in n \times l$.
- Weiterhin gilt laut (0.49)(b) $U^t =: F = \begin{pmatrix} f_{11} & \dots & f_{1l} \\ \vdots & & \vdots \\ f_{m1} & \dots & f_{ml} \end{pmatrix} \in K^{m \times l}$ mit $f_{\mu j} = u_{j\mu}$ für alle $(\mu, j) \in m \times l$ und $V^t =: G = \begin{pmatrix} g_{11} & \dots & g_{1m} \\ \vdots & & \vdots \\ g_{n1} & \dots & g_{nm} \end{pmatrix} \in K^{n \times m}$ mit $g_{i\mu} = v_{\mu i}$ für alle $(i, \mu) \in n \times m$.
- $V^t \cdot U^t =: W = \begin{pmatrix} w_{11} & \dots & w_{1l} \\ \vdots & & \vdots \\ w_{n1} & \dots & w_{nl} \end{pmatrix} \in A^{n \times l}$ mit

$$w_{ij} = \sum_{\mu=1}^m g_{i\mu} f_{\mu j} = \sum_{\mu=1}^m v_{\mu i} u_{j\mu} = \sum_{\mu=1}^m u_{j\mu} v_{\mu i} = c_{ji} = d_{ij}$$
 für alle $(i, j) \in n \times l$
- Damit hat man $W = D$ und es folgt $(U \cdot V)^t = D = W = V^t \cdot U^t$.

0.56 (S)

Ist $(R, +, \cdot)$ ein verallgemeinerter Ring, $n \in \mathbb{N}$ und $(R^{n \times n}, +, \cdot)$ der verallgemeinerte Ring der $n \times n$ -Matrizen (siehe (0.51)), so gilt:

- (a) Ist $(R, +, \cdot)$ ein Ring, so ist auch $(R^{n \times n}, +, \cdot)$ ein Ring.
- (b) Ist $(R, +, \cdot)$ ein Ring mit Einselement 1_R , so ist auch $(R^{n \times n}, +, \cdot)$ ein Ring mit Einselement. Es ist $1_{R^{n \times n}} = \begin{pmatrix} 1_R & & 0 \\ & \ddots & \\ 0 & & 1_R \end{pmatrix} \in R^{n \times n}$.
- (c) $(A \cdot B)^t = B^t \cdot A^t$ für alle $A, B \in R^{n \times n}$, falls $(R, +, \cdot)$ ein kommutativer Ring ist.

Beweis

- (a) Ist $(R, +, \cdot)$ ein Ring, dann folgt nach (0.53) mit $k = l = m = n$: Für alle $U \in R^{n \times n}, V \in R^{n \times n}, W \in R^{n \times n}$ gilt $(U \cdot V) \cdot W = U \cdot (V \cdot W)$.

- (b) Ist $(R, +, \cdot)$ ein Ring mit Einselement 1_R und $E_n := \begin{pmatrix} \delta_{11} & \dots & \delta_{1n} \\ \vdots & & \vdots \\ \delta_{n1} & \dots & \delta_{nn} \end{pmatrix} \in R^{n \times n}$

die durch $\delta_{ij} := \begin{cases} 1_R & \text{falls } i = j \\ 0_R & \text{falls } i \neq j \end{cases}$ definierte Matrix, so gilt für alle $U :=$

$$\begin{pmatrix} u_{11} & \dots & u_{1n} \\ \vdots & & \vdots \\ u_{n1} & \dots & u_{nn} \end{pmatrix} \in R^{n \times n}$$

$$(1) \quad U \cdot E_n = \begin{pmatrix} v_{11} & \dots & v_{1n} \\ \vdots & & \vdots \\ v_{n1} & \dots & v_{nn} \end{pmatrix} \in R^{n \times n} \text{ mit}$$

$$v_{ij} = \sum_{\nu=1}^n u_{i\nu} \delta_{\nu j} = u_{ij} \delta_{jj} = u_{ij} 1_R = u_{ij}$$

für alle $(i, j) \in n \times n \rightsquigarrow U \cdot E_n = U$.

$$(2) \quad E_n \cdot U = \begin{pmatrix} w_{11} & \dots & w_{1n} \\ \vdots & & \vdots \\ w_{n1} & \dots & w_{nn} \end{pmatrix} \in R^{n \times n} \text{ mit}$$

$$w_{ij} = \sum_{\nu=1}^n \delta_{i\nu} u_{\nu j} = \delta_{ii} u_{ij} = 1_R u_{ij} = u_{ij}$$

für alle $(i, j) \in n \times n \rightsquigarrow E_n \cdot U = U$.

(c) Ist $(R, +, \cdot)$ ein kommutativer Ring, so folgt aus (0.55) mit $l = m = n$: $(U \cdot V)^t = V^t \cdot U^t$ für alle $U, V \in R^{n \times n}$.

0.57 (D)

Es sei $(K, +, \cdot)$ ein Körper mit $K = \{\alpha, \beta, \dots\}$, $(V, +)$ eine abelsche Gruppe mit $V = \{a, b, \dots\}$ und

$$((K, +), (V, +), (V, +), \cdot) =: {}_K V \quad \Bigg| \quad ((V, +), (K, +), (V, +), \cdot) =: V_K$$

eine DVAG, d.h. für alle

$$(\alpha, \beta, a, b) \in K \times K \times V \times V \text{ gelte}$$

$$\begin{array}{ll|ll} ({}_K V)(I) & (\alpha + \beta)a = \alpha a + \beta a & (V_K)(I) & a(\alpha + \beta) = a\alpha + a\beta \\ ({}_K V)(II) & \alpha(a + b) = \alpha a + \alpha b & (V_K)(II) & (a + b)\alpha = a\alpha + b\alpha \end{array}$$

Gelten darüberhinaus noch die folgenden Axiome:

$$\begin{array}{ll|ll} ({}_K V)(III) & (\alpha\beta)a = \alpha(\beta a) & (V_K)(III) & a(\alpha\beta) = (a\alpha)\beta \\ ({}_K V)(IV) & 1_K a = a & (V_K)(IV) & a 1_K = a \end{array}$$

so heißt

${}_K V$ ein *linker*

V_K ein *rechter*
 K -Vektorraum.

0.58 (S)

Jeder rechte oder linke K -Vektorraum ist eine nullteilerfreie DVAG.

Beweis Der Beweis ist kurz:

$$\begin{array}{l|l}
\text{Seien } (\alpha, a) \in K \times V \text{ mit} & \\
\alpha a = 0_V & a\alpha = 0_V \\
\text{beliebig vorgegeben. Angenommen } \alpha \neq 0, \text{ dann ist} & \\
a = 1_K a = (\alpha^{-1} \alpha) a & a = a 1_K = a(\alpha \alpha^{-1}) \\
= \alpha^{-1}(\alpha a) = \alpha^{-1} 0_V = 0_V & = (a\alpha) \alpha^{-1} = 0_V \alpha^{-1} = 0_V
\end{array}$$

0.59 (D)

(a) Ein linker oder rechter Vektorraum über dem Körper $(\mathbb{R}, +, \cdot)$ der reellen Zahlen heißt ein .

(b) Ist ${}_R V$ und $\circ : \begin{cases} V \times V \rightarrow \mathbb{R} \\ (a, b) \mapsto a \circ b \end{cases}$ eine Abbildung von $V \times V$ nach \mathbb{R} , die für alle $\alpha \in \mathbb{R}$ und $(a, b, c) \in V^3$ die Bedingungen

$$[E1] \quad a \circ b = b \circ a$$

$$[E2] \quad (a + b) \circ c = a \circ c + b \circ c$$

$$[E3] \quad (\alpha a) \circ b = \alpha(a \circ b)$$

$$[E4] \quad (a \circ a) =: a^2 > 0, \text{ falls } a \neq 0$$

erfüllt, so heißt das Paar $({}_R V, \circ)$ ein *Euklidischer Vektorraum* – kurz ein EVR.

Aus [E1] und [E2] folgt

$$a \circ (b + c) \stackrel{[E1]}{=} (b + c) \circ a \stackrel{[E2]}{=} b \circ a + c \circ a \stackrel{[E1]}{=} a \circ b + a \circ c$$

Mit diesen Festlegungen ergibt sich der folgende Satz.

0.60 (S)

Ist $({}_R V, \circ)$ ein EVR so ist $((V, +), (V, +), (\mathbb{R}, +), \cdot)$ eine kommutative DVAG. Wegen (0.47) gilt für alle $a, b \in V$ eines EVR

$$(a + b)^2 = a^2 + 2a \circ b + b^2$$

0.61 (B)

Sei ein $n \in \mathbb{N}$ beliebig vorgegeben. Setzt man für alle $\alpha \in \mathbb{R}$ und alle $(\alpha_1, \alpha_2, \dots, \alpha_n) =: a$ $(\beta_1, \beta_2, \dots, \beta_n) =: b \in \mathbb{R}^n$

- $a + b := (\alpha_1 + \beta_1, \alpha_2 + \beta_2, \dots, \alpha_n + \beta_n) \in \mathbb{R}^n$,
- $\alpha a := (\alpha \alpha_1, \alpha \alpha_2, \dots, \alpha \alpha_n) \in \mathbb{R}^n$,
- $a \circ b := (\alpha_1 \circ \beta_1, \alpha_2 \circ \beta_2, \dots, \alpha_n \circ \beta_n) \in \mathbb{R}^n$,

so stellt (\mathbb{R}^n, \circ) einen EVR dar. (\mathbb{R}^n, \circ) heißt der *kanonische n -dimensionale EVR*.

Nachweis

$$[E1] \quad a \circ b = \sum_{i=1}^n \alpha_i \beta_i = \sum_{i=1}^n \beta_i \alpha_i = b \circ a$$

$$[E2] \quad \begin{aligned} (a + b) \circ c &= \sum_{i=1}^n (\alpha_i + \beta_i) \circ \gamma_i \\ &= \sum_{i=1}^n (\alpha_i \circ \gamma_i + \beta_i \circ \gamma_i) = \sum_{i=1}^n \alpha_i \gamma_i + \sum_{i=1}^n \beta_i \gamma_i \\ &= a \circ c + b \circ c \end{aligned}$$

$$[E3] \quad \begin{aligned} (\alpha a) \circ b &= \sum_{i=1}^n (\alpha \alpha_i) \beta_i \\ &= \sum_{i=1}^n \alpha (\alpha_i \beta_i) = \alpha \sum_{i=1}^n (\alpha_i \beta_i) \\ &= \alpha (a \circ b) \end{aligned}$$

$$[E4] \quad \text{Angenommen } a \neq 0_{\mathbb{R}^n}, \text{ dann gibt es } i_0 \in \{1, 2, \dots, n\} : \alpha_{i_0} \neq 0 \leadsto \alpha_{i_0} > 0.$$

Es ist

$$a \circ a = \underbrace{\alpha_1^2}_{\geq 0} + \underbrace{\alpha_2^2}_{\geq 0} + \dots + \underbrace{\alpha_{i_0}^2}_{\geq 0} + \dots + \underbrace{\alpha_n^2}_{\geq 0} \geq \alpha_{i_0}^2 > 0$$

also $a \circ a > 0$.

0.62 (A)

Es sei $\mathbb{R}^\infty := \{(\alpha_1, \alpha_2, \dots) =: a \mid \alpha_1, \alpha_2, \dots \in \mathbb{R}\}$ die Menge alle reellen Zahlenfolgen. Setze

$$H := \{a \in \mathbb{R}^\infty \mid \sum_{i=1}^{\infty} \alpha_i^2 < \infty\}$$

Beweise: Setzt man für alle $a, b \in H$ und alle $\alpha \in \mathbb{R}$

- (a) $\alpha \cdot a := (\alpha \alpha_1, \alpha \alpha_2, \alpha \alpha_3, \dots)$,
- (b) $a + b := (\alpha_1 + \beta_1, \alpha_2 + \beta_2, \dots)$ und
- (c) $\sum_{i=1}^{\infty} \alpha_i \beta_i$,

so ist $((\mathbb{R}, +), (H, +), (H, +), \cdot) =: {}_{\mathbb{R}}H$ ein Vektorraum und $({}_{\mathbb{R}}H, \circ)$ ein EVR. (Bemerkung: $({}_{\mathbb{R}}H, \circ)$ heißt *Hilbertraum*).

Lösung

Zeige zunächst, daß $((\mathbb{R}, +), (H, +), (H, +), \cdot) = {}_{\mathbb{R}}H$ ein Vektorraum ist.

- Seien $\alpha, \beta \in \mathbb{R}$ und $a, b, c \in H$ beliebig vorgegeben.
Dann sind $\alpha a, a + b \in \mathbb{R}^\infty$.
- *Problem:* $\alpha a, a + b \in H$?
- Für $x = (\xi_1, \xi_2, \dots) \in \mathbb{R}^\infty$ gilt

$$\xi_1^2 =: x_1 \leq \xi_1^2 + \xi_2^2 =: x_2 \leq \dots \leq \sum_{\nu=1}^n \xi_\nu^2 =: x_n$$

Damit gibt es ein $x \in H \Leftrightarrow \exists x \in \mathbb{R} : x_n \leq x$ für alle $n \in \mathbb{N}$.

- Es ist

$$(\alpha \alpha_1)^2 + (\alpha \alpha_2)^2 + \dots + (\alpha \alpha_n)^2 = \alpha^2 \sum_{\nu=1}^n \alpha_\nu^2 \leq \alpha^2 A$$

für alle $n \in \mathbb{N}$. Damit ist $\alpha a \in H$ (A ist eine obere Schranke).

- Für alle $n \in \mathbb{N}$ gilt:

$$\begin{aligned}
 & (\alpha_1 + \beta_1)^2 + (\alpha_2 + \beta_2)^2 + \dots + (\alpha_n + \beta_n)^2 \\
 &= \sum_{\nu=1}^n \alpha_\nu^2 + 2 \sum_{\nu=1}^n (\alpha_\nu \beta_\nu) + \sum_{\nu=1}^n \beta_\nu^2 \\
 &\leq A + 2 \sum_{\nu=1}^n |\alpha_\nu \beta_\nu| + B
 \end{aligned}$$

- Setze $\max\{|\alpha_\nu|, |\beta_\nu|\} = m_\nu$, dann ist $|\alpha_\nu \beta_\nu| = |\alpha_\nu| |\beta_\nu| \leq m_\nu^2 \leq \alpha_\nu^2 + \beta_\nu^2$.
Damit ist für alle $n \in \mathbb{N}$:

$$\begin{aligned}
 \sum_{\nu=1}^n (\alpha_\nu \beta_\nu) &\leq \sum_{\nu=1}^n (\alpha_\nu^2 \beta_\nu^2) = \sum_{\nu=1}^n \alpha_\nu^2 \sum_{\nu=1}^n \beta_\nu^2 \leq A + B \\
 &\leadsto \sum_{\nu=1}^n (\alpha_\nu \beta_\nu)^2 \leq 3(A + B)
 \end{aligned}$$

Damit ist $a + b \in H$ und somit auch $\underbrace{(a+b)}_{\in H} + \underbrace{c}_{\in H}, \underbrace{a}_{\in H} + \underbrace{(b+c)}_{\in H} \in H$.

- *Problem:* $(a + b) + c = a + (b + c)$?
- Setzt man für alle $x = \{\xi_1, \xi_2, \dots\} \in \mathbb{R}^\infty$ und für alle $\nu \in \mathbb{N} : \varphi_\nu(x) = \xi_\nu$, so gilt $x = x'$ genau dann, wenn $\varphi_\nu(x) = \varphi_\nu(x')$ für alle $\nu \in \mathbb{N}$ gilt.
- Da $(\mathbb{R}, +)$ assoziativ ist, gilt für alle $\nu \in \mathbb{N}$

$$\begin{aligned}
 \varphi_\nu((a + b) + c) &= (\alpha_\nu + \beta_\nu) + \gamma_\nu \\
 &= \alpha_\nu + (\beta_\nu + \gamma_\nu) = \varphi_\nu(a + (b + c)) \\
 &\leadsto (a + b) + c = a + (b + c)
 \end{aligned}$$

- Da $(\mathbb{R}, +)$ kommutativ ist, folgt weiter:

$$\begin{aligned}
 \varphi_\nu(a + b) &= \alpha_\nu + \beta_\nu = \beta_\nu + \alpha_\nu = \varphi_\nu(b + a) \quad \forall \nu \in \mathbb{N} \\
 &\leadsto a + b = b + a
 \end{aligned}$$

- Für $(0, 0, \dots) =: 0 \in H$ gilt $\varphi_\nu(a + 0) = \alpha_\nu + 0 = \alpha_\nu = \varphi_\nu(a) \quad \forall \nu \in \mathbb{N}$. Damit ist $a + 0 = a$.
- Für $(-\alpha_1, -\alpha_2, \dots) \in \mathbb{R}^\infty$ gilt $\sum_{\nu=1}^n \alpha_\nu^2 < A \quad \forall n \in \mathbb{N}$.
Daraus folgt $-a \in H$ und $\varphi_\nu(a + (-a)) = \alpha_\nu + (-\alpha_\nu) = 0 = \varphi_\nu(0)$ für alle $\nu \in \mathbb{N} \leadsto a + (-a) = 0$
- Damit ist $(H, +)$ abelsche Gruppe:
 $\alpha a, \beta a, (\alpha + \beta)a \in H$ und $\alpha a + \beta a \in H$
- Es ist $\varphi_\nu((\alpha + \beta)a) = (\alpha + \beta)\alpha_\nu = \alpha\alpha_\nu + \beta\alpha_\nu = \varphi_\nu(\alpha a + \beta a) \quad \forall \nu \in \mathbb{N}$. Damit ist $(\alpha + \beta)a = \alpha a + \beta a$.
- $\varphi_\nu(\alpha(a + b)) = \alpha(\alpha_\nu + \beta_\nu) = \alpha\alpha_\nu + \alpha\beta_\nu = \varphi_\nu(\alpha a + \alpha b) \quad \forall \nu \in \mathbb{N}$.
Es folgt $\alpha(a + b) = \alpha a + \alpha b$.
- $\varphi_\nu((\alpha\beta)a) = (\alpha\beta)\alpha_\nu = \alpha(\beta\alpha_\nu) = \varphi_\nu(\alpha(\beta a)) \quad \forall \nu \in \mathbb{N}$.
Damit ergibt sich $(\alpha\beta)a = \alpha(\beta a)$.

- $\varphi_\nu(1a) = 1\alpha_\nu = \alpha_\nu = \varphi_\nu(\alpha_\nu) \forall \nu \in \mathbb{N}$. Es folgt $1a = a$

Da die Gültigkeit aller Kriterien gezeigt wurde, ist $((\mathbb{R}, +), (H, +), (H, +), \cdot) =_{\mathbb{R}} H$ ein Vektorraum.

Problem: Ist $\sum_{\nu=1}^{\infty} \alpha_\nu \beta_\nu = a \circ b \in \mathbb{R}$?

- Setze $(\alpha_1, \alpha_2, \dots, \alpha_n) =: a_n$ für $n = 1, 2, \dots$ und $\sum_{\nu=1}^n \alpha_\nu \beta_\nu =: a_n \circ b_n$ dann ist nach Definition aus der Analysis $a \circ b = \lim_{n \rightarrow \infty} (a_n \circ b_n)$, falls $\lim_{n \rightarrow \infty} (a_n \circ b_n)$ existiert.
- Es ist

$$a_n \circ b_n = \sum_{\nu=1}^n \alpha_\nu \beta_\nu \leq \sum_{\nu=1}^n |\alpha_\nu \beta_\nu| \leq A + B$$

für alle $n \in \mathbb{N}$, d.h. $\sum_{\nu=1}^n \alpha_\nu \beta_\nu$ ist absolut konvergent.

- Aus der Analysis ist bekannt, daß $\sum_{\nu=1}^n \alpha_\nu \beta_\nu$ damit auch konvergent ist, d.h. es existiert $a \circ b$ und es gilt $a \circ b = \lim_{n \rightarrow \infty} (a_n \circ b_n)$.
- Für alle $n \in \mathbb{N}$ gilt $a_n \circ b_n = b_n \circ a_n \xrightarrow{[E1]} a \circ b = \lim_{n \rightarrow \infty} (a_n \circ b_n) = \lim_{n \rightarrow \infty} (b_n \circ a_n) = b \circ a$.
- [E2] $(\alpha a) \circ b = \lim_{n \rightarrow \infty} ((\alpha a_n) \circ b_n) = \alpha \lim_{n \rightarrow \infty} (a_n \circ b_n) = \alpha(a \circ b)$
- [E3] Es ist

$$\begin{aligned} (a + b) \circ c &= \lim_{n \rightarrow \infty} ((a_n + b_n) \circ c_n) = \lim_{n \rightarrow \infty} ((a_n \circ c_n) + (b_n \circ c_n)) \\ &= \lim_{n \rightarrow \infty} (a_n \circ c_n) + \lim_{n \rightarrow \infty} (b_n \circ c_n) \\ &= a \circ c + b \circ c \end{aligned}$$

- Für $a \neq 0 \exists m \in \mathbb{N} : \alpha_m \neq 0$, dann ist $\alpha_m^2 > 0$ und $a_n \circ a_n = \sum_{\nu=1}^n \alpha_\nu^2 \geq \alpha_m^2$ für alle $n \geq m$. Daraus folgt [E4] $a \circ a = \lim_{n \rightarrow \infty} (a_n \circ a_n) \geq \alpha_m^2 > 0$, falls $a \neq 0$.

Damit ist $(_{\mathbb{R}}H, \circ)$ ein EVR.

0.63 (A)

Es seien $-\infty < a < b < \infty$ reelle Zahlen und $C := C[a, b] := \{f \in \text{Abb}([a, b], \mathbb{R}) \mid f \text{ ist stetig}\}$.

Zeige: Setzt man für alle $(\alpha, f, g) \in \mathbb{R} \times C \times C$ und alle $x \in [a, b]$

- (a) $(\alpha \cdot f)(x) := \alpha \cdot f(x)$,
- (b) $(f + g)(x) := f(x) + g(x)$ und
- (c) $f \circ g := \int_a^b (f(x) \cdot g(x)) dx$,

so ist $((\mathbb{R}, +), (C, +), (C, +), \cdot) :=_{\mathbb{R}} C$ ein Vektorraum und $(_{\mathbb{R}}C, \circ)$ ein EVR.

Lösung

Seien $\alpha, \beta \in \mathbb{R}$ und $f, g, h \in C$ beliebig vorgegeben.

- f, g, h sind auf C stetig. Gemäß Analysis sind dann $\alpha f, \beta f, (\alpha + \beta)f, f + g$ und $g + h$ ebenfalls auf C stetig und für alle $x \in [a, b]$ gilt

$$\begin{aligned} ((\alpha + \beta)f)(x) &\stackrel{(a)}{=} (\alpha + \beta)f(x) = \alpha f(x) + \beta f(x) \\ &\stackrel{(a)}{=} (\alpha f)(x) + (\beta f)(x) \\ &\stackrel{(b)}{=} (\alpha f + \beta f)(x) \end{aligned}$$

Wir halten fest $(\alpha + \beta)f = \alpha f + \beta f$

- Es sind $\alpha(f + g) \in C$ und $\alpha f + \alpha g \in C$, weiterhin

$$\begin{aligned} (\alpha(f + g))(x) &\stackrel{(a)}{=} \alpha(f + g)(x) \\ &\stackrel{(b)}{=} \alpha(f(x) + g(x)) \\ &\stackrel{[\text{Dist}]}{=} \alpha f(x) + \alpha g(x) \\ &\stackrel{(a)}{=} (\alpha f)(x) + (\alpha g)(x) \\ &\stackrel{(b)}{=} (\alpha f + \alpha g)(x) \end{aligned}$$

Merke $(\alpha f + \alpha g) = \alpha(f + g)$

•

$$\begin{aligned} \overbrace{((f + g) + h)}^{\in C}(x) &\stackrel{(b)}{=} (f + g)(x) + h(x) \\ &\stackrel{(b)}{=} ((f(x) + g(x)) + h(x)) \\ &\stackrel{[\text{Dist}]}{=} f(x) + (g(x) + h(x)) \\ &\stackrel{(b)}{=} f(x) + ((g + h)(x)) \\ &\stackrel{(a)}{=} (f + (g + h))(x) \end{aligned}$$

Dementsprechend ist $(f + g) + h = f + (g + h)$

- $(f + g)(x) \stackrel{(b)}{=} f(x) + g(x) \stackrel{[\text{Komm}]}{=} g(x) + f(x) \stackrel{(b)}{=} (g + f)(x)$.
Somit ist $f + g = g + f$.

Bis hierher haben wir gezeigt, daß C eine abelsche Halbgruppe ist.

- Setze $\omega : \begin{cases} [a, b] \rightarrow \mathbb{R} \\ x \mapsto \omega(x) : 0_{\mathbb{R}} \end{cases}$, dann ist $\omega \in C$, $f + \omega \in C$ und für alle $x \in [a, b]$ gilt:

$$(f + \omega)(x) \stackrel{(b)}{=} f(x) + \omega(x) = f(x) + 0_{\mathbb{R}} = f(x)$$

Demzufolge ist $f + \omega = f$, und ω ist zweiseitig neutrales Element.

- Wegen $-1 \in \mathbb{R}$ gilt $(-1)f \in C$ und für alle $x \in [a, b]$ gilt

$$(f + (-1)f)(x) \stackrel{(b)}{=} f(x) + ((-1)f)(x) \stackrel{(a)}{=} f(x) + (-1)f(x) = 0_{\mathbb{R}}$$

Damit ist $f + (-1)f = \omega$ und (-1) ist Inverse.

Somit haben wir bis hierher gezeigt, daß $((\mathbb{R}, +), (C, +), (C, +), \cdot) =_{\mathbb{R}} C$ ein reeller Vektorraum ist.

- f, g sind auf dem Intervall $[a, b]$ stetig, damit ist (gemäß Analysis) auch $f(x) \cdot g(x) =: v(x)$ stetig auf $[a, b]$ und $\int_a^b (f(x)g(x))dx \stackrel{(c)}{=} f \circ g \in \mathbb{R}$ ist eindeutig definiert.

- Damit ist

$$\begin{aligned} (f + g) \circ h &\stackrel{(b)}{=} \int_a^b ((f + g)(x)h(x))dx \\ &= \int_a^b [f(x)h(x) + g(x)h(x)]dx \\ &\stackrel{\text{Analysis}}{=} \int_a^b (f(x)h(x))dx + \int_a^b (g(x)h(x))dx \\ &\stackrel{(c)}{=} f \circ h + g \circ h \end{aligned}$$

•

$$f \circ g \stackrel{(c)}{=} \int_a^b (f(x)g(x))dx \stackrel{(a)}{=} \int_a^b (g(x)f(x))dx \stackrel{(c)}{=} g \circ f$$

•

$$\begin{aligned} (\alpha f) \circ g &= \int_a^b ((\alpha f)(x)g(x))dx \stackrel{(a)}{=} \int_a^b ((\alpha f(x))g(x))dx \\ &= \alpha \int_a^b (f(x)g(x))dx \stackrel{(c)}{=} \alpha(f \circ g) \end{aligned}$$

- Sei $f \neq \omega$ $f \in C \setminus \{\omega\}$ beliebig vorgegeben. Dann existiert $x_0 \in (a, b)$ mit $f(x_0) \neq 0$. Sei $f^2(x_0) =: \varepsilon_0 > 0$.
- f^2 ist stetig auf $[a, b]$, daher existiert ein $\delta > 0$ mit $f^2(x) > \frac{\varepsilon_0}{2}$ in $[x_0 - \delta, x_0 + \delta]$.
- Setze $g(x) = \begin{cases} 0 & \forall [a, b] \setminus [x_0 - \delta, x_0 + \delta] \\ \frac{\varepsilon_0}{2} & \forall x \in [x_0 - \delta, x_0 + \delta] \end{cases}$. Dann kann man das Minorantenkriterium derart anwenden, daß folgt:

$$\begin{aligned} \int_a^b f^2(x)dx &\geq \int_a^b g(x)dx \\ &= \int_a^{x_0-\delta} g(x)dx + \int_{x_0-\delta}^{x_0+\delta} g(x)dx + \int_{x_0+\delta}^b g(x)dx \\ &= 0 + \frac{\varepsilon_0}{2} \cdot 2\delta + 0 \\ &= \varepsilon_0\delta > 0 \end{aligned}$$

- Also ist $f \circ f > 0$, falls $f \neq \omega$.

Demnach ist $(_{\mathbb{R}}C, \circ)$ ein EVR.

Kapitel 1

Affine Euklidische Geometrie

Aufgabenstellung: Wie kann man mit einer möglichst einleuchtenden Methode die anschaulich vorliegenden geometrischen Begriffe – wie Punkt, Gerade, Strecke, Winkel etc. – algebraisch beschreiben?

1.1 Feststellung

Legt man im anschaulich vorliegenden Raum für Entfernungsmessungen eine Längeneinheit fest, so kann man die Punkte einer Gerade mit der Menge \mathbb{R} der reellen Zahlen identifizieren („Zahlengerade“). Die Punkte einer vorgegebenen Ebene bzw. des ganzen Raumes kann man nach Festlegung eines (rechtwinkligen) Koordinatensystems mit \mathbb{R}^2 (Länge, Breite) bzw. mit \mathbb{R}^3 (Länge, Breite, Höhe) identifizieren, vgl. Abbildung 1.1

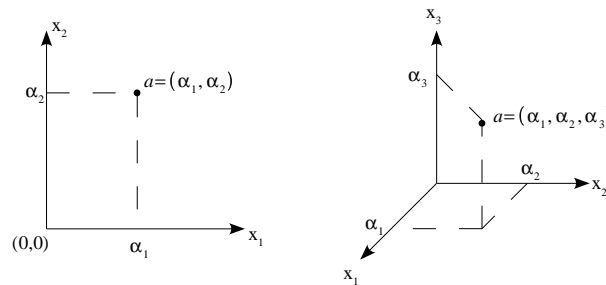


Abbildung 1.1: Punkte in der Ebene bzw. im Raum

Für den Abstand $d(a, b)$ von zwei Punkten a, b gilt:

- (a) Im \mathbb{R}^1 : $d(a, b) = |\alpha_1 - \beta_1| = \sqrt{(\alpha_1 - \beta_1)^2} \stackrel{(0.61)}{=} \sqrt{(a - b) \circ (a - b)}$
- (b) Im \mathbb{R}^2 (Satz des Pythagoras):

$$d^2(a, b) = |\alpha_1 - \beta_1|^2 + |\alpha_2 - \beta_2|^2 = (\alpha_1 - \beta_1)^2 + (\alpha_2 - \beta_2)^2 \stackrel{(0.61)}{=} (a - b) \circ (a - b)$$

$$\leadsto d(a, b) = \sqrt{(a - b) \circ (a - b)}$$
- (c) Im \mathbb{R}^3 : Seien $a = (\alpha_1, \alpha_2, \alpha_3), b = (\beta_1, \beta_2, \beta_3), h = (\beta_1, \beta_2, \alpha_3) \in \mathbb{R}^3$ Punkte im Raum (beachte die Koordinaten von h). Dann ist der Abstand zwischen a und b :

$$d^2(a, h) = (\alpha_1 - \beta_1)^2 + (\alpha_2 - \beta_2)^2 + (\alpha_3 - \alpha_3)^2$$

$$d^2(a, b) = d^2(a, h) + (\alpha_3 - \beta_3)^2 = (\alpha_1 - \beta_1)^2 + (\alpha_2 - \beta_2)^2 + (\alpha_3 - \beta_3)^2 \stackrel{(0.61)}{=}$$

$$(a-b) \circ (a-b) \\ \leadsto d(a,b) = \sqrt{(a-b) \circ (a-b)}$$

Diese sowohl im \mathbb{R}^1 als auch im \mathbb{R}^2 und im \mathbb{R}^3 gültige Abstandsformel motiviert die folgenden Definitionen.

1.2 (D)

Ist $(\mathbb{R}V, \circ)$ ein EVR, so heißen die Elemente von V *Punkte* und für alle $a, b \in V$ heißt

$$\sqrt{(a-b)^2} =: \|a-b\| =: |a-b| =: d(a,b) \geq 0$$

der *euklidische Abstand der Punkte* a, b .

1.3 (D)

Es sei $(\mathbb{R}V, \circ)$ ein reeler Vektorraum und $\|\dots\| : \begin{cases} V \rightarrow \mathbb{R}^+ := \{\rho \in \mathbb{R} \mid \rho \geq 0\} \\ a \mapsto \|a\| \end{cases}$

eine Abbildung von V nach \mathbb{R}^+ . Gilt für alle $\alpha \in \mathbb{R}$ und alle $a, b \in V$

$$(a) \quad \|a\| = 0_{\mathbb{R}} \Leftrightarrow a = 0_V,$$

$$(b) \quad \|\alpha a\| = |\alpha| \|a\| \text{ und}$$

$$(c) \quad \|a+b\| \leq \|a\| + \|b\|,$$

so heißt das Paar $(\mathbb{R}V, \circ)$ ein *normierter Vektorraum* und $\|a\| \in \mathbb{R}^+$ heißt die *Norm von a*.

1.4 (S+D)

Ist $(\mathbb{R}V, \circ)$ ein EVR, so gilt für alle $a, b \in V$ die *Cauchy-Schwartz'sche Ungleichung*

$$|a \circ b| \leq \sqrt{a^2} \circ \sqrt{b^2}$$

und $(\mathbb{R}V, \|\cdot\|)$ mit $\|\cdot\| : \begin{cases} V \rightarrow \mathbb{R}^+ \\ a \mapsto \|a\| := \sqrt{a \circ a} \end{cases}$ ist eine normierter Vektorraum.

$\|a\| = \sqrt{a \circ a}$ heißt die *Euklidische Norm von a* (im EVR $(\mathbb{R}V, \circ)$).

Beweis Es sei $(\mathbb{R}V, \circ)$ ein EVR und $\|a\| = \sqrt{a \circ a}$ für alle $a \in V$.

- Ist $a \neq 0_V$, dann ist $a^2 > 0$ und $\|a\| > 0_{\mathbb{R}}$.
Ist $a = 0_V$, so ist nach (0.43)(a) und (0.60) $a^2 = 0_{\mathbb{R}}$ und $\|a\| = 0_{\mathbb{R}}$.
Damit ist $\|a\| \in \mathbb{R}^+$ für alle $a \in V$ und es gilt $\|a\| = 0_{\mathbb{R}} \Leftrightarrow a = 0_V$, d.h. es gilt (1.3)(a).

- Seien $\alpha \in \mathbb{R}$ und $a, b \in V$ beliebig vorgegeben.

$$\begin{aligned} (\alpha a) \circ (\alpha a) &= \alpha[a \circ (\alpha a)] = \alpha[(\alpha a) \circ a] = \alpha[\alpha(a \circ a)] = \alpha^2 a^2 \\ \|\alpha a\| &= \sqrt{(\alpha a) \circ (\alpha a)} = \sqrt{\alpha^2 a^2} = \sqrt{\alpha^2} \sqrt{a^2} = |\alpha| \|a\| \end{aligned}$$

Damit gilt (1.3)(b).

- Ist $b = 0_V$, so gilt $a \circ b = 0_{\mathbb{R}}$ und $(a \circ b)^2 = 0_{\mathbb{R}} = a^2 0_{\mathbb{R}} = a^2 b^2$.

Ist $b \neq 0_V$, so gilt wegen [E4] $b^2 > 0$ und $0_{\mathbb{R}} \leq \left(a - \frac{a \circ b}{b^2} b\right)^2$.

Setze $\frac{a \circ b}{b^2} =: \rho \in \mathbb{R}$ und $a - \frac{a \circ b}{b^2} b = a - \rho b =: c \in V$. Dann ist:

$$\begin{aligned}
 \left(a - \frac{a \circ b}{b^2} b\right)^2 &= (a - \rho b) \circ c \\
 &= a \circ c - (\rho b) \circ c \\
 &= a \circ c - \rho(b \circ c) \\
 &= a \circ (a - \rho b) - \rho[b \circ (a - \rho b)] \\
 &= a^2 - a \circ (\rho b) - \rho[b \circ a - b \circ (\rho b)] \\
 &= a^2 - (\rho b) \circ a - \rho[a \circ b - (\rho b) \circ b] \\
 &= a^2 - \rho(b \circ a) - \rho[a \circ b - \rho(b \circ b)] \\
 &= a^2 - 2\rho(a \circ b) + \rho^2 b^2 \\
 &= a^2 - 2\frac{a \circ b}{b^2} a \circ b + \frac{(a \circ b)^2}{(b^2)^2} b^2 \\
 &= a^2 - \frac{(a \circ b)^2}{b^2}
 \end{aligned}$$

Damit ergibt sich eine Folgerungskette:

$$\begin{aligned}
 0 &\leq a^2 - \frac{(a \circ b)^2}{b^2} \\
 \leadsto \frac{(a \circ b)^2}{b^2} &\leq a^2 \\
 \leadsto (a \circ b)^2 &\leq a^2 b^2 \quad \text{falls } b \neq 0_V \\
 \leadsto |a \circ b| &\leq \sqrt{(a \circ b)^2} \leq \sqrt{a^2 b^2} = \sqrt{a^2} \sqrt{b^2} = \|a\| \|b\|
 \end{aligned}$$

Es gilt demnach die Cauchy-Schwarz'sche Ungleichung, mit der weitere Schlüsse möglich sind:

$$\begin{aligned}
 (a + b)^2 &= a^2 + 2a \circ b + b^2 = \|a\|^2 + 2(a \circ b) + \|b\|^2 \\
 &\leq \|a\|^2 + a|a \circ b| + \|b\|^2 \\
 &\leq \|a\|^2 + 2\|a\| \|b\| + \|b\|^2 = (\|a\| + \|b\|)^2 \\
 \leadsto \|a - b\| &= \sqrt{(a - b)^2} \leq \sqrt{(\|a\| + \|b\|)^2} = \|a\| + \|b\|
 \end{aligned}$$

Damit gilt auch (1.3)(c).

Da alle drei Bedingungen erfüllt sind, ist $({}_R V, \|\cdot\|)$ ein normierter Vektorraum.

1.5 (D)

Es sei M eine Menge und $d: \begin{cases} M \times M \rightarrow \mathbb{R}^+ := \{\rho \in \mathbb{R} \mid \rho \geq 0\} \\ (a, b) \mapsto d(a, b) \end{cases}$ eine Abbildung

von $M \times M$ nach \mathbb{R}^+ . Das Paar (M, d) heißt genau dann *metrischer Raum*, wenn für alle $a, b, c \in M$ gilt:

$$(a) \quad d(a, b) = 0 \Leftrightarrow a = b$$

$$(b) \quad d(a, b) = d(b, a)$$

$$(c) \quad d(a, b) + d(b, c) \geq d(a, c) \quad \text{Dreiecksungleichung}$$

1.6 (S)

Jeder normierte Vektorraum $(\mathbb{R}V, \|\cdot\|)$ stellt bezüglich der Abbildung

$$d: \begin{cases} M \times M \rightarrow \mathbb{R}^+ \\ (a, b) \mapsto d(a, b) := \|a - b\| \end{cases}$$

einen metrischen Raum dar.

Beweis Ist $(\mathbb{R}V, \|\cdot\|)$ ein normierter Vektorraum (siehe (1.3)) und die Abbildung d wie oben definiert, so gilt für alle $a, b, c \in V$:

- (a) $d(a, b) = 0 \Leftrightarrow \|a - b\| = 0 \Leftrightarrow a - b = 0_V \Leftrightarrow a = b$
- (b) $d(a, b) = \|a - b\| = |-1|\|a - b\| = \|(-1)a - b\| = \|b - a\| = d(b, a)$
- (c) $d(a, c) = \|a - c\| = \|(a - b) + (b - c)\| \leq \|a - b\| + \|b - c\| = d(a, b) + d(b, c)$

1.7 (A+D)

Eine Bijektion $\gamma: \begin{cases} M \rightarrow M \\ m \mapsto m^\gamma \end{cases}$ eines metrischen Raumes (M, d) heißt *abstandstreu* oder *Bewegung*, wenn für alle $a, b \in M$ gilt:

$$d(a^\gamma, b^\gamma) = d(a, b)$$

Zeige: Die Menge $\mathcal{B}(M, d) := \{\gamma \in \text{Bij}(M) \mid \gamma \text{ ist Bewegung}\}$ bildet – Nacheinander- ausführung von Abbildungen als Verknüpfung genommen – eine Untergruppe von $(\text{Bij}(M), \cdot)$.

$\mathcal{B}(M, d)$ heißt die *Gruppe der Bewegungen des metrischen Raumes (M, D)* .

Lösung

Seien $\alpha, \beta \in \mathcal{B}(M, d)$ und $a, b \in M$ beliebig vorgegeben.

- Da β und α Bewegungen sind, läßt sich folgern:

$$d((a^\alpha)^\beta, (b^\alpha)^\beta) = d(a^\alpha, b^\alpha) = d(a, b)$$

Damit ist $\alpha \cdot \beta \in \mathcal{B}(M, d) \forall \alpha, \beta \in \mathcal{B}(M, d)$

- Ist die Umkehrabbildung einer Bewegung ebenfalls eine Bewegung, d.h. gilt $d(a^{\beta^{-1}}, b^{\beta^{-1}}) = d(a, b)$?
- Jedenfalls ist $d(a^{\beta^{-1}}, b^{\beta^{-1}}) = d((a^{\beta^{-1}})^\beta, (b^{\beta^{-1}})^\beta) = d(a, b)$, da β eine Bewegung ist und $\beta^{-1} \cdot \beta = \text{id}_M$ gilt.
Also ist $\beta^{-1} \in \mathcal{B}(M, d)$ und mit der oben gezeigten Behauptung folgt $\alpha \cdot \beta^{-1} \in \mathcal{B}(M, d)$.
- Es ist $\mathcal{B}(M, d) \neq \{\}$, da z.B. $\text{id}_M \in \mathcal{B}(M, d)$. Nach dem Untergruppenkriterium ist $\mathcal{B}(M, d)$ eine Untergruppe von $(\text{Bij}(M), \cdot)$.

1.8 (S+D)

(a) Ist ${}_K V$ ein beliebiger Vektorraum, so bilden die Elemente von

$$T := \{\tau_a \mid a \in V\} \text{ mit } \tau_a : \begin{cases} V \rightarrow V \\ x \mapsto x^{\tau_a} := x + a \end{cases} \quad - \text{ Hintereinanderausföhrung von Abbildungen als Verknöpfung genommen} - \text{ eine Untergruppe von } (\text{Bij}(V), \cdot).$$

T heiÖt die *Translationsgruppe* des Vektorraumes ${}_K V$. *Gruppe!Translations-*

(b) Ist ${}_K V$ ein EVR (\mathbb{R}, \circ) , so gilt $T \subset \mathcal{B}(V, d)$.

Beweis

- (a) • Sei $a \in V$ beliebig vorgegeben.
 • Wegen $x^{\tau_a} = y \Leftrightarrow x + a = y \Leftrightarrow x = y - a$ gilt $\tau_a \in \text{Bij}(V)$ und es folgt $\{\tau_a \mid a \in V\} = T \subset \text{Bij}(V)$.
 • $(\text{Bij}(V), \cdot)$ ist Gruppe (laut (0.23)(c) die Gruppe aller Einheiten von $\text{Abb}(V)$).
 • Sei $\tau_b \in T$ beliebig vorgegeben, dann sind

$$\begin{aligned} x^{\tau_b \tau^{-b}} &= (x + b) + (-b) = x = x^{\text{id}_V} \\ x^{\tau^{-b} \tau_b} &= (x - b) + b = x = x^{\text{id}_V} \end{aligned}$$

für alle $x \in V$. Damit folgt $\tau_b^{-1} = \tau_{-b} \in T$ für alle $\tau_b \in T$.

- Seien $\tau_a, \tau_b \in T$ beliebig vorgegeben, dann sind $\tau_a, \tau_b^{-1} = \tau_{-b} \in T$ und es gilt für alle $x \in V$

$$x^{\tau_a \tau_b^{-1}} = x^{\tau_a \tau_{-b}} = (x + a) + (-b) = x + (a - b) = x^{\tau_{a-b}}$$

Somit ist $\tau_a \tau_b^{-1} = \tau_{a-b}$ für alle $\tau_a, \tau_b \in T$.

Nach dem Untergruppenkriterium ist T Untergruppe von $(\text{Bij}(V), \cdot)$.

(b) Ist $(\mathbb{R}V, \circ)$ ein EVR und $\tau_a \in T$, so gilt für alle $x, y \in V$

$$d(x^{\tau_a}, y^{\tau_a}) = \|x^{\tau_a} - y^{\tau_a}\| = \|(x + a) - (y + a)\| = \|x - y\| = d(x, y)$$

Damit ist $\tau_a \in \mathcal{B}(V, d)$.

1.9 (S+D)

- (a) Eine Abbildung $\sigma : \begin{cases} V \rightarrow V \\ x \mapsto x^\sigma \end{cases}$ eines EVR $(\mathbb{R}V, \circ)$ heiÖt *skalarprodukttreu*, wenn für alle $x, y \in V$ gilt:

$$x^\sigma \circ y^\sigma = x \circ y$$

- (b) Für eine Bijektion $\sigma : \begin{cases} V \rightarrow V \\ x \mapsto x^\sigma \end{cases}$ eines EVR $(\mathbb{R}V, \circ)$ sind äquivalent:

- (1) σ ist skalarprodukttreu.
- (2) $\sigma \in \mathcal{B}(V, d)$ und $0_V^\sigma = 0_V$

Beweis

(a) Definition, nicht beweisbar

(b) Anwendung der Beweismühle:

(1) \leadsto (2):

- Sei σ eine skalarprodukttreue Bijektion, dann ist $0_V^\sigma \circ 0_V^\sigma = 0_V \circ 0_V = 0_{\mathbb{R}} \leadsto 0_V^\sigma = 0_V$.
- Seien $x, y \in V$ beliebig vorgegeben. $(x^\sigma)^2 = x^\sigma \circ x^\sigma = x \circ x = x^2$, analog gilt $(y^\sigma)^2 = y^2$.

$$\begin{aligned}
 d^2(x^\sigma, y^\sigma) &= (x^\sigma - y^\sigma) \circ (x^\sigma - y^\sigma) \\
 &= (x^\sigma)^2 - 2(x^\sigma \circ y^\sigma) + (y^\sigma)^2 \\
 &= x^2 - 2(x \circ y) + y^2 \\
 &= (x - y)^2 = d^2(x, y)
 \end{aligned}$$

- Folglich ist $d(x^\sigma, y^\sigma) = d(x, y) \forall x, y \in V$.
- Damit ist $\sigma \in \mathcal{B}(V, d)$ mit $0_V^\sigma = 0_V$, d.h. es gilt (2).

(2) \leadsto (1):

- Sei umgekehrt $\sigma \in \mathcal{B}(V, d)$ mit $0_V^\sigma = 0_V$ beliebig vorgegeben. Seien $x, y \in V$ beliebig vorgegeben.
- $(x^\sigma)^2 = (x^\sigma - 0_V)^2 = d^2(x^\sigma, 0_V) = d^2(x^\sigma, 0_V^\sigma) = d^2(x, 0_V) = (x - 0_V)^2 = x^2$, d.h. $(x^\sigma)^2 = x^2$ und analog $(y^\sigma)^2 = y^2$.

$$\begin{aligned}
 d^2(x^\sigma, y^\sigma) &= d^2(x, y) \\
 \Leftrightarrow (x^\sigma - y^\sigma)^2 &= (x - y)^2 \\
 \Leftrightarrow (x^\sigma)^2 - 2(x^\sigma \circ y^\sigma) + (y^\sigma)^2 &= x^2 - 2(x \circ y) + y^2 \\
 \Leftrightarrow (-2)(x^\sigma \circ y^\sigma) &= (-2)(x \circ y) \\
 \Leftrightarrow x^\sigma \circ y^\sigma &= x \circ y
 \end{aligned}$$

d.h. σ ist skalarprodukttreue Bijektion.**1.10 (S)**

Für eine Bijektion $\alpha : \begin{cases} V \rightarrow V \\ x \mapsto x^\alpha \end{cases}$ eines EVR $(\mathbb{R}V, \circ)$ sind äquivalent:

- (a) $\alpha \in \mathcal{B}(V, d)$
- (b) $\alpha = \sigma\tau_a$, σ ist eine skalarprodukttreue Bijektion und $a \in V$, τ_a wie in Satz (1.8) definiert.

Beweis

- (a) \leadsto (b): Sei $\alpha \in \mathcal{B}(V, d)$ beliebig vorgegeben. Dann ist $0_V^\alpha =: a \in V$ und $\alpha\tau_{-a} =: \sigma \in \mathcal{B}(V, d)$ mit $0_V^\sigma = 0_V^{\alpha\tau_{-a}} = a^{\tau_{-a}} = a - a = 0$.
Damit ist σ skalarprodukttreue Bijektion von V und $\alpha = \alpha\tau_{-a}\tau_a = \sigma\tau_a$, d.h. es gilt (b).

- (b) \leadsto (a): Sei eine skalarprodukttreue Bijektion $\sigma \in \mathcal{B}(V, d)$ beliebig vorgegeben. $\sigma, \tau_a \in \mathcal{B}(V, d) \leadsto \sigma\tau_a := \alpha \in \mathcal{B}(V, d)$, d.h. es gilt (a).

1.11 (S)

Eine skalarprodukttreue Abbildung σ eines EVR $(\mathbb{R}V, \circ)$ ist stets eine lineare Abbildung, d.h. für alle $(\alpha, a, b) \in \mathbb{R} \times V \times V$ gilt:

$$(a) \quad (\alpha a)^\sigma = \alpha a^\sigma$$

$$(b) \quad (a + b)^\sigma = a^\sigma + b^\sigma$$

Beweis

(a) Forme um:

$$\begin{aligned} & ((\alpha a)^\sigma - \alpha a^\sigma) \circ ((\alpha a)^\sigma - \alpha a^\sigma) \\ &= (\alpha a)^\sigma \circ (\alpha a)^\sigma - (\alpha a)^\sigma \circ (\alpha a^\sigma) - (\alpha a^\sigma) \circ (\alpha a)^\sigma + (\alpha a^\sigma) \circ (\alpha a^\sigma) \\ &= (\alpha a)^\sigma \circ (\alpha a)^\sigma - 2[(\alpha a)^\sigma - (\alpha a^\sigma)] + \alpha[a^\sigma \circ (\alpha a^\sigma)] \\ &= \alpha^2 a^2 - 2\alpha[a \circ (\alpha a)] + \alpha[a \circ (\alpha a)] \\ &= \alpha^2 a^2 - 2\alpha^2 a^2 + \alpha^2 a^2 = 0_{\mathbb{R}} \end{aligned}$$

Folglich gilt $(\alpha a)^\sigma - \alpha a^\sigma = 0_V$ bzw. $(\alpha a)^\sigma = \alpha a^\sigma$.

(b) Auch hier ist geschicktes Rechnen möglich:

$$\begin{aligned} & ((a + b)^\sigma - (a^\sigma + b^\sigma)) \circ ((a + b)^\sigma - (a^\sigma + b^\sigma)) \\ &= (a + b)^\sigma \circ (a + b)^\sigma - (a + b)^\sigma \circ a^\sigma - (a + b)^\sigma \circ b^\sigma - a^\sigma \circ (a + b)^\sigma \\ & \quad - b^\sigma \circ (a + b)^\sigma + a^\sigma \circ a^\sigma + a^\sigma \circ b^\sigma + b^\sigma \circ a^\sigma + b^\sigma \circ b^\sigma \\ &= (a + b) \circ (a + b) - (a + b) \circ a - (a + b) \circ b - a \circ (a + b) \\ & \quad - b \circ (a + b) + a \circ a + a \circ b + b \circ a + b \circ b \\ & \dots \\ &= ((a + b) - (a + b))^2 = 0_V^2 = 0_{\mathbb{R}} \end{aligned}$$

Folglich gilt $(a + b)^\sigma - (a^\sigma + b^\sigma) = 0_V$ bzw. $(a + b)^\sigma = a^\sigma + b^\sigma$.

1.12 (S)

Ist $\sigma : \begin{cases} V \rightarrow V \\ x \mapsto x^\sigma \end{cases}$ eine lineare Abbildung eines Vektorraumes $_K V$ in sich, so gilt für alle $(n, (\alpha_1, \dots, \alpha_n), (a_1, \dots, a_n)) \in \mathbb{N} \times K^n \times V^n$:

$$(+) \quad \left(\sum_{i=1}^n \alpha_i a_i \right)^\sigma = \sum_{i=1}^n \alpha_i a_i^\sigma$$

Beweis Sei σ eine lineare Abbildung. Setze

$$\{n \in \mathbb{N} \mid \text{Für alle } (\alpha_1, \dots, \alpha_n) \in K^n, (a_1, \dots, a_n) \in V^n \text{ gilt } (+)\} =: S$$

Für alle $(\alpha, a) \in K \times V$ gilt $(\alpha a)^\sigma \stackrel{(1.11)(a)}{=} \alpha a^\sigma \rightsquigarrow 1 \in S$.

Seien $n \in S, (\alpha_1, \dots, \alpha_n, \alpha_{n+1}) \in K^{n+1}, (a_1, \dots, a_n, a_{n+1}) \in V^{n+1}$ beliebig vorge-

geben. Dann gilt für $\sum_{i=1}^n \alpha_i a_i =: b$, $\alpha_{n+1} a_{n+1} =: c \in V$:

$$\begin{aligned} \left(\sum_{i=1}^{n+1} \alpha_i a_i \right)^\sigma &= (b+c)^\sigma \stackrel{(1.11)(b)}{=} b^\sigma c^\sigma \\ &= \left(\sum_{i=1}^n \alpha_i a_i \right)^\sigma + (\alpha_{n+1} a_{n+1})^\sigma \\ &= \sum_{i=1}^n \alpha_i a_i^\sigma + \alpha_{n+1} a_{n+1}^\sigma \\ &= \sum_{i=1}^{n+1} \alpha_i a_i^\sigma \end{aligned}$$

Damit ist $n+1 \in S$ für alle $n \in S$ und nach dem Prinzip der vollständigen Induktion folgt $S = \mathbb{N}$.

1.13 (D)

- (a) Das für alle $(i, j) \in \mathbb{N} \times \mathbb{N}$ durch $\delta_{ij} := \begin{cases} 1 & \text{falls } i = j \\ 0 & \text{falls } i \neq j \end{cases}$ definierte Zeichen δ_{ij} heißt *Kroneckersymbol*.
- (b) Die für $i = 1, 2, \dots, n$ definierten n -Tupel $e_{ij} := (\delta_{i1}, \delta_{i2}, \dots, \delta_{in}) \in K^n$ heißen *Einheitsvektoren des Vektorraums $_K K^n$* .

1.14 (S)

Für die kanonischen n -dimensionalen Euklidischen Vektorräume (\mathbb{R}^n, \circ) (siehe (0.61)) gilt:

Ist $\sigma : \begin{cases} \mathbb{R}^n \rightarrow \mathbb{R}^n \\ x \mapsto x^\sigma \end{cases}$ eine Bijektion, so sind äquivalent:

- (a) σ ist eine Bewegung mit $0^\sigma = 0$.
- (b) Für alle $x \in \mathbb{R}^n$ gilt $x^\sigma = x \cdot A$, wobei A eine orthogonale $n \times n$ -Matrix ist, d.h. $A \in \mathbb{R}^{n \times n}$ genügt $A \cdot A^t = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$.

Beweis Sei (\mathbb{R}^n, \circ) ein vorgegebener kanonischer n -dimensionaler EVR und $\sigma : \begin{cases} \mathbb{R}^n \rightarrow \mathbb{R}^n \\ x \mapsto x^\sigma \end{cases}$ eine vorgegebene Bijektion.

(a) \rightsquigarrow (b):

- Sei σ eine Bewegung des metrischen Raumes (\mathbb{R}^n, d) mit $0^\sigma = 0$. Für alle $x, y \in \mathbb{R}^n$ gilt dann nach Satz (1.9): $x^\sigma \circ y^\sigma = x \circ y$.
- Für $e_i^\sigma = (\alpha_{i1}, \alpha_{i2}, \dots, \alpha_{in}) := a_i \in \mathbb{R}^n$ gilt: $a_i \circ a_j = e_i^\sigma \circ e_j^\sigma = (\delta_{i1}\delta_{j1} + \delta_{i2}\delta_{j2} + \dots + \delta_{in}\delta_{jn}) = \delta_{ij}\delta_{jj} = \delta_{ij} = \begin{cases} 1 & \text{falls } i = j \\ 0 & \text{falls } i \neq j \end{cases}$.

- Damit gilt für $\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} \alpha_{11} & \dots & \alpha_{1n} \\ \vdots & & \vdots \\ \alpha_{n1} & \dots & \alpha_{nn} \end{pmatrix} =: A \in \mathbb{R}^{n \times n}$:

$$(\text{i-te Zeile von } A) \circ (\text{j-te Spalte von } A) = \delta_{ij}$$

respektive in Matrizenmultiplikationsschreibweise (MMSw):

$$(\text{i-te Zeile von } A) \cdot (\text{j-te Spalte von } A^t) = \delta_{ij}$$

$$\text{d.h. } A \cdot A^t = \begin{pmatrix} \delta_{11} & \dots & \delta_{1n} \\ \vdots & & \vdots \\ \delta_{n1} & \dots & \delta_{nn} \end{pmatrix} = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$$

- Damit ist σ nach (1.11) lineare Abbildung.
- Schließlich gilt für alle

$$\begin{aligned} x &= (\xi_1, \xi_2, \dots, \xi_n) \\ &= \xi_1(1, 0, \dots, 0) + \xi_2(0, 1, \dots, 0) + \dots + \xi_n(0, 0, \dots, 1) \\ &= \sum_{\nu=1}^n \xi_\nu e_\nu \end{aligned}$$

und es folgt:

$$\begin{aligned} x^\sigma &= \left(\sum_{\nu=1}^n \xi_\nu e_\nu \right)^\sigma = \sum_{\nu=1}^n \xi_\nu e_\nu^\sigma = \sum_{\nu=1}^n \xi_\nu a_\nu \\ &= \sum_{\nu=1}^n \xi_\nu \left(\sum_{\mu=1}^n \alpha_{\nu\mu} e_\mu \right) \\ &= \sum_{\mu=1}^n \left(\sum_{\nu=1}^n \xi_\nu \alpha_{\nu\mu} \right) e_\mu \\ &= \left(\sum_{\nu=1}^n \xi_\nu \alpha_{\nu 1}, \sum_{\nu=1}^n \xi_\nu \alpha_{\nu 2}, \dots, \sum_{\nu=1}^n \xi_\nu \alpha_{\nu n} \right) \\ &= (\xi, \dots, \xi_n) \begin{pmatrix} \alpha_{11} & \dots & \alpha_{1n} \\ \vdots & & \vdots \\ \alpha_{n1} & \dots & \alpha_{nn} \end{pmatrix} \\ &= x \cdot A \end{aligned}$$

- Damit gilt (b).

(b) \rightsquigarrow (a):

- Ist umgekehrt $\sigma_a : \begin{cases} \mathbb{R}^n \rightarrow \mathbb{R}^n \\ x \mapsto x^\sigma \end{cases}$ eine Bijektion und $A \in \mathbb{R}^{n \times n}$ eine

orthogonale Matrix, so gilt für alle $x, y \in \mathbb{R}^n$:

$$\begin{aligned}
 x^{\sigma_a} \circ x^{\sigma_a} &= (x \cdot A) \circ (x \cdot A) \\
 &= (x \cdot A) \cdot (y \cdot A^t) \quad \text{Übergang zur MMSw} \\
 &= (x \cdot A) \cdot (A^t \cdot y^t) \\
 &= x \cdot (A \cdot A^t) y^t \\
 &= x \cdot \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \cdot y^t \\
 &= x \cdot y^t \\
 &= x \circ y
 \end{aligned}$$

- Damit ist σ_a Bewegung mit $0^{\sigma_a} = 0$.
- Es gilt (a).

1.15 (S)

Für eine Bijektion $\beta : \begin{cases} \mathbb{R}^n \rightarrow \mathbb{R}^n \\ x \mapsto x^\beta \end{cases}$ eines kanonischen n-dimensionalen EVR $(\mathbb{R}\mathbb{R}^n, \circ)$ sind äquivalent:

- (a) β ist eine Bewegung.
- (b) Für alle $x \in \mathbb{R}^n$ gilt $x^\beta = x \cdot A + a$ mit einer orthogonalen Matrix $A \in \mathbb{R}^{n \times n}$ und einem $a \in \mathbb{R}^n$.

Beweis

- (a) \leadsto (b): Ist β eine vorgegebene Bewegung, so gilt $0^\beta =: a \in \mathbb{R}^n$ und nach (1.7) und (1.8) ist $\beta\tau_{-a} =: \sigma$ eine Bewegung mit $0^\sigma = 0$. Nach (1.14) ist weiterhin $x^\sigma = a \cdot A$ mit einer orthogonalen Matrix A .
Setzt man ein, erhält man $x^\beta = x^{\beta\tau_{-a}\tau_a} = x^{\sigma\tau_a} = x \cdot A + a$ für alle $x \in \mathbb{R}^n$.

- (b) Ist $\gamma : \begin{cases} \mathbb{R}^n \rightarrow \mathbb{R}^n \\ x \mapsto x \cdot A + a \end{cases}$ eine Bijektion mit $a \in \mathbb{R}^n$ und einer orthogonalen Matrix $A \in \mathbb{R}^{n \times n}$, so ist $\sigma_a := \gamma\tau_{-a} : \begin{cases} \mathbb{R}^n \rightarrow \mathbb{R}^n \\ x \mapsto x \cdot A \end{cases}$ ebenfalls eine Bijektion.
 σ_a ist nach (1.14) eine Bewegung, damit ist nach (1.7) und (1.8) $\gamma = \sigma_a\tau_a$ ebenfalls eine Bewegung.

1.16 (A)

Es sei $(\mathbb{R}V, \circ)$ ein EVR und (V, d) der zugehörige metrische Raum. Beweise oder widerlege: Ist $\gamma \in \text{Abb}(V)$ eine Abbildung, die für alle $a, b \in V$ der Bedingung

$$(+) \quad d(a^\gamma, b^\gamma) = d(a, b)$$

genügt, ist stets auch injektiv bzw. surjektiv.

Kläre eventuell die obigen Behauptungen nur für die kanonischen n-dimensionalen EVRe $(\mathbb{R}\mathbb{R}^n, \circ)$ ¹.

¹Hilfe: Es ist $\det(AA^t) = \det \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} = 1 = \det(A) \det(A)^t$, d.h. es gilt $\det A \neq 0$

Lösung

- (a) *Injektivität*: Sei (M, d) ein metrischer Raum und $\gamma \in \text{Abb}(M)$ genüge (+). Seien $a, b \in M$ mit $a \neq b$ beliebig vorgegeben.

$$d(a^\gamma, b^\gamma) \stackrel{(+)}{=} d(a, b) > 0 \leadsto a^\gamma \neq b^\gamma$$

Danach ist γ injektiv.

- (b) *Surjektivität*: Die Surjektivität gilt nicht immer; Gegenbeispiel: Betrachte im Hilbertraum die Abbildung

$$\sigma : \begin{cases} H \rightarrow H \\ (\alpha_1, \alpha_2, \alpha_3, \dots) \mapsto (0, \alpha_1, \alpha_2, \alpha_3, \dots) \end{cases}$$

σ ist nicht surjektiv, genügt aber der Bedingung (+) für alle $a := (\alpha_1, \alpha_2, \alpha_3, \dots), b := (\beta_1, \beta_2, \beta_3, \dots)$, denn

$$d^2(a^\sigma, b^\sigma) = \sum_{\nu=1}^{\infty} (\alpha_\nu - \beta_\nu)^2 = d^2(a, b)$$

Bemerkung In den kanonischen n -dimensionalen EVR $(\mathbb{R}\mathbb{R}^n, \circ)$ ist die Surjektivität immer gegeben, denn für alle Abbildungen, die in solchen EVR durch Matrizen

$$A \text{ dargestellt werden, gilt } \det(AA^t) = \det \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} = 1 = \det(A) \det(A^t),$$

d.h. $\det A \neq 0$. Es existiert somit zu jeder solchen Abbildung A die (eindeutige) Umkehrabbildung A^{-1} , was die Surjektivität zeigt.

1.17 (D)

Ist (V, d) ein metrischer Raum, $m \in V$ und $0 \leq \rho \in \mathbb{R}$, so heißt

$$S(m, \rho) := \{x \in V \mid d(m, x) = \rho\}$$

die (V, d) -Sphäre mit dem Mittelpunkt m und dem Radius ρ .

1.18 (B)

- (a) Für den EVR $(\mathbb{R}\mathbb{R}^2, \circ)$ ist $(S(\mu_1, \mu_2), \rho) = \{(\xi_1, \xi_2) \in \mathbb{R}^2 \mid (\xi_1 - \mu_1)^2 + (\xi_2 - \mu_2)^2 = \rho^2\}$ die Kreislinie mit dem Mittelpunkt $m = (\mu_1, \mu_2)$ und dem Radius ρ .
- (b) Für den EVR $(\mathbb{R}\mathbb{R}^3, \circ)$ ist $(S(\mu_1, \mu_2, \mu_3), \rho) = \{(\xi_1, \xi_2, \xi_3) \in \mathbb{R}^3 \mid (\xi_1 - \mu_1)^2 + (\xi_2 - \mu_2)^2 + (\xi_3 - \mu_3)^2 = \rho^2\}$ die Oberfläche der Kugel mit dem Mittelpunkt $m = (\mu_1, \mu_2, \mu_3)$ und dem Radius ρ .

Problem

Wie kann man im \mathbb{R}^2 bzw. im \mathbb{R}^3 für zwei beliebig vorgegebene Punkte $a \neq b$ die anschaulich gegebene Verbindungsgerade \overline{ab} beschreiben (definieren)?

- Für jeden Punkt $x \in \mathbb{R}^2$ bzw. $x \in \mathbb{R}^3$ gilt $x \in S(a, |a - x|) \cap S(b, |b - x|) =: D(x)$.

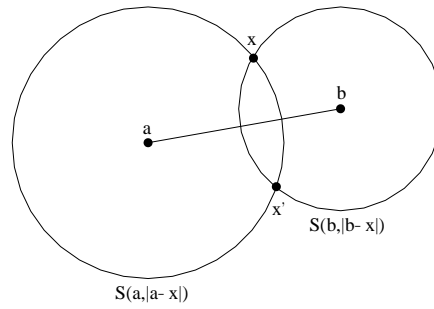


Abbildung 1.2: Zur Definition der Verbindungsgeraden

- Gilt $x \notin \overline{ab}$, so existiert noch mindestens ein Punkt $x' \neq x$ mit $x' \in D(x)$.
- Im Fall $x \in \overline{ab}$ gilt $D(x) = \{x\}$.

Dies motiviert die folgende Definition.

1.19 (D)

Sind $a, b \in V$ zwei verschiedene Punkte eines EVR $(\mathbb{R}V, \circ)$, so heißt

$$\overline{ab} =: \{x \in V \mid S(a, |a-x|) \cap S(b, |b-x|) = \{x\}\}$$

die *Verbindungsgerade* der Punkte a, b .

1.20 (S)

Ist $(\mathbb{R}V, \circ)$ ein EVR, so gilt² für alle $a, b \in V$ mit $a \neq b$:

$$\overline{ab} = \{a + \rho(b-a) \mid \rho \in \mathbb{R}\} =: a + \mathbb{R}(b-a) =: G_a^{b-a}$$

Beweis

- Seien $a, b \in V$ mit $a \neq b$ und ein $x \in \overline{ab}$ beliebig vorgegeben. Setze $\frac{|x-a|}{|b-a|} =: \alpha \in \mathbb{R}$ und $\frac{|x-b|}{|b-a|} =: \beta \in \mathbb{R}$, dann folgt $\left\{ \begin{array}{l} |x-a| = \alpha|b-a| \\ |x-b| = \beta|b-a| \end{array} \right\}$ und $\left\{ \begin{array}{l} (x-a)^2 = \alpha^2(b-a)^2 \\ (x-b)^2 = \beta^2(b-a)^2 \end{array} \right\}$.
- Multipliziere aus und forme um:

$$\begin{aligned} x^2 - 2a \circ x + a^2 &= \alpha^2(b-a)^2 \\ [-] \quad x^2 - 2b \circ x + b^2 &= \beta^2(b-a)^2 \\ \rightsquigarrow \quad 2b \circ x - 2a \circ x + a^2 - b^2 &= (\alpha^2 - \beta^2)(b-a)^2 \end{aligned}$$

²Prof. Leißner verwendet den Platzhalter \mathbb{R} in solchen Zusammenhängen gerne im Sinne von „steht für eine beliebige reelle Zahl“. Insbesondere kommen häufig Argumentationen wie $a \cdot \mathbb{R} = \mathbb{R}$ oder $a + \mathbb{R} = \mathbb{R}$ vor, was nichts anderes bedeuten soll als „Eine beliebige reelle Zahl, multipliziert mit bzw. addiert zu einer festen Zahl a , ist immernoch eine beliebige (andere) reelle Zahl“.

$$\begin{aligned}
(b-a) \circ [2x - (b+a) - (\alpha^2 - \beta^2)(b-a)] &= 0 \\
(b-a) \circ [2x \underbrace{(\beta^2 - \alpha^2 - 1)}_{=:2\sigma} b - \underbrace{(\beta^2 - \alpha^2 + 1)a}_{=:2\sigma+2}] &= 0 \\
(b-a) \circ [2x + 2\sigma b - (2\sigma + 2)a] &= 0 \\
2(b-a) \circ [x + \sigma b - (\sigma + 1)a] &= 0 \\
(b-a) \circ [(x-a) + \sigma(b-a)] &= 0 \\
(b-a) \circ [x - \underbrace{(a - \sigma(b-a))}_{=:p}] &= 0
\end{aligned}$$

- Resümee: Aus $\left\{ \begin{array}{l} (x-a)^2 = \alpha^2(b-a)^2 \\ (x-b)^2 = \beta^2(b-a)^2 \end{array} \right\}$ folgt $(b-a) \circ (x-p) = 0$ mit $p =:$
 $a + \rho(b-a)$ und $\rho = -\sigma = \frac{1 + \alpha^2 - \beta^2}{2}$.
- Damit ist $(p-a) \circ (x-p) = \rho(b-a) \circ (x-p) = 0$
und $(p-b) \circ (x-p) = (\rho-1)(b-a) \circ (x-p) = 0$.
- Es ist $x = p + (x-p)$, eingesetzt:

$$\begin{aligned}
(x-a)^2 &= ((p+(x-a))-a)^2 = ((p-a)+(x-p))^2 \\
&= (p-a)^2 + 2 \underbrace{(p-a) \circ (x-p)}_{=0} + (x-p)^2 \\
&= (p-a)^2 + (x-p)^2
\end{aligned}$$

Analog ergibt sich $(x-b)^2 = (p-b)^2 + (x-p)^2$.

- Setze $p - (x-p) =: x'$ ein:

$$\begin{aligned}
(x'-b)^2 &= ((p-b)-(x-b))^2 \\
&= (p-b)^2 - 2 \underbrace{(p-b) \circ (x-p)}_{=0} + (x-p)^2 \\
&= (p-b)^2 + (x-p)^2 \\
&= (x-b)^2
\end{aligned}$$

Analog ergibt sich $(x'-a)^2 = (x-a)^2$ und es ist

$$x' \in S(a, |a-x|) \cap S(b, |b-x|) = \{x\}$$

- Damit ist $x = x'$ bzw. $p + (x-p) = p - (x-b) \rightsquigarrow 2(x-p) = 0_V \rightsquigarrow (x-p) = 0_V \rightsquigarrow x = p = a + \rho(b-a)$.

- Bis hierher haben wir damit eine Inklusion gezeigt:

$$\overline{ab} \subset \{a + \rho(b-a) \mid \rho \in \mathbb{R}\} = G_a^{b-a}$$

- Zeige nun die umgekehrte Inklusion. Sei $a + \rho(b-a) =: p \in G_a^{b-a}$ beliebig vorgegeben.
Dann ist $p-a = \rho(b-a)$ bzw. $p-b = (\rho-1)(b-a)$.
- Es gilt $p \in S(a, |p-b|) \cap S(b, |p-b|) = D(p)$.

- Sei $x \in V \cap D(p)$ beliebig vorgegeben.
Dann ist $\left\{ \begin{array}{l} (x-a)^2 = (p-a)^2 = \rho^2(b-a)^2 \\ (x-b)^2 = (p-b)^2 = (\rho-1)^2(b-a)^2 \end{array} \right\}$,
woraus folgt $(b-a) \circ (x-p') = 0$ mit $p' = a + \rho'(b-a)$.
- Ein Vergleich mit dem Vorgehen bei der ersten Inklusion zeigt Parallelen zwischen α bzw. β und ρ , man erhält:

$$\rho' = \frac{1 + \rho^2 - (\rho-1)^2}{2} = \frac{2\rho}{2} = \rho$$

und es folgt $p' = p$, sowie $(b-a) \circ (x-p) = 0$.

- Der Trick aus der ersten Inklusion war sehr hilfreich, machen wir ihn also zur Methode:

$$\begin{aligned} (x-a)^2 &= ((p+(x-p))-a)^2 = ((p-a)+(x-p))^2 \\ &= (p-a)^2 + 2(p-a) \circ (x-p) + (x-p)^2 \\ &= (p-a)^2 + 2\rho(b-a) \circ (x-p) + (x-p)^2 \\ &= (p-a)^2 + (x-p)^2 \\ &= (x-a)^2 + (x-p)^2 \end{aligned}$$

Damit muß $(x-p)^2 = 0_{\mathbb{R}}$ sein, bzw. $x-p = 0_V$ und weiter $x = p$, woraus sich wiederum $D(p) = \{p\}$ und $p \in \overline{ab}$ ergibt, womit wir die andere Inklusion

$$G_a^{b-a} \subset \overline{ab}$$

gezeigt haben.

Damit ist die Behauptung $\overline{ab} = G_a^{b-a}$ gezeigt.

1.21 (S)

Ist $(_{\mathbb{R}}V, \circ)$ ein EVR, so gilt:

$$\{\overline{ab} \mid a, b \in V \text{ und } a \neq b\} = \{G_p^u =: p + \mathbb{R}u \mid p, u \in V \text{ und } u \neq 0_V\} =: \mathcal{G}(_{\mathbb{R}}V)$$

Es heißt $\mathcal{G}(_{\mathbb{R}}V)$ die *Grundmenge der affinen Geometrie über dem EVR* $(_{\mathbb{R}}V, \circ)$.

Beweis

- Setze $\{\overline{ab} \mid a, b \in V \text{ und } a \neq b\} =: \Gamma$. Sei $\overline{ab} \in \Gamma$ beliebig vorgegeben. Dann ist $b-a \neq 0_V$ und es gilt

$$\overline{ab} \stackrel{(1.20)}{=} G_a^{b-a} \subset \{G_p^u \mid p, u \in V \text{ und } u \neq 0_V\} =: \Delta$$

$$\leadsto \Gamma \subset \Delta$$

- Sei umgekehrt $G_p^u \in \Delta$ beliebig vorgegeben. Es ist $p+u = q \neq p$, woraus folgt

$$G_p^u = G_p^{q-p} \stackrel{(1.20)}{=} \overline{pq} \in \Gamma$$

$$\leadsto \Delta \subset \Gamma$$

Folglich gilt $\Delta = \Gamma = \mathcal{G}(_{\mathbb{R}}V)$.

1.22 S+D

Ist $(\mathbb{R}V, \circ)$ ein EVR, so gilt für alle $a, b \in V$ mit $a \neq b$:

$$\begin{aligned}\overline{ab} &:= \{x \in \overline{ab} \mid d(x, a) \leq d(a, b) \text{ und } d(x, b) \leq d(a, b)\} \\ &= \{a + \rho(b - a) \mid 0 \leq \rho \leq 1\}\end{aligned}$$

und \overline{ab} heißt die *Verbindungsstrecke der Punkte a, b* .

Beweis Seien $a, b \in V$ mit $a \neq b$ und ein $x \in \overline{ab}$ beliebig vorgegeben. Nach Satz (1.20) ist dann $x = a + \rho(b - a)$ mit einem $\rho \in \mathbb{R}$. Es ist

$$\begin{aligned}d(x, a) \leq d(a, b) &\Leftrightarrow \sqrt{(x - a)^2} \leq \sqrt{(a - b)^2} \\ &\Leftrightarrow ((a + \rho(b - a)) - a)^2 \leq (a - b)^2 \\ &\Leftrightarrow \rho^2(b - a)^2 \leq (a - b)^2 \\ &\Leftrightarrow \rho^2 \leq 1 \\ &\Leftrightarrow |\rho| \leq 1\end{aligned}$$

Analog folgt $d(x, b) \leq d(a, b) \Leftrightarrow |1 - \rho| \leq 1$.

Aus der Kombination beider Feststellungen folgt: Für $x = a + \rho(b - a) \in \overline{ab}$ gilt $d(x, a) \leq d(a, b)$ und $d(x, b) \leq d(a, b)$ genau dann, wenn $|\rho| \leq 1$ und $|1 - \rho| \leq 1$, d.h. wenn $0 \leq \rho \leq 1$.

1.23 (S+D)

Es seien a, b, m Punkte in einem EVR mit $a \neq b$. Dann sind äquivalent:

- (a) $d(a, m) = d(m, b) = \frac{1}{2}d(a, b)$
- (b) $m = \frac{1}{2}(a + b)$

und es heißt $m =: m(a, b) = \frac{1}{2}a + \frac{1}{2}b \in \overline{ab}$ der *Mittelpunkt der Strecke \overline{ab}* .

Beweis

(a) \leadsto (b):

- Setze $|a - m| = |m - b| = \frac{1}{2}|a - b| =: \delta$.
- Dann ist

$$\begin{aligned}(a - b)^2 &= ((a - m) + (m - b))^2 = (a - m)^2 + 2(a - m) \circ (m - b) + (m - b)^2, \\ \text{woraus } 4\delta^2 &= \delta^2 + 2(a - m) \circ (m - b) + \delta^2 \text{ und weiter } 2\delta^2 = 2(a - m) \circ (m - b) \\ &\text{folgt.}\end{aligned}$$

- Weiterhin ist

$$\begin{aligned}((a - m) - (m - b))^2 &= (a - m)^2 - 2(a - m) \circ (m - b) + (m - b)^2 \\ &= \delta^2 - 2\delta^2 + \delta^2 = 0_{\mathbb{R}}\end{aligned}$$

- Nach [E4] ist folglich

$$\begin{aligned}((a - m) - (m - b)) &= 0_V \\ \leadsto (a + b) &= 2m \\ m &= \frac{1}{2}(a + b)\end{aligned}$$

(b) \leadsto (a):

- Sei umgekehrt $a, b \in V$ mit $a \neq b$ beliebig vorgeben.
- Setze $\frac{1}{2}a + \frac{1}{2}b =: m$.
- Dann ist

$$\begin{aligned}
 a - m &= \frac{a - b}{2} = m - b \\
 \leadsto (a - m)^2 &= \frac{1}{4}(a - b)^2 = (m - b)^2 \\
 \leadsto \sqrt{(a - m)^2} &= \frac{1}{2}\sqrt{(a - b)^2} = \sqrt{(m - b)^2}
 \end{aligned}$$

mit anderen Worten $d(a, m) = \frac{1}{2}d(a, b) = d(m, b)$.

1.24 (A)

Es seien $a_1 = a_4, a_2 = a_5, a_3 = a_6$ drei verschiedene Punkte eines EVR, die für $i = 1, 2, 3$ der Bedingung $a_i \notin \overline{a_{i+1}a_{i+2}}$ genügen, siehe Abbildung 1.3

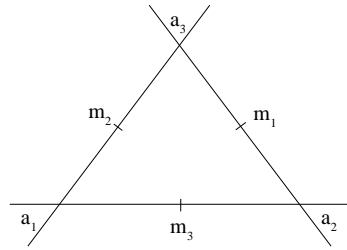


Abbildung 1.3: Dreieck

Zeige: Bezeichnet $m_i = \frac{1}{2}(a_{i+1} + a_{i+2})$ für $i = 1, 2, 3$ den Mittelpunkt der Strecke $\overline{a_{i+1}a_{i+2}}$, so gilt:

- (a) $a_i \neq m_i$
- (b) $\frac{1}{3}(a_1 + a_2 + a_3) =: s \in \overline{a_1m_1} \cap \overline{a_2m_2} \cap \overline{a_3m_3}$
- (c) $d(a_i, s) : d(s, m_i) = 2 : 1$

Es heißt s der *Schwerpunkt des Dreiecks* $\triangle(a_1, a_2, a_3)$.

Lösung

(a) Es ist

$$m_i = \frac{1}{2}(a_{i+1} + a_{i+2}) = a_{i+1} + \frac{1}{2}(a_{i+2} - a_{i+1}) \in a_{i+1} + \mathbb{R}(a_{i+2} - a_{i+1})$$

mit $a_{i+1} + \mathbb{R}(a_{i+2} - a_{i+1}) \stackrel{(1.20)}{=} \overline{a_{i+1}a_{i+2}}$.

Da nach Voraussetzung $a_i \notin \overline{a_{i+1}a_{i+2}}$, folgt $a_i \neq m_i$ für $i = 1, 2, 3$.

(b) Es ist

$$\begin{aligned}
 a_i + \frac{2}{3}(m_i - a_i) &= a_i + \frac{2}{3} \left(\frac{a_{i+1} + a_{i+2}}{2} - a_i \right) \\
 &= \frac{1}{3}a_i + \frac{1}{3}(a_{i+1} + a_{i+2}) \\
 &= \frac{1}{3}(a_1 + a_2 + a_3) \\
 &= s \in \{a_i + \rho(m_i - a_i) \mid 0 \leq \rho \leq 1\} \\
 &= \overline{a_i m_i} \text{ für } i = 1, 2, 3
 \end{aligned}$$

Folglich ist $s \in \overline{a_1 m_1} \cap \overline{a_2 m_2} \cap \overline{a_3 m_3}$.

$$(c) \text{ Es ist } s - m_i = \frac{1}{3}(a_i + a_{i+1} + a_{i+2}) - \frac{a_{i+1} + a_{i+2}}{2} = \frac{1}{3}a_i - \frac{1}{6}a_{i+1} - \frac{1}{6}a_{i+2}.$$

$$\text{Weiterhin ist } a_i - s = a_i - \frac{1}{3}(a_i + a_{i+1} + a_{i+2}) = \frac{2}{3}a_i - \frac{1}{3}a_{i+1} - \frac{1}{3}a_{i+2} = 2(s - m_i).$$

Daraus folgt:

$$d(a_i, s) = \sqrt{(a_i - s)^2} = \sqrt{(2(s - m_i))^2} = 2\|s - m_i\| = 2d(s, m_i)$$

1.25 (D+A)

Sind $a, b \in V$ zwei verschiedene Punkte eines EVR, so heißt

$$\overline{ab} := \overline{ab} \cup \{x \in \overline{ab} \mid b \in \overline{ax}\}$$

die b enthaltende Halbgerade mit Anfangspunkt a , siehe auch Abbildung 1.4.

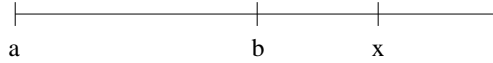


Abbildung 1.4: Zur Definition der Halbgeraden

Zeige: $\overline{ab} = \{a + \rho(b - a) \mid \rho \geq 0\}$

Lösung

Es gilt $x \in \overline{ab} \setminus \{a\}$ genau dann, wenn $x = a + \sigma(b - a)$ mit $\sigma \neq 0$. Bilde die Umkehrfunktion $\sigma^{-1}(x - a) = b - a$ und forme um zu $b = a + \sigma^{-1}(x - a)$.

Also ist $x \in \overline{ab}$ und $b \in \overline{ax}$, was nach (1.22) gleichbedeutend ist mit $b = a + \sigma^{-1}(x - a)$ mit $0 < \sigma^{-1} \leq 1$.

Mit anderen Worten ist demnach $x = a + \sigma(b - a)$ mit $0 < \sigma \leq 1$ und es folgt daraus

$$\overline{ab} = \overline{ab} \cup \{x \in \overline{ab} \mid b \in \overline{ax}\} \stackrel{(1.22)}{=} \{a + \rho(b - a) \mid \rho \geq 0\}$$

1.26 (D)

Eine Teilmenge $A \subset V$ eines reellen Vektorraums ${}_R V$ heißt *konvex*, wenn für alle $p, q \in A$ mit $p \neq q$ gilt:

$$\overline{ab} = \{p + \rho(q - p) \mid 0 \leq \rho \leq 1\} = \{\alpha p + \beta q \mid \alpha, \beta \in \mathbb{R}^+ \text{ und } \alpha + \beta = 1\} \subset A$$

1.27 (A)

Zeige: Ist m ein Punkt in einem EVR $(\mathbb{R}V, \circ)$ und $0 < \delta \in \mathbb{R}$, so ist

$$U_\delta(m) := \{x \in V \mid |x - m| < \delta\}$$

stets konvex.

$U_\delta(m)$ heißt die δ -Umgebung des Punktes m im EVR $(\mathbb{R}V, \circ)$. Deltaumgebung δ -Umgebung

Lösung

- Seien $a, b \in U_\delta(m)$ mit $a \neq b$ beliebig vorgegeben. Dann ist $|x - m| < \delta$ und $|b - m| < \delta$.
- Sei $x \in \overline{ab}$ beliebig vorgegeben. Nach (1.22) gilt dann $x = \alpha a + \beta b$ mit $\alpha, \beta \in \mathbb{R}^+$ und $\alpha + \beta = 1$.
- Somit ist $x - m = \alpha(a - m) + \beta(b - m)$ und weiter

$$\begin{aligned} (x - m)^2 &= [\alpha(a - m) + \beta(b - m)]^2 \\ &= \alpha^2(a - m)^2 + 2\alpha\beta(a - m) \circ (b - m) + \beta^2(b - m)^2 \\ &< (\alpha^2 + \beta^2)\delta^2 + 2\alpha\beta \underbrace{|a - m|}_{< \delta} \underbrace{|b - m|}_{< \delta} \\ &\leq (\alpha^2 + 2\alpha\beta + \beta^2)\delta^2 = (\alpha + \beta)^2\delta^2 = \delta^2 \end{aligned}$$

- Damit folgt die Behauptung

$$|x - m| < \delta \rightsquigarrow \overline{ab} \subset U_\delta(m)$$

1.28 (S)

Ist $\mathbb{R}V$ ein reeller Vektorraum und $\text{Konvex}^* := \{C \subset V \mid C \text{ ist konvex}\}$, so gilt:
Für jede Teilmenge $\mathcal{K} \subset \text{Konvex}^*$ gilt:

$$\bigcap_{C \in \mathcal{K}} C = \{x \in V \mid x \in C \text{ für alle } C \in \mathcal{K}\} =: D \in \text{Konvex}^*$$

„Der Durchschnitt beliebig vieler konvexer Mengen ist konvex“

Beweis

- Sei $\mathcal{K} \subset \text{Konvex}^*$ beliebig vorgegeben.
- Setze $\bigcap_{C \in \mathcal{K}} C =: D$. Seien $p, q \in D$ mit $p \neq q$ beliebig vorgegeben.
- Dann ist $p, q \in C$ für alle $C \in \mathcal{K}$ und da $C \in \text{Konvex}^*$ ist, ist auch $\overline{pq} \subset C$ für alle $C \in \mathcal{K}$.
- Damit ist $\overline{pq} \subset D$.
- Für alle $p, q \in D$ mit $p \neq q$ gilt demnach $\overline{pq} \subset D$; nach (1.26) ist D konvex.

1.29 (D)

Es sei M eine Menge und $\text{Hülle}^* \subset \text{Pot}(M)$ eine Teilmenge der Potenzmenge von M .

Das Paar $(M, \text{Hülle}^*)$ heißt ein *Hüllensystem* und die Elemente von Hülle^* heißen *Hüllen*, wenn gilt:

- (i) $M \in \text{Hülle}^*$
- (ii) $\bigcap_{H \in \mathcal{H}} H =: D \in \text{Hülle}^*$ für alle $\mathcal{H} \subset \text{Hülle}^*$
 („Der Durchschnitt von beliebig vielen Hüllen ist stets wieder eine Hülle.“)

1.30 (S+D) Hauptsatz über Hüllensysteme

Ist $(M, \text{Hülle}^*)$ ein Hüllensystem und $S \subset M$, so ist

$$\bigcap_{H \in S^*} H =: \text{Hülle}(S) \quad \text{mit } S^* := \{H \in \text{Hülle}^* \mid H \supset S\}$$

eine kleinste Hülle, die S umfaßt, d.h. es gilt:

- (a) $\text{Hülle}(S) \in \text{Hülle}^*$
- (b) $\text{Hülle}(S) \supset S$
- (c) Aus $H \in \text{Hülle}^*$ und $H \supset S$ folgt stets $H \supset \text{Hülle}(S)$.

$\text{Hülle}(S)$ heißt die von S (im Hüllensystem $(M, \text{Hülle}^*)$) *erzeugte* oder die von S *aufgespannte Hülle*.

Beweis Seien ein Hüllensystem $(M, \text{Hülle}^*)$ und $S \subset M$ beliebig, dann aber fest vorgegeben.

- Setze $\{H \in \text{Hülle}^* \mid H \subset S\} =: S^*$.
- Setze $\bigcap_{H \in S^*} H = \{x \in M \mid x \in H \text{ für alle } H \in S^*\} =: D =: \text{Hülle}(S)$.
- Nach (1.29 (i)) folgt die Aussage (a): $\text{Hülle}(S) \in \text{Hülle}^*$.
- Sei ein $s \in S$ beliebig vorgegeben, dann ist $s \in H$ für alle $H \in S^*$ und es folgt $s \in D$. Damit ergibt sich Aussage (b): $\text{Hülle}(S) \supset S$.
- Sei $H' \in \text{Hülle}^*$ mit $H' \supset S$ beliebig vorgegeben. Dann ist $H' \in S^*$ und es folgt $H' \supset \bigcap_{H \in S^*} H = \text{Hülle}(S)$. Damit hat man die Aussage (c): Aus $H \in \text{Hülle}^*$ und $H \supset S$ folgt stets $H \supset \text{Hülle}(S)$.

1.31 (B)

- (a) Ist O^* das System aller offenen Teilmengen von \mathbb{R} , so gibt es z.B. eine kleinste offene Menge O , die $O \supset [0, 1]$ genügt.
- (b) Ist A^* das System aller abgeschlossenen Teilmengen von \mathbb{R} , so ist das Paar (\mathbb{R}, A^*) ein Hüllensystem (lt. Analysis-Vorlesung). Nach dem Hauptsatz über Hüllensysteme existiert damit zu jedem $S \subset \mathbb{R}$ eine kleinste abgeschlossene Teilmenge A , die $A(S) \supset S$ genügt. Es ist z.B. $A((0, 1)) = [0, 1]$.

1.32 (S)

Ist (V, Konvex^*) das Hüllensystem aller konvexen Teilmengen eines reellen Vektorraums ${}_R V$ und $S \subset V$, so gilt für die *konvexe Hülle von S* :

- (i) $\text{Konvex}(S) =: \overline{S} = \left\{ \sum_{\nu=1}^n \alpha_\nu s_\nu \mid n \in \mathbb{N} \text{ und } (\alpha_\nu, S_\nu) \in \mathbb{R}^+ \times S \text{ und } \sum_{\nu=1}^n \alpha_\nu = 1 \right\}$
- (ii) Ist $S =: \{b_1, b_2, \dots, b_m\}$ eine *endliche* Teilmenge von V , so läßt sich (i) vereinfachen zu:
 $\overline{\{b_1, \dots, b_m\}} = \left\{ \sum_{\mu=1}^m \beta_\mu b_\mu \mid \beta_\mu \in \mathbb{R}^+ \text{ und } \sum_{\mu=1}^m \beta_\mu = 1 \right\}$

Beweis Sei $S \subset V$ beliebig vorgegeben.

- (i) • Setze für $n = 1, 2, 3, \dots$ $\left\{ \sum_{\nu=1}^n \alpha_\nu S_\nu \mid (\alpha_\nu, S_\nu) \in \mathbb{R}^+ \times S \text{ und } \sum_{\nu=1}^n \alpha_\nu = 1 \right\} =: S_n$ und $\left\{ n \in \mathbb{N} \mid S_n \subset \overline{S} \right\} =: T$.
- $S_1 = \left\{ \sum_{\nu=1}^1 \alpha_\nu S_\nu \mid (\alpha_1, S_1) \in \mathbb{R}^+ \times S \text{ und } \sum_{\nu=1}^1 \alpha_\nu = 1 \right\} = \{1S_1 \mid S_1 \in S\} = S$.
- Da $\overline{S} \supset S$, ist $1 \in T$.
- Seien $n \in T$ und $x = \sum_{\nu=1}^{n+1} \alpha_\nu S_\nu \in S_{n+1}$ beliebig vorgegeben.
- Dann $\begin{cases} \text{entweder } \exists \nu_0 \in \{1, 2, \dots, n-1\} : \alpha_{\nu_0} = 0 \leadsto x \in S_n \stackrel{n \in T}{\subset} \overline{S} \\ \text{oder} \quad \text{für } \nu=1, 2, \dots, n+1 : \alpha_\nu > 0 \leadsto 0 < \sum_{\nu=1}^n \alpha_\nu = 1 - \alpha_{n+1} < 1 \end{cases}$
- Damit gilt $0 < \frac{\alpha_\nu}{1 - \alpha_{n+1}} =: \beta_\nu$ für $\nu = 1, 2, \dots, n$ und
- $$\sum_{\nu=1}^n \beta_\nu = \frac{1}{1 - \alpha_{n+1}} \sum_{\nu=1}^n \alpha_\nu = 1.$$
- Folglich ist $\sum_{\nu=1}^n \beta_\nu S_\nu =: y \in S_n \stackrel{n \in T}{\subset} \overline{S}$
- Weiterhin ist $x = \sum_{\nu=1}^n \alpha_\nu S_\nu = (1 - \alpha_{n+1})(\sum_{\nu=1}^n \beta_\nu S_\nu) + \alpha_{n+1} S_{n+1} \in \overline{yS_{n+1}} \stackrel{S_{n+1} \in \overline{S}}{\subset} \overline{S} \leadsto S_{n+1} \subset \overline{S}$.
- Folglich ist $n+1 \in T$ für alle $n \in T$, d.h. $T = \mathbb{N}$ und weiter

$$\overline{S} \supset \bigcup_{n=1}^{\infty} S_n = \left\{ \sum_{\nu=1}^n \alpha_\nu s_\nu \mid n \in \mathbb{N} \text{ und } (\alpha_\nu, S_\nu) \in \mathbb{R}^+ \times S \text{ und } \sum_{\nu=1}^n \alpha_\nu = 1 \right\} =: C$$

- Es gilt $C \supset S_1 = S$.
- Sind $x := \sum_{\nu=1}^n \alpha_\nu s_\nu$, $y := \sum_{\mu=1}^m \beta_\mu s_\mu \in C$ und $z := \alpha x + \beta y \in \overline{xy}$ beliebig vorgegeben, so gilt

$$\begin{aligned} \alpha x + \beta y &= \alpha \left(\sum_{\nu=1}^n \alpha_\nu s_\nu \right) + \beta \left(\sum_{\mu=1}^m \beta_\mu s_\mu \right) \\ &= \sum_{\nu=1}^n (\alpha \alpha_\nu) s_\nu + \sum_{\mu=1}^m (\beta \beta_\mu) s_\mu \in S_{n+m} \subset C \end{aligned}$$

da $\alpha \alpha_\nu, \beta \beta_\mu \in \mathbb{R}^+$ und

$$\sum_{\nu=1}^n \alpha \alpha_\nu + \sum_{\mu=1}^m \beta \beta_\mu = \alpha \left(\sum_{\nu=1}^n \alpha_\nu \right) + \beta \left(\sum_{\mu=1}^m \beta_\mu \right) = \alpha + \beta = 1$$

Damit ist $C \in \text{Konvex}^*$.

- Damit ist die umgekehrte Inklusion $C \supset \overline{S}$ gezeigt und es folgt die Aussage (i): $C = \overline{S}$
- (ii) • Im Fall $S =: \{b_1, b_2, \dots, b_k\}$ setze $x =: \sum_{\nu=1}^n \alpha_\nu s_\nu$ mit $n \in \mathbb{N}$; $(\alpha_\nu, s_\nu) \in \mathbb{R}^+ \times S$; $\sum_{\nu=1}^n \alpha_\nu = 1$ und $\mu \in \{1, 2, \dots, m\}$.
 - $I_\mu := \{\nu \in \{1, 2, \dots, n\} \mid s_\nu = b_\mu\}$ mit $\beta_\mu := \begin{cases} \sum_{\nu \in I_\mu} \alpha_\nu & \text{falls } I_\mu \neq \{\} \\ 0 & \text{falls } I_\mu = \{\} \end{cases}$
 - Dann ist $x = \sum_{\mu=1}^m \beta_\mu b_\mu$ mit $\beta_\mu \in \mathbb{R}^+$ und $\sum_{\mu=1}^m \beta_\mu = 1$.

1.33 (B)

Im \mathbb{R}^2 gilt

$$\begin{aligned} & \overline{\{(0,0), (1,0), (0,1)\}} \\ &= \{\alpha(0,0) + \beta(1,0) + \gamma(0,1) \mid \alpha, \beta, \gamma \geq 0 \text{ und } \alpha + \beta + \gamma = 1\} \\ &= \{(\beta, \gamma) \mid \beta, \gamma \geq 0 \text{ und } \beta + \gamma \leq 1\} \end{aligned}$$

Weiterhin

$$\begin{aligned} & \overline{\{(0,0), (1,0), (0,1), (1,1)\}} \\ &= \{\alpha(0,0) + \beta(1,0) + \gamma(0,1) + \delta(1,1) \\ &= (\beta + \delta, \gamma + \delta) \mid \beta, \gamma, \delta \geq 0 \text{ und } \beta + \gamma + \delta \leq 1\} \end{aligned}$$

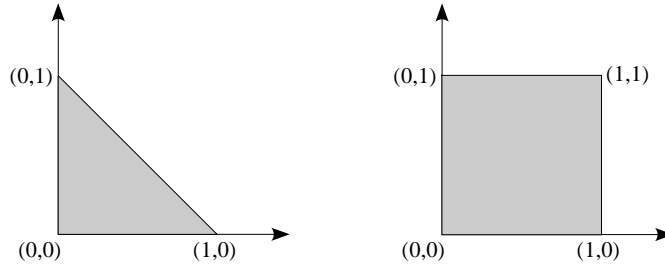


Abbildung 1.5: Konvexe Hüllen im \mathbb{R}^2

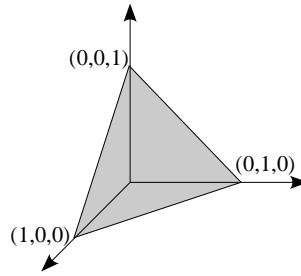
Im \mathbb{R}^3 gilt

$$\overline{\{(1,0,0), (0,1,0), (0,0,1)\}} = \{(\alpha, \beta, \gamma) \mid \alpha, \beta, \gamma \geq 0 \text{ und } \alpha + \beta + \gamma \leq 1\}$$

1.34 (D)

Eine Teilmenge $U \subset V$ eines VR ${}_K V$ heißt *Untervektorraum von ${}_K V$* , kurz UVR, wenn gilt:

- (i) $(U, +)$ ist Untergruppe von $(V, +)$.
- (ii) $K \cdot U := \{\alpha a \mid (\alpha, a) \in K \times U\} \subset U$

Abbildung 1.6: Konvexe Hülle im \mathbb{R}^3

1.35 (A)

Zeige: Ist ${}_K V$ ein Vektorraum, so gilt

- (i) (V, UVR^*) mit $\text{UVR}^* := \{U \subset V \mid U \text{ ist Untervektorraum von } {}_K V\}$ ist ein Hüllensystem.
- (ii) Für alle $S \subset V$ gilt $\text{UVR}(S) = \{\sum_{\nu=1}^n \alpha_\nu s_\nu \mid n \in \mathbb{N} \text{ und } (\alpha_\nu, s_\nu) \in K \times S\} =: \text{Lin}(S)$
- (iii) $(\{b_1, b_2, \dots, b_m\}) = \{\sum_{\mu=1}^m \beta_\mu b_\mu \mid \beta_\mu \in K\}$

Lösung

- (i)
 - Es gilt $V \in \text{UVR}^*$.
 - Sei $\chi \in \text{UVR}^*$ beliebig vorgegeben. Dann ist (siehe 1.36) $\bigcap_{U \in \chi} U =: D \in \text{Ugr}^*(V, +)$.
 - Für alle $U \in \chi$ gilt $D \subset U$, also auch $K \cdot D \subset K \cdot U \underset{(1.34)}{\subset} U$.
 - Daraus folgt wiederum $K \cdot D \subset \bigcap_{U \in \chi} U = D$ und weiter $D \in \text{UVR}^*$.
 - Damit ist (V, UVR^*) ein Hüllensystem.
- (ii)
 - Setze für $n = 1, 2, 3, \dots$ $\{\sum_{\nu=1}^n \alpha_\nu s_\nu \mid (\alpha_\nu, s_\nu) \in k \times S\} =: S_n$.
 - Setze $\{n \in \mathbb{N} \mid S_n \in \text{UVR}(S)\} =: T$.
 - $S_1 = \{\alpha_1 s_1 \mid (\alpha_1, s_1) \in k \times S\} \subset \text{UVR}(S)$ und $S = \{1 s_1 = s_1 \mid s_1 \in S\} \subset S_1$
 $\leadsto s \subset s_1 \subset \text{UVR}(S)$. Damit ist $1 \in T$.
 - Seien $n \in T$ und $x := \sum_{\nu=1}^{n+1} \alpha_\nu s_\nu \in S_{n+1}$ beliebig vorgegeben.
 - Dann ist $\sum_{\nu=1}^n \alpha_\nu s_\nu =: a \underset{n \in T}{\in} \text{UVR}(S)$ und $\alpha_{n+1} s_{n+1} =: b \in S_1 \subset \text{UVR}(S)$.
 Da $\text{UVR}(S)$ Untergruppe von $(V, +)$ ist, gilt $x = a + b \in \text{UVR}(S)$.
 - Damit ist $S_{n+1} \subset \text{UVR}(S)$, falls $n \in T$. Weiterhin ist $n+1 \in T$, falls $n \in T$. Hieraus folgt nach dem Prinzip der vollständigen Induktion $T = \mathbb{N}$.
 - Erste Inklusion: $\text{UVR}(S) \supset \bigcup_{n=1}^\infty S_n = \{\sum_{\nu=1}^n \alpha_\nu s_\nu \mid n \in \mathbb{N} \text{ und } (\alpha_\nu, s_\nu) \in k \times S\} =: \text{Lin}(S)$
 - Umgekehrt gilt (siehe 1.36 und 1.34): $\text{Lin}(S) \supset S_1 \supset S$.
 - Seien $\sum_{\nu=1}^n \alpha_\nu s_\nu =: a$; $\sum_{\mu=1}^m \beta_\mu t_\mu \in \text{Lin}(S)$ beliebig vorgegeben.

- Dann ist $a - b = \sum_{\nu=1}^n \alpha_\nu s_\nu + \sum_{\mu=1}^m (-\beta_\mu) t_\mu \in S_{n+m} \subset \text{Lin}(S)$ und nach dem Untergruppenkriterium ist $(\text{Lin}(S), +)$ eine Untergruppe von $(V, +)$.
- Sei $\sum_{\nu=1}^n \alpha_\nu s_\nu =: a \in \text{Lin}(S)$ beliebig vorgegeben. Dann ist $\rho a = \sum_{\nu=1}^n (\rho \alpha_\nu) s_\nu \in \text{Lin}(S)$ und es folgt, da $\rho \in K$ und $a \in \text{Lin}(S)$ beliebig, $K \cdot \text{Lin}(S) \subset \text{Lin}(S)$.
- Damit stellen wir fest $\text{Lin}(S) \in \text{UVR}^*$. Da nach dem Hauptsatz für Hüllensysteme aber auch $\text{Lin}(S) \supset \text{UVR}(S)$ gilt, folgt die Aussage:

$$\text{UVR}(S) = \text{Lin}(S)$$

(iii) Analog zeigt man diese Aussage wie bei \overline{S} und $\overline{\{b_1, \dots, b_n\}}$.

1.36 (A)

Zeige: Ist (G, \cdot) eine Gruppe, so gilt:

- (G, Ugr^*) mit $\text{Ugr}^* =: \{U \subset G \mid U \text{ ist Untergruppe von } (G, \cdot)\}$ ist ein Hüllensystem.
- Für alle $S \subset V$ mit $S \neq \{\}$ gilt

$$\text{Ugr}(S) = \{s_1^{\varepsilon_1} \cdot s_2^{\varepsilon_2} \cdot \dots \cdot s_n^{\varepsilon_n} \mid n \in \mathbb{N} \text{ und } s_\nu \in S \text{ und } \varepsilon_\nu \in \{+1, -1\}\}$$

Lösung

- Es gilt $G \in \text{Ugr}^*$.
 - Sei $\chi \subset \text{Ugr}^*$ beliebig vorgegeben.
 - Setze $\bigcap_{U \in \chi} U = \{x \in G \mid x \in U \forall U \in \chi\} =: D$, dann ist $1_G \in D$ und es folgt $D \neq \{\}$.
 - Seien $a, b \in D$ beliebig vorgegeben, dann sind $a, b \in U \forall U \in \chi$ und, da $U \in \text{Ugr}^*$, es folgt nach dem Untergruppenkriterium $ab^{-1} \in U \forall U \in \chi \rightsquigarrow ab^{-1} \in D \rightsquigarrow ab^{-1} \in D \forall a, b \in D$.
 - Damit ist $D \in \text{Ugr}^*$ und (G, Ugr^*) ist ein Hüllensystem.
- Setze für $n = 1, 2, 3, \dots$ $\{s_1^{\varepsilon_1}, s_2^{\varepsilon_2}, \dots, s_n^{\varepsilon_n} \mid (s_\nu \varepsilon_\nu) \in S \times \{+1, -1\}\} =: S_n$.
 - Setze $\{n \in \mathbb{N} \mid S_n \subset \text{Ugr}(S)\} =: T$.
 - Sei $s_1^{\varepsilon_1} \in S_1$ beliebig vorgegeben.
Dann ist $\begin{cases} \text{entweder} & \varepsilon_1 = +1 \rightsquigarrow s_1^{\varepsilon_1} = s_1 \in S \subset \text{Ugr}(S) \\ \text{oder} & \varepsilon_1 = -1 \rightsquigarrow s_1^{\varepsilon_1} = s_1^{-1} = 1_G s_1^{-1} \in \text{Ugr}(S) \end{cases}$. Daraus folgt $S \subset S_1 \subset \text{Ugr}(S)$ und weiter $1 \in T$.
 - Seien $n \in T$ und $s_1^{\varepsilon_1} \cdot s_2^{\varepsilon_2} \cdot \dots \cdot s_n^{\varepsilon_n} \cdot s_{n+1}^{\varepsilon_{n+1}} \in S_{n+1}$ beliebig vorgegeben.
 - Dann ist $s_1^{\varepsilon_1} \cdot \dots \cdot s_n^{\varepsilon_n} =: a \in \text{Ugr}(S)$ und $s_{n+1}^{\varepsilon_{n+1}} =: b \in S_1 \subset \text{Ugr}(S)$. Daraus folgt mit dem Untergruppenkriterium $s_1^{\varepsilon_1} \cdot \dots \cdot s_n^{\varepsilon_n} \cdot s_{n+1}^{\varepsilon_{n+1}} = ab^{-1} \in \text{Ugr}(S)$ und weiter $n+1 \in T \forall n \in T$.
 - Nach dem Prinzip der Vollständigen Induktion ist damit $T = \mathbb{N}$.
 - $\text{Ugr}(S) \supset \bigcup_{n=1}^{\infty} S_n = \{s_1^{\varepsilon_1}, \dots, s_n^{\varepsilon_n} \mid n \in \mathbb{N} \text{ und } (s_\nu \varepsilon_\nu) \in S \times \{+1, -1\}\} =: \langle S \rangle$.
 - Umgekehrt gilt $\langle S \rangle \supset S_1 \supset S \neq \{\}$.

- Seien $s_1^{\varepsilon_1} \cdot \dots \cdot s_n^{\varepsilon_n} =: a$; $t_1^{\eta_1} \cdot t_2^{\eta_2} \cdot \dots \cdot t_{m-1}^{\eta_{m-1}} \cdot t_m^{\eta_m} =: b \in \langle S \rangle$ beliebig vorgegeben.
- Dann ist $a \cdot b^{-1} = s_1^{\varepsilon_1} \dots s_n^{\varepsilon_n} \cdot t_m^{-\eta_m} \dots t_1^{-\eta_1} \in S_{m+n} \subset \langle S \rangle$. Nach dem Untergruppenkriterium folgt $\langle S \rangle \in \text{Ugr}^*$ und der Hauptsatz über Hüllensysteme besagt $\langle S \rangle \in \text{Ugr}(S)$, womit die Behauptung (ii) folgt: $\text{Ugr}(S) = \langle S \rangle$.

Bemerkung: Im Fall $S = \{a\}$ heißt $\langle \{a\} \rangle =: \langle a \rangle = \{a_1^{\varepsilon_1}, \dots, a_n^{\varepsilon_n} \mid n \in \mathbb{N} \mid \varepsilon_\nu \in \{+1, -1\}\} \stackrel{a^{-1}a^1=1_G}{=} \{a^\gamma \mid \gamma \in \mathbb{Z}\}$ die von $a \in G$ erzeugte zyklische Gruppe.

1.37 Nachtrag

Im Hüllensystem (V, Konvex^*) aller konvexen Teilmengen eines reellen Vektorraumes ${}_R V$ gilt stets:

(a) $\overline{\{\}} = \{\}$, denn $\{\}$ ist konvex.

(b)

$$\begin{aligned} \overline{\{p, q\}} &= \{\alpha p + \beta q \mid \alpha, \beta \in \mathbb{R}^+ \text{ und } \alpha + \beta = 1\} \\ &= \begin{cases} \{(\alpha + \beta)p = 1p\} = \{p\} & \text{falls } p = q \\ \overline{pq} & \text{falls } p \neq q \end{cases} \end{aligned}$$

1.38 (D+A)

Ist $(M, \text{Hülle}^*)$ ein Hüllensystem, so heißt die Abbildung

$$\text{Hülle} : \begin{cases} \text{Pot}(M) \rightarrow \text{Hülle}^* \\ A \mapsto \text{Hülle}(A) =: \bar{A} \end{cases}$$

der *Hüllenoperator des Hüllensystems* $(M, \text{Hülle}^*)$.

Zeige: Für alle $A, B \in \text{Pot}(M)$ gilt:

- (i) $\bar{A} \supset A$ (Extensionalität)³
- (ii) $\bar{\bar{A}} = \bar{A}$ (Idempotenz)
- (iii) Aus $A \supset B$ folgt stets $\bar{A} \supset \bar{B}$ (Monotonie).
- (iv) $\overline{A \cup B} = \bar{A} \cup \bar{B}$

Lösung

(i) Siehe Hauptsatz für Hüllensysteme (HSH).

- (ii) • $\bar{\bar{A}} \supset \bar{A}$ (wegen (i)).
- $\left. \begin{array}{l} \bar{A} \in \text{Hülle}^* \text{ lt. HSH} \\ \bar{A} \subset \bar{\bar{A}} \end{array} \right\} \leadsto \bar{\bar{A}} \subset \bar{A}$
- Es folgt die Aussage $\bar{\bar{A}} = \bar{A}$.

³wurde bereits in (1.30) gezeigt

- (iii) Angenommen $A \subset B$, dann ist wegen (i) auch $A \subset B \subset \bar{B}$, also $A \subset \bar{B}$, und da $B \in \text{Hülle}^*$ folgt nach dem HSH $\bar{A} \subset \bar{B}$.

- (iv) • $\left. \begin{array}{l} \bar{A} \supset A \\ \bar{B} \supset B \end{array} \right\} \rightsquigarrow \bar{A} \cup \bar{B} \supset A, B \rightsquigarrow \bar{A} \cup \bar{B} \supset A \cup B \stackrel{(iii)}{\rightsquigarrow} \overline{\bar{A} \cup \bar{B}} \supset \overline{A \cup B}$
- $A \cup B \left\{ \begin{array}{l} \supset A \\ \supset B \end{array} \right\} \rightsquigarrow \overline{A \cup B} \supset \left\{ \begin{array}{l} \bar{A} \\ \bar{B} \end{array} \right\} \rightsquigarrow \overline{A \cup B} \supset \bar{A} \cup \bar{B}$
- Wegen (iii) ist $\overline{\bar{A} \cup \bar{B}} \supset \overline{\bar{A} \cup \bar{B}}$ und nach (ii) folgt weiter $\overline{A \cup B} = \overline{\bar{A} \cup \bar{B}} \supset \overline{\bar{A} \cup \bar{B}}$.
- Damit ist $\overline{A \cup B} = \overline{\bar{A} \cup \bar{B}}$.

1.39 (S)

Zu zwei verschiedenen Punkten $p \neq q$ eines reellen Vektorraumes ${}_{\mathbb{R}}V$ existiert stets genau eine Gerade $G_a^u \in \mathcal{G}({}_{\mathbb{R}}V)$, die $p \in G_a^u$ und $q \in G_a^u$ genügt. Dies ist die Gerade $\overline{pq} = G_a^{q-p}$.

Beweis

- Sei $G_a^u \in \mathcal{G}({}_{\mathbb{R}}V)$ eine beliebig vorgegebene Gerade, die $p \in G_a^u$ und $q \in G_a^u$ genügt.
- Nach Definition sind die Punkte p und q darstellbar als $p =: a + \alpha u$ bzw. $q = a + \beta u$ mit $\alpha, \beta \in \mathbb{R}$.
- $q - p = (\beta - \alpha)u$ mit $\beta \neq \alpha$, da $p \neq q$
- Es folgt $u = (\beta - \alpha)^{-1}(q - p)$ und weiter $\mathbb{R}u = \mathbb{R}(\beta - \alpha)^{-1}(q - p)$ und, da $\mathbb{R}(\beta - \alpha)^{-1} = \mathbb{R}$, $\mathbb{R}u = \mathbb{R}(q - p)$.
- $G_a^u = a + \mathbb{R}u = (p - \alpha u) + \mathbb{R}u = p + (\mathbb{R} - \alpha)u \stackrel{\mathbb{R} - \alpha = \mathbb{R}}{=} p + \mathbb{R}u = p + \mathbb{R}(q - p) = G_p^{q-p} = \overline{pq}$
- Demnach genügt höchstens $G = G_p^{q-p} \in \mathcal{G}({}_{\mathbb{R}}V)$ der Anforderung $p, q \in G$. Umgekehrt gilt $p = p + 0(q - p)$, $q = p + 1(q - p) \in G_p^{q-p}$.

1.40 (D)

Die Schreibweise $A \cap B = c$ bedeutet: Es gilt

- (a) A, B sind Mengen mit $|A \cap B| = 1$ und
- (b) c ist das eindeutig bestimmte Element von $A \cap B$, d.h. es gilt $A \cap B = \{c\}$.

Heuristik: Existenz einer Senkrechten

Wann steht im \mathbb{R}^2 oder im \mathbb{R}^3 eine Gerade G_b^v auf einer Geraden G_a^u senkrecht? Es muss offenbar gelten:

- (1) $G_a^u \cap G_b^v =: p$
- Für $p - u, p + u \in G_a^u$ gilt $\frac{(p - u) + (p + u)}{2} = p$, damit folgt:

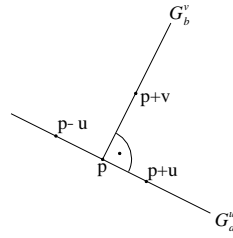


Abbildung 1.7: Zur Definition der Senkrechten

(2) p ist der Mittelpunkt der Strecke $\overline{p-u, p+u}$.

Wegen (1) gilt $p = b + \rho v$ mit einem $\rho \in \mathbb{R}$, man kann daher auch schreiben:

(3) $p + v = b + (\rho + 1)v \in G_b^v \setminus \{p\}$

(4) $\angle(p-u, p, p+v) = \angle(p+u, p, p+v) = 90^\circ$

Die Strahlensätze ermöglichen nun eine Argumentationskette:

$$\begin{aligned}
 \Delta(p-u, p, p+v) &\equiv \Delta(p+u, p, p+v) \\
 &\Leftrightarrow d(p+v, p-u) = d(p+v, p+u) \\
 &\Leftrightarrow ((p+v) - (p-u))^2 = ((p+v) - (p+u))^2 \\
 &\Leftrightarrow (v+u)^2 = (v-u)^2 \\
 &\Leftrightarrow v^2 + 2(v \circ u) + u^2 = v^2 - 2(v \circ u) + u^2 \\
 &\Leftrightarrow 4(v \circ u) = 0_{\mathbb{R}} \\
 &\Leftrightarrow v \circ u = 0_{\mathbb{R}} \\
 &\stackrel{[E4]}{\Leftrightarrow} u \circ v = 0
 \end{aligned}$$

Dies motiviert die folgende Definition.

1.41 (D)

Ist $(_{\mathbb{R}}V)$ ein EVR, so heißen zwei Geraden G_a^u, G_b^v zueinander orthogonal, in Zeichen $G_a^u \perp G_b^v$, wenn gilt:

(a) $G_a^u \cap G_b^v \neq \{\}$

(b) $u \circ v = 0$

1.42 (S)

Aus $G_a^u \perp G_b^v$ folgt $|G_a^u \cap G_b^v| = 1$.

Beweis

- Sei $G_a^u \perp G_b^v$, dann gilt $u \circ v = 0$.
- Angenommen $G_a^u = G_b^v$, dann wäre wegen $a = a + 0u \in G_a^u$ auch $a \in G_b^v$ und man könnte schreiben $a =: b + \alpha v$ mit einem $\alpha \in \mathbb{R}$.
- Dann wäre aber auch $G_b^v = b + \mathbb{R}v = (a - \alpha v) + \mathbb{R}v = a + (\mathbb{R} - \alpha)v \stackrel{\mathbb{R}-\alpha=\mathbb{R}}{=} a + \mathbb{R}v = G_a^v$.

- Also $G_a^v = G_b^u \stackrel{\text{Ann.}}{=} G_a^u$, folglich $a + u = a + \rho v$ mit einem $\rho \in \mathbb{R}$.
- Weiterhin ist $u = \rho v$ mit $\rho \neq 0$, da sonst $u = 0v = 0$ q.e.a.
- Mit o.g. Annahme ergibt sich also $v \circ v = \rho v \circ v = \rho v^2 \neq 0$ q.e.a.
- Demnach ist die Annahme nicht haltbar: $G_a^u \neq G_b^v$ und gemäß (1.39) und (1.41 (a)) folgt $|G_a^u \cap G_b^v| = 1$.

Heuristik: Eindeutigkeit einer Lotgeraden

Seien ein EVR $(\mathbb{R}V, \circ)$ und $(x, G_a^u) \in V \times \mathcal{G}(\mathbb{R}V)$ mit $x \notin G_a^u$ beliebig vorgegeben. Ist G_b^v eine Gerade, die

$$(+) \quad x \in G_b^v \text{ und } G_b^v \perp G_a^u$$

genügt, so muß gelten:

- $G_a^u \cap G_b^v =: p$, woraus folgt $p = a + \rho u = b + \beta v$ mit $\rho, \beta \in \mathbb{R}$.
- Setze $x = b + \xi v$ mit $\xi \in \mathbb{R}$.
- Dann ist $x - p = (\xi - \beta)v$ mit $\xi \neq \beta$, da $x \notin G_a^u \ni p$. Demnach ist $v = (\xi - \beta)^{-1}(x - p)$.
- $\mathbb{R}v = \mathbb{R}(\xi - \beta)^{-1}(x - p) = \mathbb{R}(x - p)$, da $\mathbb{R}(\xi - \beta)^{-1} = \mathbb{R}$.
- Da $p, x \in G_b^v$, folgt nach (1.39) $G_b^v = \overline{xp} = G_x^{x-p}$.
- $(p - x) \circ u = ((\xi - \beta)v) \circ u = 0$ nach Voraussetzung; demzufolge gilt $[(a + \rho u) - x] \circ u = (a - x) \circ u + \rho u^2 = 0$.
- Da $u^2 > 0$ erhält man $\rho = \frac{(x - a) \circ u}{u^2}$ bzw. $p = a + \frac{(x - a) \circ u}{u^2}u$ und weiter $x - p = (x - a) + \frac{(a - x) \circ u}{u^2}u$.
- Also gilt $G_b^v = G_x^{x-p} = G_x^{(x-a) + \frac{(a-x) \circ u}{u^2}u} =: G_x^w$ mit $w := (x - a) + \frac{(a - x) \circ u}{u^2}u$.

Damit ist zu jeder bzw. jedem beliebig vorgegebenen $G_a^u \in \mathcal{G}(\mathbb{R}V)$ und $x \in V \setminus G_a^u$ höchsten G_x^w eine Gerade, die (+) genügt.

Umgekehrt gilt:

- Angenommen $w = (x - a) + \frac{(a - x) \circ u}{u^2}u = 0_V \Leftrightarrow (x - a) = \frac{(x - a) \circ u}{u^2}u \Leftrightarrow x = a + \frac{(x - a) \circ u}{u^2}u \Leftrightarrow x \in G_a^u$.
- Aus $x \notin G_a^u$ folgt also $w \neq 0_V$.
- Weiterhin ist $x = x + 0w \in G_x^w$.
- Es gilt $G_a^u \ni p = a + \frac{(x - a) \circ u}{u^2}u = x + (-1) \left[(x - a) + \frac{(a - x) \circ u}{u^2}u \right] = x + (-1)w \in G_x^w$, also $G_a^u \cap G_b^v \neq \{\}$.
- $u \circ w = u \circ \left[(x - a) + \frac{(a - x) \circ u}{u^2}u \right] = u \circ (x - a) + \frac{(a - x) \circ u}{u^2}u^2 = 0$

Damit genügt G_x^w der Bedingung (+) und $G_x^w \in \mathcal{G}(\mathbb{R}V)$. Man hat demnach eine eindeutige Lotgerade.

1.43 (S+D)

Ist $\mathbb{R}V$ ein EVR, so gibt es zu beliebig vorgegebenen $(x, G_a^u) \in V \times \mathcal{G}(\mathbb{R}V)$ mit $x \notin G_a^u$ stets genau eine Gerade $G_b^v \in \mathcal{G}(\mathbb{R}V)$, die

$$x \in G_b^v \text{ und } G_b^v \perp G_a^u$$

genügt.

$G_b^v =: (x \perp G_a^u)$ heißt die *Lotgerade auf die Gerade G_a^u durch den Punkt x* . $G_a^u \cap (x \perp G_a^u) =: p$ heißt der *Fußpunkt des Lotes von x auf die Gerade G_a^u* und es gilt

$$(x \perp G_a^u) = G_p^{x-p} \text{ mit } p = \frac{(x-a) \circ u}{u^2} u$$

1.44 Heuristik

Es seien $b \neq a \neq c$ Punkte im \mathbb{R}^2 oder \mathbb{R}^3 .

Wie berechnet man die Größe des anschaulich vorliegenden Winkels $\angle(b, a, c)$, unter dem sich die Geraden \overline{ab} und \overline{ac} schneiden?

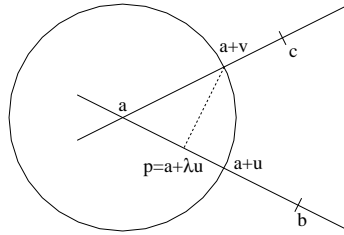


Abbildung 1.8: Zur Definition des Winkels

- Setze $\frac{1}{\|b-a\|}(b-a) =: u$ und $\frac{1}{\|c-a\|}(c-a) =: v$.
- Dann sind $u^2 = \frac{1}{\|b-a\|^2}(b-a)^2 = 1$ und $v^2 = \frac{1}{\|c-a\|^2}(c-a)^2 = 1$.
- Nach (1.20) ist $\overline{ab} = G_a^{b-a} = a + \mathbb{R}(b-a) = a + \mathbb{R}\frac{1}{\|b-a\|}(b-a) = a + \mathbb{R}u = G_a^u$
analog: $\overline{ac} = G_a^{a-c} = G_a^v$
- $d(a+u, a) = \|(a+u) - a\| = \|u\| = 1$
 $d(a+v, a) = \|(a+v) - a\| = \|v\| = 1$
- Ist E eine Ebene im \mathbb{R}^3 , die die Punkte $b \neq a \neq c$ enthält, so liegen die Punkte $a+u \in \overline{ab}$ und $a+v \in \overline{ac}$ auf dem Kreis K in E mit dem Mittelpunkt a und dem Radius 1.
- Die Länge φ des kürzesten Kreisbogens von $a+u$ nach $a+v$ heißt das *Bogenmaß* des Winkels $\angle(b, a, c)$. Es ist also stets $0 \leq \varphi(\angle(b, a, c)) \leq \pi$.
- Ist $p = a + \lambda u$ der Fußpunkt des Lotes von $a+v$ auf $\overline{ab} = G_a^u$, so gilt laut (1.43)
 $p = a + \frac{(a+v-a) \circ u}{u^2} u$, also $\lambda = \frac{v \circ u}{u^2} = u \circ v$ mit $|\lambda| = |u \circ v| \leq \sqrt{u^2} \sqrt{v^2} = 1$.
- Demzufolge ist $-1 \leq \lambda \leq 1$. Demzufolge ist $\lambda = 1$, genau dann wenn $\varphi = 1$;
 $\lambda = 0$ genau dann, wenn $\varphi = \frac{\pi}{2}$ und $\lambda = -1$ genau dann, wenn $\varphi = \pi$.

- Es folgt aus $0 < \lambda < 1$, daß $\varphi \in]0, \frac{\pi}{2}[$ bzw. aus $-1 < \lambda < 0$, daß $\varphi \in]\frac{\pi}{2}, \pi[$.
- Es heißt λ der *Cosinus* des von den Geraden \overline{ab} und \overline{ac} eingeschlossenen Winkels (Definition des Cosinus am Einheitskreis), also

$$\lambda = u \circ v = \frac{(b-a) \circ (c-a)}{\|b-a\| \cdot \|c-a\|} = \cos \angle(b, a, c)$$

1.45 (D)

Ist $({}_n\mathbb{R}V, \circ)$ ein EVR und sind $a, b, c \in V$ mit $b \neq a \neq c$, so gilt laut (1.44): $(b-a) \circ (c-a) \leq \|b-a\| \cdot \|c-a\|$ und es heißt die reelle Zahl

$$-1 \leq \frac{(b-a) \circ (c-a)}{\|b-a\| \cdot \|c-a\|} \leq 1$$

der *Cosinus des von den Geraden $\overline{ab}, \overline{ac}$ eingeschlossenen Winkels*; respektive $\arccos \frac{(b-a) \circ (c-a)}{\|b-a\| \cdot \|c-a\|}$ die *Größe des von \overline{ab} und \overline{ac} eingeschlossenen Winkels*.

1.46 (D)

Sind $A, B \subset M$ nichtleere Teilmengen eines metrischen Raumes (M, d) , so heißt

$$d(A, B) := \inf\{d(a, b) \mid a \in A \text{ und } b \in B\} \geq 0$$

der *Abstand der Menge A von den Menge B* .

Gilt $A = \{a\}$ resp. $B = \{b\}$ resp. $A = \{a\}$ und $B = \{b\}$, so wird anstatt $d(\{a\}, B)$ resp. $d(A, \{b\})$ resp. $d(\{a\}, \{b\})$. auch kürzer $d(a, B)$ resp. $d(A, b)$ resp. $d(a, b)$ geschrieben.

1.47 (S)

Ist $({}_R V, \circ)$ ein EVR, $G_a^u \in \mathcal{G}({}_R V)$ und $x \in V$, so gibt es genau ein $p \in G_a^u$ mit der Eigenschaft $d(x, G_a^u) = d(x, p)$ Und es ist

$$p = \begin{cases} x & \text{falls } x \in G_a^u \\ a + \frac{(x-a) \circ u}{u^2} u = G_a^u \cap (p \perp G_a^u) & \text{falls } x \notin G_a^u \end{cases}$$

und

$$d(x, p) = \begin{cases} 0 & \text{falls } x \in G_a^u \\ \sqrt{(x-a)^2 - \frac{[(x-a) \circ u]^2}{u^2}} & \text{falls } x \notin G_a^u \end{cases}$$

Beweis

- Sei $G_a^u \in \mathcal{G}({}_R V)$ und $x \in V$ beliebig vorgegeben.
- Im Fall $x \in G_a^u$ gilt für alle $q \in G_a^u \setminus \{x\}$ $d^2(x-q) = x-q^2 > 0 = d^2(x, x)$.
- Im Fall $x \notin G_a^u$ gilt $(x \perp G_a^u) \cap G_a^u =: p = a + \frac{(x-a) \circ u}{u^2} u = a + \pi u$.
- Es ist $G_p^u = (a + \pi u) + \mathbb{R}u = a + (\pi + \mathbb{R})u = a + \mathbb{R}u = G_a^u$.

- Sei $q \in G_a^u \setminus \{p\}$ beliebig vorgegeben. Dann ist $q = p + \rho u$ mit $\rho \neq 0$.
- Daraus folgt $d^2(x, q) = (x - q)^2 = [(x - p) - \rho u]^2 = (x - p)^2 - 2\rho(x - p) \circ u + \rho^2 u^2$.
- Es ist $(x - p) \circ u = \left[(x - a) - \frac{(x - a) \circ u}{u^2} u \right] \circ u = (x - a) \circ u - \frac{(x - a) \circ u}{u^2} u^2 = 0$.
- Demzufolge ist $d^2(x, q) = (x - p)^2 + \rho^2 u^2 > (x - p)^2 = d^2(x, p)$. Weiterhin folgt $d(x, p) = d(x, G_a^u)$ und $d(x, q) > d(x, p)$ für alle $q \in G_a^u \setminus \{p\}$.
- Es ist

$$\begin{aligned} (x - p)^2 &= \left((x - a) - \frac{(x - a) \circ u}{u^2} u \right)^2 \\ &= (x - a)^2 - 2 \frac{(x - a) \circ u}{u^2} (x - a) \circ u + \frac{[(x - a) \circ u]^2}{(u^2)^2} u^2 \\ &= (x - a)^2 - \frac{[(x - a) \circ u]^2}{u^2} > 0 \end{aligned}$$

- Damit ist $d(x, p) = \sqrt{(x - a)^2 - \frac{[(x - a) \circ u]^2}{u^2}} > 0$.

1.48 (A)

Berechne im kanonischen 3-dimensionalen EVR (\mathbb{R}^3, \circ)

- $(x \perp G_a^u)$
- $G_a^u \cap (x \perp G_a^u)$
- $d(x, G_a^u)$

für $x = (0, 0, 1)$, $a = (1, 0, 0)$ und $u = (1, 1, 1)$.

Lösung

Für den Fußpunkt p des Lotes von x auf G_a^u gilt

$$\begin{aligned} p &= a + \frac{(x - a) \circ u}{u^2} \cdot u \\ &= (1, 0, 0) + \frac{(-1, 0, 1) \circ (1, 1, 1)}{(1, 1, 1)^2} \cdot (1, 1, 1) \\ &= (1, 0, 0) + \frac{(-1 + 0 + 1)}{3} \cdot (1, 1, 1) \\ &= (1, 0, 0) \end{aligned}$$

Damit ist $x - p = (-1, 0, 1)$ und $(x \perp G_a^u) \stackrel{(1.46)}{=} G_x^{x-p} = G_{(0,0,1)}^{(-1,0,1)} = \{(\rho, 0, \rho + 1) \mid \rho \in \mathbb{R}\}$.

$$\begin{aligned} d(x, G_a^u) &= \sqrt{(x - a)^2 - \frac{[(x - a) \circ u]^2}{u^2}} \\ &= \sqrt{(-1, 0, 1)^2 - \frac{[(-1, 0, 1) \circ (1, 1, 1)]^2}{(1, 1, 1)^2}} \\ &= \sqrt{2 - \frac{0}{3}} = \sqrt{2} \end{aligned}$$

1.49 Heuristik

Es sein G_a^u eine Gerade im \mathbb{R}^2 oder im \mathbb{R}^3 .

Wann ist eine Gerade $G_b^v \neq G_a^u$ zu G_a^u parallel?

G_b^v ist zu G_a^u anschaulich genau dann parallel, wenn $d(x, G_a^u) = d(y, G_a^u) =: \delta$ konstant ist ($\delta > 0$) für alle $x, y \in G_b^v$.

- Für alle $x =: b + \rho v \in G_b^v$ gilt:

$$\begin{aligned}
 & d(b + \rho v, G_a^u) = d(b, G_a^u) \\
 \Leftrightarrow_{(1.47)} & (b + \rho v - a)^2 - \frac{[(b + \rho v - a) \circ u]^2}{u^2} = (b - a)^2 - \frac{[(b - a) \circ u]^2}{u^2} \\
 & \Leftrightarrow_{(b-a)=:w} (w + \rho v)^2 - \frac{[(w + \rho v) \circ u]^2}{u^2} = w^2 - \frac{[w \circ u]^2}{u^2} \\
 \Leftrightarrow & w^2 + 2\rho(w \circ v) + \rho^2 v^2 - \frac{[w \circ u + \rho v \circ u]^2}{u^2} = w^2 - \frac{[w \circ u]^2}{u^2} \\
 \Leftrightarrow & 2\rho(w \circ v) + \rho^2 v^2 - \frac{(w \circ v)^2 + 2\rho(w \circ u) \cdot (v \circ u) + \rho^2 (v \circ u)^2}{u^2} = -\frac{(w \circ u)^2}{u^2} \\
 \Leftrightarrow & \rho^2 v^2 + 2\rho(w \circ v) = \frac{2\rho(w \circ u) \cdot (v \circ u) + \rho^2 (v \circ u)^2}{u^2} \\
 \Leftrightarrow & \rho^2 u^2 v^2 + 2\rho u^2 (w \circ v) = 2\rho(w \circ u) \cdot (v \circ u) + \rho^2 (v \circ u)^2 \\
 \Leftrightarrow & \rho^2 [u^2 v^2 - (v \circ u)^2] + 2\rho [u^2 (w \circ v) - (w \circ u) \cdot (v \circ u)] = 0
 \end{aligned}$$

Folglich ist $u^2 v^2 - (v \circ u)^2 = 0 = u^2 (w \circ v) - (w \circ u) \cdot (v \circ u)$.

- Zwischenresultat: $G_b^v \parallel G_a^u \Leftrightarrow u^2 v^2 - (v \circ u)^2 = 0 = u^2 (w \circ v) - (w \circ u) \cdot (v \circ u)$.
- Angenommen $\mathbb{R}u = \mathbb{R}v$, dann wäre $u \in \mathbb{R}v$, da $u = 1u \in \mathbb{R}u$. Setze $u = \alpha v$ mit einem $\alpha \in \mathbb{R} \setminus \{0\}$.
- Dann folgt

$$\left\{ \begin{array}{l} u^2 v^2 = (\alpha v)^2 v^2 = (\alpha^2 v^2) v^2 \\ (u \circ v)^2 = ((\alpha v) \circ v)^2 = (\alpha v^2)^2 = \alpha^2 (v^2)^2 \end{array} \right\} \leadsto u^2 v^2 - (u \circ v)^2 = 0$$

- Weiterhin ist

$$\begin{aligned}
 u^2 (w \circ v) - (w \circ u) (v \circ u) &= (\alpha v^2 (w \circ v) - (w \circ (\alpha v)) \cdot (v \circ (\alpha v))) \\
 &= \alpha^2 v^2 (w \circ v) - \alpha (w \circ v) \alpha v^2 \\
 &= 0 \leadsto G_b^v \parallel G_a^u.
 \end{aligned}$$

- Zwischenresultat: $G_b^v \parallel G_a^u$, falls $\mathbb{R}u = \mathbb{R}v$.
- Angenommen $G_b^v \parallel G_a^u$.
- Es ist

$$\begin{aligned}
 v^2 \left(u - \frac{u \circ v}{v^2} v \right)^2 &= v^2 \left(u^2 - 2 \frac{u \circ v}{v^2} (u \circ v) + \frac{u \circ v}{(v^2)^2} v^2 \right) \\
 &= v^2 \left(u^2 - \frac{(u \circ v)^2}{v^2} \right) \\
 &= u^2 v^2 - (u \circ v)^2 \\
 &= 0
 \end{aligned}$$

Damit folgt

$$\left(u - \frac{u \circ v}{v^2} v \right)^2 = 0$$

- Folglich gilt $u = \frac{u \circ v}{v^2} v = \alpha v$ mit $\alpha \neq 0_{\mathbb{R}}$ (da sonst $u = 0v = 0v$) und weiter $\mathbb{R}u = \mathbb{R}(\alpha v) = \mathbb{R}v$.
- Resultat: Aus $G_b^v \parallel G_a^u$ folgt $\mathbb{R}u = \mathbb{R}v$.

1.50 (D)

Ist $(\mathbb{R}V, \circ)$ ein EVR, so setzt man für alle $(G_b^v, G_a^u) \in \mathcal{G}(\mathbb{R}V) \times \mathcal{G}(\mathbb{R}V)$:
 $G_b^v \parallel G_a^u$ – lies G_b^v ist parallel zu G_a^u – gilt dann und nur dann, wenn auch $\mathbb{R}u = \mathbb{R}v$ gilt.

1.51 (A)

Es seien $a_5 := a_1, a_2, a_3, a_4$ vier verschiedene Punkte in einem EVR $(\mathbb{R}V, \circ)$ und m_i für $i = 1, 2, 3, 4$ die Mittelpunkte der Strecken $\overline{a_i a_{i+1}}$.

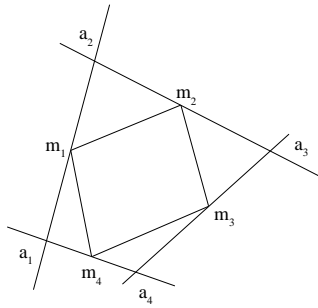


Abbildung 1.9: Skizze zu Aufgabe 1.51

Zeige: Dann gilt:

- $m_1 \neq m_2 \neq m_3 \neq m_4 \neq m_1$
- Die Punkte m_1, m_2, m_3, m_4 liegen entweder alle auf einer Geraden oder sie bilden ein Parallelogramm, d.h. es gilt:
 $\overline{m_1 m_2} \parallel \overline{m_3 m_4}$ und $\overline{m_2 m_3} \parallel \overline{m_4 m_1}$ mit $\overline{m_1 m_2} \cap \overline{m_3 m_4} = \{\} = \overline{m_2 m_3} \cap \overline{m_4 m_1}$

Lösung

- Angenommen $m_1 = m_2$, dann wäre $\frac{a_1 + a_2}{2} = \frac{a_2 + a_3}{2}$, bzw. $a_1 + a_2 = a_2 + a_3 \rightsquigarrow a_1 = a_3$ q.e.a.
 Folglich ist $m_1 \neq m_2$.
- Allgemein: Angenommen $m_i = m_{i+1}$, dann wäre $\frac{a_i + a_{i+1}}{2} = \frac{a_{i+1} + a_{i+2}}{2}$
 bzw. $a_i + a_{i+1} = a_{i+1} + a_{i+2} \rightsquigarrow a_i = a_{i+2}$ q.e.a.
 Folglich ist $m_i \neq m_{i+1}$.
- Es ist $\overline{m_1 m_2} = G_{m_1}^{m_2 - m_1}$ und $\overline{m_3 m_4} = G_{m_3}^{m_4 - m_3}$ mit

$$m_4 - m_3 = \frac{a_4 + a_1}{2} - \frac{a_3 + a_4}{2} = \frac{a_1 - a_3}{2}$$

und

$$m_2 - m_1 = \frac{a_2 + a_3}{2} - \frac{a_1 + a_2}{2} = \frac{a_3 - a_1}{2}$$

- Daraus folgt

$$\begin{aligned}
 \mathbb{R}(m_4 - m_3) &= \mathbb{R}\left(\frac{1}{2}(a_1 - a_3)\right) \\
 &= (\mathbb{R} \cdot \frac{1}{2})(a_1 - a_3) \\
 &= \mathbb{R}(a_1 - a_3) \\
 &= \mathbb{R}\left(-\frac{1}{2}(a_3 - a_1)\right) \\
 &= \mathbb{R}(m_2 - m_1)
 \end{aligned}$$

Folglich ist $\overline{m_1 m_2} \parallel \overline{m_3 m_4}$.

- Analog zeigt man $\overline{m_2 m_3} \parallel \overline{m_4 m_1}$.
- (ii) • Angenommen, es existiert ein $p \in \overline{m_1 m_2} \cap \overline{m_3 m_4}$, dann wäre $p \in G_{m_1}^{m_2 - m_1}$ bzw. $p = m_1 + \rho(m_2 - m_1)$ mit einem $\rho \in \mathbb{R}$.
- Es folgt:

$$\begin{aligned}
 G_p^{m_2 - m_1} &= m_1 + \rho(m_2 - m_1) + \mathbb{R}(m_2 - m_1) \\
 &= m_1 + (\rho + \mathbb{R})(m_2 - m_1) \\
 &\stackrel{\rho + \mathbb{R} = \mathbb{R}}{=} m_1 + \mathbb{R}(m_2 - m_1) \\
 G_{m_1}^{m_2 - m_1} &= \overline{m_1 m_2}
 \end{aligned}$$

- Analog gilt $G_p^{m_4 - m_3} = G_{m_3}^{m_4 - m_3} = \overline{m_3 m_4}$
- Demzufolge ist

$$\overline{m_1 m_2} = G_p^{m_2 - m_1} = p + \mathbb{R}(m_2 - m_1) = p + \mathbb{R}(m_4 - m_3) = \overline{m_3 m_4}$$

d.h. $m_1, m_2, m_3, m_4 \in \overline{m_1 m_2} = \overline{m_3 m_4}$

- Angenommen, es existiert ein $p \in \overline{m_2 m_3} \cap \overline{m_4 m_1}$, dann wäre $\overline{m_2 m_3} = \overline{m_4 m_1}$ und es folgt $m_1, m_2, m_3, m_4 \in \overline{m_2 m_3} = \overline{m_1 m_4}$.

1.52 (A)

Zeige: Ist α eine Bewegung eines EVR $(\mathbb{R}V, \circ)$, so gilt für alle

- (I) $(m, \rho) \in V \times \mathbb{R}^+ : [S(m, \rho)]^\alpha = \{x^\alpha \mid x \in S(m, \rho)\} = S(m^\alpha, \rho)$
- (II) $a, b \in V$ mit $a \neq b : \overline{ab}^\alpha = \{x^\alpha \mid x \in \overline{ab}\} = \overline{a^\alpha b^\alpha}$
- (III) $a, b, c \in V$ mit $a \neq b \neq c : \varphi(\angle(a^\alpha, b^\alpha, c^\alpha)) = \varphi(\angle(a, b, c))$
- (IV) $G, H \in \mathcal{G}(\mathbb{R}V) :$
 - (i) $G^\alpha \perp H^\alpha$, falls $G \perp H$
 - (ii) $G^\alpha \parallel H^\alpha$, falls $G \parallel H$

Lösung

Laut Vorlesung gilt:

VL1 Sei (M, d) ein metrischer Raum.

- (a) $\gamma \in \text{Bij}(M)$ heißt Bewegung, wenn gilt: $d(a^\alpha, b^\alpha) = d(a, b) \forall a, b \in M \times M$.

- (b) $\mathcal{B}(M, d) =: \{\gamma \in \text{Bij}(M) \mid \gamma \text{ ist Bewegung}\}$ ist Untergruppe von $(\text{Bij}(M), \cdot)$.

VL2 Jeder EVR $(\mathbb{R}V, \circ)$ wird durch $d : \begin{cases} V \times V \rightarrow \mathbb{R} \\ (a, b) \mapsto d(a, b) := \|a - b\| := \sqrt{(a - b)^2} \end{cases}$ zu einem metrischen Raum (V, d) .

VL3 Für $\alpha \in \text{Bij}(V)$ sind äquivalent:

- (a) $\alpha \in \mathcal{B}(V, d)$
 (b) $\alpha : \begin{cases} V \rightarrow V \\ x \mapsto x^\alpha = x^\rho + t \end{cases} \quad \rho \in \text{Bij}(V) \text{ mit } (u \circ v)^\rho = u^\rho \circ v^\rho$
 für alle $u, v \in V$ und $t \in V$

VL4 Eine skalarprodukttreue Bijektion ρ ist eine lineare Abbildung, d.h für alle $(\rho, u, v) \in \mathbb{R} \times V \times V$ gilt:

- (a) $(\rho u)^\rho = \rho u^\rho$
 (b) $(u + v)^\rho = u^\rho + v^\rho$

Es ist $0_V^\rho + 0_V^\rho \stackrel{\text{VL4}}{=} (0_v + 0_v)^\rho = 0_V^\rho = 0_v \rightsquigarrow 0_V^\rho = 0_v$.

VL5 Ist ρ eine skalarprodukttreue Bijektion, so gilt $0_V^\rho = 0_v$ und $u^\rho \neq 0_v$, falls $u \neq 0_v$.

Beweis

- (I) • Seien $(m, \rho) \in V \times \mathbb{R}^+$ und $x \in S(m, \rho)$ beliebig vorgegeben.
 • Dann ist

$$\begin{aligned} (m^\alpha - x^\alpha)^2 &\stackrel{\text{VL3}}{=} [(m^\varphi + t) - (x^\varphi + t)]^2 \\ &= [m^\varphi - x^\varphi]^2 \\ &\stackrel{\text{VL4}}{=} (m - x)^{\varphi^0} (m - x)^\varphi \\ &\stackrel{\text{VL3}}{=} (m - x) \circ (m - x) = (m - x)^2 \\ &\stackrel{x \in S(m, \varphi)}{=} \rho^2 \end{aligned}$$

- Daraus folgt $x^\varphi \in S(m^\varphi, \rho)$ und weiter $[S(m, \rho)]^\alpha \subset S(m^\alpha, \rho)$ für alle $(m, \rho, \alpha) \in V \times \mathbb{R}^+ \times \mathcal{B}(M, d)$.
 • Dies läßt sich auf $S(m^\alpha, \rho)$ mit $\alpha^{-1} \stackrel{\text{VL2}}{\in} \mathcal{B}(V, d)$ anwenden und liefert:

$$[S(m^\alpha, \rho)]^{\alpha^{-1}} \subset S\left((m^\alpha)^{\alpha^{-1}}\right) = S(m, \rho)$$

- Damit folgt

$$S(m^\alpha, \rho) = S(m^\alpha, \rho)^{\alpha^{-1} \cdot \alpha} \subset S(m, \rho)^\alpha \subset S(m^\alpha, \rho)$$

und weiter $[S(m, \rho)]^\alpha = S(m^\alpha, \rho)$.

- Sei $G_a^u = \{a + \rho u \mid \rho \in \mathbb{R}\} \in \mathcal{G}(\mathbb{R}V)$ beliebig vorgegeben.

- Dann ist

$$\begin{aligned}
 (G_a^u)^\alpha &= \{(a + \rho u)^\alpha \mid \rho \in \mathbb{R}\} \\
 &\stackrel{\text{VL3}}{=} \{(a + \rho u)^\varphi + t \mid \rho \in \mathbb{R}\} \\
 &\stackrel{\text{VL4}}{=} \{a^\varphi + (\rho u)^\varphi + t \mid \rho \in \mathbb{R}\} \\
 &\stackrel{\text{VL4}}{=} \{(a^\varphi + t) + \rho(u^\varphi) \mid \rho \in \mathbb{R}\} \\
 &\stackrel{\text{VL2}}{=} a^\alpha + \mathbb{R}u^\varphi \\
 &= G_a^{u^\varphi}
 \end{aligned}$$

- $\leadsto (G_a^u)^\alpha = G_{a^\alpha}^{u^\alpha} \in \mathcal{G}(\mathbb{R}V)$ für alle $G_a^u \in \mathcal{G}(\mathbb{R}V)$.

(II) • Setze $\overline{ab} =: A$ $\overline{a^\alpha b^\alpha} =: B$.

- Dann ist $\begin{cases} \alpha|_A \in \text{Abb}(A, B) \\ \alpha^{-1}|_B \in \text{Abb}(B, A) \end{cases}$

- Es ist $\alpha|_A \alpha^{-1}|_B = \text{id}_B$ und $\alpha^{-1}|_B \alpha|_A = \text{id}_A$ und mit (2.25) folgt daraus $\alpha|_A \in \text{Bij}(A, B)$.

- Folglich gilt: $\overline{ab}^\alpha = (G_a^{b-a})^\alpha = G_{a^\alpha}^{(b-a)^\varphi} \stackrel{\text{VL4}}{=} G_{a^\alpha}^{b^\varphi - a^\varphi} = G_{a^\alpha}^{(b^\varphi + t) - (a^\varphi + t)} \stackrel{\text{VL3}}{=} G_{a^\alpha}^{b^\alpha - a^\alpha} = \overline{a^\alpha b^\alpha}$

(III) • Seien $u, v, r, s \in V$ beliebig vorgegeben.

- Dann gilt

$$\begin{aligned}
 &(u^\alpha - v^\alpha) \circ (r^\alpha - s^\alpha) \\
 &\stackrel{\text{VL3}}{=} ((u^\varphi + t) - (v^\varphi + t)) \circ ((r^\varphi + t) - (s^\varphi + t)) \\
 &= (u^\varphi - v^\varphi) \circ (r^\varphi - s^\varphi) \\
 &\stackrel{\text{VL4}}{=} (u - v)^\alpha \circ (r - s)^\alpha \\
 &\stackrel{\text{VL3}}{=} (u - v) \circ (r - s)
 \end{aligned}$$

- Für alle $u, v, r, s \in V$ gilt somit $(u^\alpha - v^\alpha) \circ (r^\alpha - s^\alpha) = (u - v) \circ (r - s)$.

- Weiterhin gilt:

$$\begin{aligned}
 &\rho(\angle(b^\alpha, a^\alpha, c^\alpha)) \\
 &= \arccos \frac{(b^\alpha - a^\alpha) \circ (c^\alpha - a^\alpha)}{\|b^\alpha - a^\alpha\| \cdot \|c^\alpha - a^\alpha\|} \\
 &= \arccos \frac{(b^\alpha - a^\alpha) \circ (c^\alpha - a^\alpha)}{\sqrt{(b^\alpha - a^\alpha) \circ (b^\alpha - a^\alpha)} \cdot \sqrt{(c^\alpha - a^\alpha) \circ (c^\alpha - a^\alpha)}} \\
 &= \arccos \frac{(b - a) \circ (c - a)}{\sqrt{(b - a) \circ (b - a)} \cdot \sqrt{(c - a) \circ (c - a)}} \\
 &= \arccos \frac{(b - a) \circ (c - a)}{\|b - a\| \cdot \|c - a\|} \\
 &= \rho(\angle(b, a, c))
 \end{aligned}$$

- (IV) (i) • Seien $G_a^u, G_b^v \in \mathcal{G}(\mathbb{R}V)$ vorgegeben.
- Angenommen $G_a^u \perp G_b^v \leadsto G_a^u \cap G_b^v \neq \{\}$ und $u \circ v = 0$.
 - Damit ist $(G_a^u \cap G_b^v)^\alpha \neq \{\}$.

- Da $(G_a^u)^\alpha \cap (G_b^v)^\alpha \supset (G_a^u \cap G_b^v)^\alpha$, folgt $(G_a^u)^\alpha \cap (G_b^v)^\alpha \neq \{\}$.
- Es ist $(G_a^u)^\alpha = G_{a^\alpha}^{u^\varphi}$, $(G_b^v)^\alpha = G_{b^\alpha}^{v^\varphi}$ und weiter $u^\varphi \circ v^\varphi \stackrel{\text{VL3}}{=} (u \circ v) = 0_{\mathbb{R}}$.

Ergebnis: $(G_a^u)^\alpha \perp (G_b^v)^\alpha$, falls $G_a^u \perp G_b^v$.

- (ii)
- Angenommen $G_a^u \parallel G_b^v$, dann ist $\mathbb{R}u = \mathbb{R}v$.
 - Es ist $(G_a^u)^\alpha = G_{a^\alpha}^{u^\varphi} = \{a^\alpha + \rho u^\varphi \mid \rho \in \mathbb{R}\} \stackrel{\text{VL4}}{=} \{a^\alpha + (\rho u)^\varphi \mid \rho \in \mathbb{R}\} = a^\alpha + (\mathbb{R}u)^\varphi = a^\alpha + (\mathbb{R}v)^\varphi$.
 - Es ist $\mathbb{R}v^\varphi = \{\rho v^\varphi \mid \rho \in \mathbb{R}\} \stackrel{\text{VL4}}{=} \{(\rho v)^\varphi \mid \rho \in \mathbb{R}\} = (\mathbb{R}v)^\varphi = (\mathbb{R}u)^\varphi = \{(\rho u)^\varphi \mid \rho \in \mathbb{R}\} \stackrel{\text{VL4}}{=} \{\rho u^\varphi \mid \rho \in \mathbb{R}\} = \mathbb{R}u^\varphi$.

Ergebnis: $(G_a^u)^\alpha = G_{a^\alpha}^{u^\varphi} \parallel G_{b^\alpha}^{v^\varphi} = (G_b^v)^\alpha$, da $\mathbb{R}u^\varphi = \mathbb{R}v^\varphi$

Kapitel 2

Inzidenzräume, Affine Räume

Die affine Geometrie über einem Vektorraum $_K V$

2.1 (D)

Es seien $\mathcal{P} := \{a, b, \dots\}$ eine Menge und $\mathcal{G} := \{A, B, \dots\} \subset \text{Pot}(\mathcal{P})$ eine Teilmenge der Potenzmenge von \mathcal{P} . Wir nennen die Elemente von \mathcal{P} *Punkte* und die Elemente von \mathcal{G} *Geraden*.

Das Paar $(\mathcal{P}, \mathcal{G})$ heißt *Inzidenzraum* – kurz IR –, wenn gilt:

[I_1] Zu jedem beliebig vorgegebenen $p, q \in \mathcal{P}$ mit $p \neq q$ existiert stets genau eine – mit \overline{pq} bezeichnete – Gerade $G \in \mathcal{G}$, die $p \in G$ und $q \in G$ genügt. \overline{pq} heißt die *Verbindungsgerade von p und q* .

[I_2] $|G| \geq 2$ für alle $G \in \mathcal{G}$.

2.2 (B)

(a) Es sei E die Menge aller Punkte des Anschauungsraumes, die anschaulich in der Blattebene liegen, \mathcal{G}_E die Menge aller Geraden dieses Raumes, die $G \subset E$. Dann ist (E, \mathcal{G}_E) ein Inzidenzraum (IR).

(b) Sei $T \subset E$ eine Teilmenge von E und $\mathcal{G}_T := \{G \cap T \mid G \in \mathcal{G}_E \text{ und } |G \cap T| > 1\}$; dann ist (T, \mathcal{G}_T) ein IR.

(c) $\mathcal{P} := \{b \text{ (ein Bleistift)}, r \text{ (ein Radiergummi)}, k \text{ (ein Kugelschreiber)}, p \text{ (ein Blatt Papier)}\}$ und $\mathcal{G} := \{S \subset \mathcal{P} \mid |S| = 2\}$; dann ist $(\mathcal{P}, \mathcal{G})$ ein IR.

2.3 (S)

Ist $(\mathcal{P}, \mathcal{G})$ ein IR, so gilt

(i) $\mathcal{G} = \{\overline{pq} \mid p, q \in \mathcal{P} \text{ und } p \neq q\}$

(ii) Aus $G, H \in \mathcal{G}$ und $|G \cap H| > 1$ folgt stets $G = H$.

Beweis

- (i)
 - Setze $\{\overline{pq} \mid p, q \in \mathcal{P} \text{ und } p \neq q\} =: \Gamma$. Sei $\overline{pq} \in \Gamma$ beliebig vorgegeben.
 - Dann ist $\overline{pq} \in \mathcal{G}_{[I_1]}$ und $\Gamma \in \mathcal{G}$.
 - Sei $G \in \mathcal{G}$ beliebig vorgegeben. Nach $[I_2]$ existiert ein $p, q \in G$ mit $p \neq q$ und es folgt $G \in \Gamma$ und weiter $\mathcal{G} \subset G$.
 - Damit ist $\mathcal{G} = \Gamma$.
- (ii)
 - Seien $G, H \in \mathcal{G}$ mit $|G \cap H| > 1$ beliebig vorgegeben.
 - Dann existieren $p, q \in G \cap H$ mit $p \neq q$ und es folgt

$$\left\{ \begin{array}{lcl} p, q \in G & \rightsquigarrow & G \stackrel{[I_1]}{=} \overline{pq} \\ p, q \in H & \rightsquigarrow & H \stackrel{[I_1]}{=} \overline{pq} \end{array} \right\} \rightsquigarrow G = H$$

2.4 (D)

Es sei M eine Menge und $\mathcal{K} \in \text{Pot}(M)$ eine Teilmenge der Potenzmenge von M . \mathcal{K} heißt genau dann *Klasseneinteilung von M* , wenn gilt

- (i) $\{\} \notin \mathcal{K}$
- (ii) Zu jedem $a \in M$ existiert *genau eine* – mit $K(a)$ oder $[a]$ bezeichnete – Teilmenge $K \in \mathcal{K}$, die $a \in K$ genügt.

2.5 (B) „Eselsbrücke“

$M =: S$ ist die Menge der Schüler einer Schule, dann entspricht $K(a)$ der Klasse, zu der Schüler a gehört.

2.6 (D)

- (a) Ist M eine Menge, so heißt jede Teilmenge $R \subset M \times M$ eine *Relation auf M* und anstatt $(a, b) \in R$ wird auch kürzer aRb geschrieben¹.
- (b) Es seien R eine Relation auf M und $a, b, c \in M$.
 R heißt
 - (i) *reflexiv*, wenn stets aRa gilt;
 - (ii) *symmetrisch*, wenn aus aRb stets bRa folgt;
 - (iii) *antisymmetrisch*, wenn aus aRb und bRa stets $a = b$ folgt, sowie
 - (iv) *transitiv*, wenn aus aRb und bRc stets aRc folgt.
- (c) Eine Relation R auf M heißt
 - (i) *Äquivalenzrelation*, wenn R reflexiv, symmetrisch und transitiv ist.
 - (ii) *Ordnungsrelation*, wenn R reflexiv, antisymmetrisch und transitiv ist.

¹Da R Teilmenge, können an R auch Anforderungen gebunden sein, z.B. $a > b$.

2.7 (B)

Es sein M eine Menge.

- (a) Ist \mathcal{K} eine Klasseneinteilung von M , so ist $\{(a, b) \in M \times M \mid K(a) = K(b)\} =: R_1$ eine Äquivalenzrelation.
- (b) $\{(A, B) \in \text{Pot}(M) \times \text{Pot}(M) \mid \text{Es gibt eine Bijektion } \varphi : A \rightarrow B\} =: R_2$ ist eine Äquivalenzrelation auf $\text{Pot}(M)$.
- (c) $\{(A, B) \in \text{Pot}(M) \times \text{Pot}(M) \mid A \subset B\} =: R_3$ ist eine Ordnungsrelation auf $\text{Pot}(M)$.
- (d) $\{(\alpha, \beta) \in \mathbb{R} \times \mathbb{R} \mid \alpha \leq \beta\} =: R_4$ ist eine Ordnungsrelation auf \mathbb{R} .

2.8 (S+D) Hauptsatz über Äquivalenzrelationen

Ist R eine Äquivalenzrelation auf einer Menge M , so stellt

$$\frac{M}{R} := \{[a] \mid a \in M\} \text{ mit } [a] := \{x \in M \mid xRa\}$$

eine Klasseneinteilung von M dar.

$\frac{M}{R}$ heißt die *von R auf M induzierte Klasseneinteilung* und $[a]$ heißt die *Äquivalenzklasse* von a (bezüglich der Äquivalenzrelation R).

Beweis Es sei R eine Äquivalenzrelation auf einer Menge M .

- Sei $a \in M$ beliebig, dann aber fest vorgegeben.
- Setze $\{x \in M \mid xRa\} =: [a]$.
- Setze $\{[a] \mid a \in M\} =: \frac{M}{R}$. Dann ist $\frac{M}{R} \subset \text{Pot}(M)$.
- Da R reflexiv, folgt $a \in [a]$ und weiter $\{a\} \subset \frac{M}{R}$.
- Sei $b \in M$ mit $a \in [b]$ beliebig vorgegeben.
- Sei weiterhin $x \in [a]$ beliebig vorgegeben. Dann gilt xRa und aRb und, da R transitiv, auch xRb . Damit ist aber auch $x \in [b]$ und es folgt $[a] \subset [b]$.
- Folglich gilt für alle $a, b \in M$ mit $a \in [b]$ $[a] \subset [b]$.
- Angenommen $a \in [b]$, dann gilt aRb , und, da R symmetrisch, auch bRa , womit $b \in [a]$ wäre, woraus $[b] \subset [a]$ folgen würde.
- Wir haben gezeigt, daß $[a] = [b]$ und daß für alle $b \in M$ mit $a \in [b]$ gilt $[a] = [b]$.
- Schlußendlich folgt die Behauptung: Zu jedem $a \in M$ ist $[a]$ das einzige Element von $\frac{M}{R}$, das a enthält.

2.9 Bemerkung

In (2.7)(b) $R_2 = \{(A, B) \in \text{Pot}(M) \times \text{Pot}(M) \mid \text{Es gibt eine Bijektion von } A \text{ auf } B\}$ heißt die Äquivalenzklasse $[A]$ von $A \in \text{Pot}(M)$ die *Mächtigkeit* von A und wird mit $[A] =: |A|$ oder $[A] = \#(A)$ bezeichnet.

2.10 (A)

Ist $(\mathbb{Z}, +, \cdot)$ der Ring der ganzen Zahlen und n eine natürliche Zahl, so heißen zwei Zahlen $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ *kongruent modulo n* – in Zeichen $a \equiv_n b$ – wenn gilt $a - b = \gamma \cdot n$ mit einem $\gamma \in \mathbb{Z}$.

Zeige:

- (a) \equiv_n ist eine Äquivalenzrelation auf \mathbb{Z} .
- (b) $\frac{\mathbb{Z}}{\equiv_n} =: \mathbb{Z}_n = \{[0], [1], \dots, [n-1]\}$ mit $[i] \neq [j]$ für alle $0 \leq j < j \leq n-1$.
- (c) Ist $a_n \equiv_n a'$ und $b \equiv_n b'$ so gilt $a + b \equiv_n a' + b'$ und $ab \equiv_n a'b'$.
- (d) \mathbb{Z}_n wird durch die Definition $\begin{cases} \mathbb{Z}_n \times \mathbb{Z}_n \rightarrow \mathbb{Z}_n \\ ([a], [b]) \mapsto [a] + [b] = [a + b] \\ ([a], [b]) \mapsto [a] \cdot [b] = [ab] \end{cases}$ zu einem kommutativen Ring $(\mathbb{Z}_n, +, \cdot)$ mit $[1]$ als Einselement.
- (e) $(\mathbb{Z}_n, +, \cdot)$ ist genau dann nullteilerfrei, wenn n eine Primzahl ist.

Lösung

Fehlt in meinen Unterlagen, vermutlich wurde sie nicht an den Übungsterminen vor der Klausur behandelt.

2.11 (D)

Es sei $(\mathcal{P}, \mathcal{G})$ ein Inzidenzraum (IR).

- (a) $S \subset \mathcal{P}$ heißt *kollinear*, wenn gilt²: Es gibt ein $G \in \mathcal{G}$ mit $S \subset G$.
- (b) $\{P_1, P_2, \dots, P_n\} =: E_n \subset \mathcal{P}$ heißt *n-eck*, wenn gilt:
 - (i) $|E_n| = n$ und
 - (ii) $|G \cap E_n| \leq 2$ für alle $G \in \mathcal{G}$.

2.12 (D)

Es sei $(\mathcal{P}, \mathcal{G})$ ein IR und $\parallel \subset \mathcal{G} \times \mathcal{G}$ eine Äquivalenzrelation auf \mathcal{G} .

Gilt $G \parallel H$, so heißen G und H *parallel* und die Äquivalenzklassen $[G]$, $G \in \mathcal{G}$ heißen *Parallelklassen*.

Das Tripel $(\mathcal{P}, \mathcal{G}, \parallel)$ heißt *Inzidenzraum mit Euklidischem Parallelenaxiom* – kurz IREP –, wenn das Euklidische Parallelenaxiom (EP) gilt:

Zu jedem beliebig vorgegebenen $(p, G) \in \mathcal{P} \times \mathcal{G}$ gibt es stets genau eine – mit $(p \parallel G)$ bezeichnete – Gerade H , die $p \in H$ und $H \parallel G$ genügt (siehe Abbildung 2.1).

$(p \parallel G)$ heißt die *Parallele* zur Geraden G durch den Punkt p .

²Vereinfacht gesagt stellt man sich die Frage, ob die Punkte auf einer Geraden liegen.

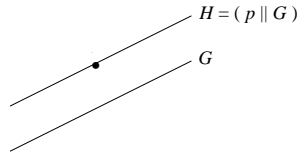


Abbildung 2.1: Zum Euklidischen Parallelaxiom

2.13 (S)

Sind G, H parallele Geraden eines IREP, so folgt aus $G \cap H \neq \{\}$ stets $G = H$

Beweis Sei $(\mathcal{P}, \mathcal{G}, \parallel)$ ein IREP und seien $G, H \in \mathcal{G}$, die die Voraussetzungen aus (2.12) erfüllen. Dann existiert ein $p \in G \cap H$.

$$G \stackrel{(\text{EP})}{=} (p \parallel H) \stackrel{H \text{ ist reflexiv}}{\underset{(\text{EP})}{=}} H$$

2.14 (D)

Ein IREP $(\mathcal{P}, \mathcal{G}, \parallel)$ heißt *affiner Raum* – kurz AR –, wenn das Schnittaxiom (Sax) gilt (vgl. Abbildung 2.2):

(Sax) Sind $p \neq q, p' \neq q'$ Punkte, die $\overline{pq} \parallel \overline{p'q'}$ genügen, so gilt für alle $r \in \mathcal{P} \setminus \overline{pq}$:

$$(p' \parallel \overline{pr}) \cap (q' \parallel \overline{qr}) \neq \{\}$$

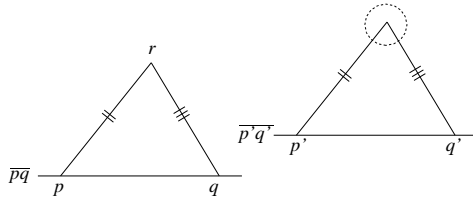


Abbildung 2.2: Zum Schnittaxiom

2.15 (D+S)

Es sein ${}_K V$ ein linker k -Vektorraum über einem (nicht notwendigerweise kommutativen) Körper $(K, +, \cdot)$. Setzt man

$$(I) \quad V =: \mathcal{P}({}_K V) =: \mathcal{P}$$

$$(II) \quad \{G_a^u := a + Ku := \{a + \rho u \mid \rho \in K\} \mid a, u \in V \text{ mit } u \neq 0_V\} = \mathcal{G}({}_K V) =: \mathcal{G}$$

$$(III) \quad \{(G_a^u, G_b^v) \in \mathcal{G} \times \mathcal{G} \mid Ku = Kv\} = \parallel({}_K V) =: \parallel$$

so stellt \parallel eine eindeutig, d.h. repräsentantenunabhängig definierte Äquivalenzrelation auf \mathcal{G} dar und

$$(\mathcal{P}, \mathcal{G}, \parallel) =: \text{Aff}({}_K V)$$

ist ein AR mit den folgenden Eigenschaften:

$$(a) \quad |G_a^u| = |K| \geq 2$$

- (b) Aus $p \in G_a^u$ folgt: $G_a^u = G_p^u$.
- (c) $\overline{pq} = G_p^{p-q} = \{\alpha p + \beta q \mid \alpha + \beta = 1\}$.
- (d) $(p \parallel G_a^u) = G_p^u$

Der AR $\text{Aff}({}_K V)$ heit die *Affine Geometrie ber dem Vektorraum ${}_K V$* .

Beweis Sei ${}_K V$ ein linker K -Vektorraum und seien $\mathcal{P}({}_K V) =: \mathcal{P}, \mathcal{G}({}_K V) := \mathcal{G}, \parallel({}_K V) := \parallel$ gem (I) bis (III) definiert.

Seien $p, q \in \mathcal{P}$ mit $p \neq q$ und G_a^u, G_b^v, G_c^w beliebig, dann aber fest vorgegeben.

ad (a) und [I2]

- $\rho := \begin{cases} K \rightarrow G_a^u \\ \lambda \mapsto a + \lambda u \end{cases}$ ist eindeutig definierte Abbildung von K auf G_a^u .
- Angenommen $\rho(\lambda_1) = \rho(\lambda_2)$, dann wre $a + \lambda_1 u = a + \lambda_2 u$ und es wrde folgen $(\lambda_1 - \lambda_2)u = 0_v$ sowie, da $u \neq 0_v$, weiterhin $\lambda_1 - \lambda_2$ bzw. $\lambda_1 = \lambda_2$, d.h. ρ ist injektiv.
- Damit ist ρ Bijektion von K auf G_a^u .
- Da mindestens $\{0_K, 1_K\} \in K$ und $0_K \neq 1_K$, folgt die Aussage $|G_a^u| = |K| \geq 2$.

ad (b)

- Angenommen $p \in G_a^u$, dann wre $p = a + \rho u$ mit einem $\rho \in K$.
- Damit wre $G_p^u = (a + \rho u) + K u = a + (\rho + K)u \stackrel{\rho+K=K}{=} a + K u = G_a^u$

ad (c) und [I1]

- Wegen $p \neq q$ gilt $q - p \neq 0$. Damit ist $G_p^{q-p} \in \mathcal{G}$ und $\begin{cases} p = p + 0_k(q - p) \in G_p^{q-p} \\ q = p + 1_k(q - p) \in G_p^{q-p} \end{cases}$
- Ist umgekehrt $G_a^u \in \mathcal{G}$ mit $p, q \in G_a^u$ beliebig vorgegeben, so ist $q \in G_a^u \stackrel{(b)}{=} G_p^u$, d.h. $q = p + \rho u$ mit einem $\rho \in K$.
- Demzufolge ist $q - p = \rho u$.
- Angenommen $\rho = 0_K$, dann wre $q - p = 0_K \cdot u = 0_v$, d.h. $q = p$ q.e.a.
- Daher ist $\rho \neq 0_K$ und es folgt $K(q - p) = K(\rho u) = (K\rho)u \stackrel{K\rho=K}{=} K u$.
- Wir erhalten $G_a^u = G_p^u \stackrel{(II)}{=} p + K u = p + K(q - p) \stackrel{(II)}{=} G_p^{q-p}$.
- Damit gilt [I1] und es ist $\overline{pq} = G_p^{p-q} = \{p + \rho(q - p) \mid \rho \in K\} = \{\underbrace{(1 - \rho)}_{=: \alpha} p + \underbrace{\rho}_{=: \beta} q \mid \rho \in K\} = \{\alpha p + \beta q \mid \alpha + \beta = 1\}$.

Aus (a) und (c) folgt, da gem (2.1) $(\mathcal{P}, \mathcal{G})$ ein IR ist.

Problem: Ist \parallel **eindeutig, d.h. repräsentantenunabhängig definiert?**

- Angenommen $G_a^u = G_{a'}^{u'}$, d.h. $a \in a + Ku = G_a^u = G_{a'}^{u'} \stackrel{(b)}{=} G_a^{u'} = a + Ku'$, woraus folgt $Ku = Ku'$.
- Aus $G_a^u = G_{a'}^{u'}$ folgt $Ku = Ku'$.
- Angenommen $G_a^u = G_{a'}^{u'}$ und $G_b^v = G_{b'}^{v'}$, so gilt $G_a^u \parallel G_b^v \Leftrightarrow Ku = Kv \Leftrightarrow Ku' = Kv' \Leftrightarrow G_{a'}^{u'} \parallel G_{b'}^{v'}$.
- Damit ist \parallel eindeutig definierte Relation auf \mathcal{G} mit $G_a^u \parallel G_a^u$ (folgt aus $Ku = Ku$ und (III)), d.h. \parallel ist reflexiv.
- Angenommen $G_a^u \parallel G_b^v$ und $G_b^v \parallel G_c^w$, dann ist $Ku = Kv$ und $Kv = Kw$, also $Ku = Kw$ bzw. $G_a^u \parallel G_c^w$ und es folgt, daß \parallel transitiv ist.

Gemäß (2.6) ist \parallel eine Äquivalenzrelation auf \mathcal{G} .

ad (d) und EP

- Sei $(p, G_a^u) \in \mathcal{P} \times \mathcal{G}$ beliebig vorgegeben.
- Da $u \neq 0_V$, ist nach (II) $G_p^u \in \mathcal{G}$ bzw. $p = p + 0_K u \in G_p^u$ und (nach (III)) $G_a^u \parallel G_p^u$.
- Sei umgekehrt $G_b^v \in \mathcal{G}$ mit $p \in G_b^v$ und $G_b^v \parallel G_a^u$ beliebig vorgegeben.
- Nach (a), (II) und (III) ist dann $G_b^v = G_p^v = p + Kv = p + Ku = G_p^u$.

Gemäß (2.13) ist $(\mathcal{P}, \mathcal{G}, \parallel)$ ein IREP und es gilt (d) $(p \parallel G_a^u) = G_p^u$.

ad (Sax)

- Seien $p \neq q, p' \neq q', r \in \mathcal{P}$ mit $\overline{pq} \parallel \overline{p'q'}$ und $r \notin \overline{pq}$ beliebig vorgegeben.
- Nach (c) ist $\overline{pq} = G_p^{q-p}$.
- Aus $\overline{pq} \parallel \overline{p'q'}$ folgt $\overline{p'q'} \stackrel{(EP)}{=} (p' \parallel \overline{pq})$ und weiter $(p' \parallel G_p^{q-p}) = G_{p'}^{q-p}$ bzw. $q' = p' + \rho(q - p)$ mit einem $\rho \in K$.
- Daraus folgt $x := q' + \rho(r - q) = p' + \rho(q - p) + \rho(r - q) = p' + \rho(r - p)$.
- Nun ist $p' + \rho(r - p) \in p' + K(r - p) \cap q' + K(r - q) = G_{p'}^r - p \cap G_{q'}^{r-q} = (p' \parallel \overline{pr}) \cap (q' \parallel \overline{qr})$, d.h. es gilt $(p' \parallel \overline{pr}) \cap (q' \parallel \overline{qr}) \neq \{\}$.

Es gilt somit das Schnittaxiom (Sax).

Beweisschluß Da alle in (2.14) geforderten Voraussetzungen erfüllt sind, ist $(\mathcal{P}, \mathcal{G}, \parallel)$ ein Affiner Raum (AR).

Bemerkung

Die hier dargestellte Affine Geometrie ist ein spezieller Affiner Raum, d.h. Affine Räume existieren.

2.16 (S)

Sind G, H Geraden eines AR, so folgt aus $G \nparallel H$ stets $|G \cap H| \leq 1$.

Beweis Angenommen $|G \cap H| > 1$. Wegen $[I_1]$ wäre dann $G = H$ und, da \parallel reflexiv, es würde $G \parallel H$ folgen.

2.17 (S)

In einem AR $(\mathcal{P}, \mathcal{G}, \parallel)$ gilt stets:

(Sax)* Sind $p \neq q, p' \neq q'$ Punkte mit $\overline{pq} \parallel \overline{p'q'}$, so gilt für alle $r \in \mathcal{P} \setminus \overline{pq}$:

(I) Die Geraden $\overline{p'q'}$, $(p' \parallel \overline{pr})$ $(q' \parallel \overline{qr})$ sind paarweise nicht parallel.

(II) $|(p' \parallel \overline{pr}) \cap (q' \parallel \overline{qr})| = 1$ und $(p' \parallel \overline{pr}) \cap (q' \parallel \overline{qr}) =: r' \in \mathcal{P} \setminus \overline{p'q'}$.

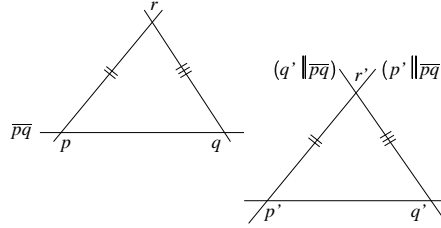


Abbildung 2.3: Zum (erweiterten) Schnittaxiom (Sax)*

Beweis

- Angenommen $(p' \parallel \overline{pr}) \parallel \overline{p'q'}$.

Dann wäre $\overline{pr} \parallel (p' \parallel \overline{pr}) \parallel \overline{p'q'} \parallel \overline{pq}$, und weiter, da \parallel transitiv, $\overline{pr} \parallel \overline{pq} \xrightarrow{(2.13)}$

$\overline{pr} = \overline{pq} \xrightarrow{r \in \overline{pr}} r \in \overline{pq}$ q.e.a.

- Demzufolge ist $(p \parallel \overline{pr}) \nparallel \overline{p'q'}$ und nach (2.16) folgt $(p' \parallel \overline{pr}) \cap \overline{p'q'} = p'$.

- Analog zeigt man $(q' \parallel \overline{qr}) \nparallel \overline{q'p'}$ bzw. $(q' \parallel \overline{qr}) \cap \overline{q'p'} = q'$.

- Angenommen $(p' \parallel \overline{pr}) \parallel (q' \parallel \overline{qr})$. Dann wäre nach (2.13) und (Sax) $(p' \parallel \overline{pr}) = (q' \parallel \overline{qr}) \stackrel{[I_1]}{=} \overline{p'q'}$ und weiter, da \parallel reflexiv, $(p' \parallel \overline{pr}) \parallel \overline{p'q'}$ q.e.a.

- Demzufolge ist $(p' \parallel \overline{pr}) \nparallel (q' \parallel \overline{qr})$ und nach (2.16) folgt $|(p' \parallel \overline{pr}) \cap (q' \parallel \overline{qr})| = 1$.

- Angenommen $(p' \parallel \overline{pr}) \cap (q' \parallel \overline{qr}) =: r' \in \overline{p'q'}$. Dann wäre

– entweder $r' \neq p'$, d.h. $(p' \parallel \overline{pr}) \stackrel{[I_1]}{=} \overline{p'r'} \stackrel{[I_1]}{=} \overline{p'q'}$, und weiter, da \parallel reflexiv, $(p' \parallel \overline{pr}) \parallel \overline{p'q'}$ q.e.a.

– oder $r' = p'$, d.h. $r' \neq q'$ bzw. $(q' \parallel \overline{qr}) \stackrel{[I_1]}{=} \overline{r'q'} \stackrel{[I_1]}{=} \overline{p'q'}$, woraus wegen der Reflexivität von \parallel folgen würde $(q' \parallel \overline{qr}) \parallel \overline{p'q'}$ q.e.a.

- Damit ist $r' \notin \overline{p'q'}$

2.18 (D)

Ein AR $(\mathcal{P}, \mathcal{G}, \parallel)$ heißt *Affiner Desargues'scher Raum* – kurz ADR –, wenn der *Affine Satz von Desargues* (AD) gilt (vgl. Abbildung 2.4):

Sind G_1, G_2, G_3 drei verschiedene Geraden durch einen Punkt Z und a_i, b_i für $i = 1, 2, 3$ Punkte, die $a_i, b_i \in G_i \setminus G_{i+1}$ genügen, so folgt aus $\overline{a_1a_2} \parallel \overline{b_1b_2}$ und $\overline{a_2a_3} \parallel \overline{b_2b_3}$ auch stets $\overline{a_3a_1} \parallel \overline{b_3b_1}$.

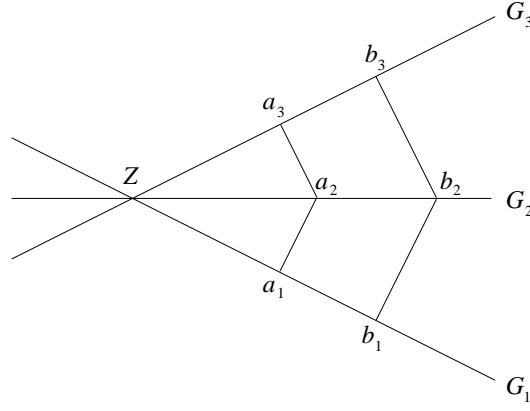


Abbildung 2.4: Zum Affinen Satz von Desargues

2.19 (S)

$\text{Aff}(KV)$ ist auch stets ein ADR.

Beweis Seien $G_4 = G_1, G_2, G_3$ Geraden und a_i, b_1 Punkte, die die Voraussetzungen von (AD) erfüllen.

- Aus $G_1 \neq G_2 \neq G_3 \neq G_4$ folgt mit $[I_1]$, daß $G_1 \cap G_2 = G_2 \cap G_3 = G_3 \cap G_1 =: Z$.
- Aus $a_i, b_i \in G_i \setminus G_{i+1}$ folgt $Z \notin \{a_1, a_2, a_3, b_1, b_2, b_3\}$. und weiter $G_i \stackrel{[I_1]}{=} \overline{za_i} \stackrel{(2.15)}{=} G_z^{a_i-z}$ für $i = 1, 2, 3$.
- Da $b_1 \in G_1$, läßt sich b_1 darstellen als $b_1 = z + \rho(a_1 - z)$ mit einem eindeutig bestimmten $\rho \in K$.
- Angenommen $\rho = 0_K$, dann wäre $b_1 = z$ q.e.a., daher ist $\rho \neq 0_K$.
- Es ist $z + \rho(a_2 - z) = z + \rho(a_1 - z) + \rho(a_2 - a_1) = b_1 + \rho(a_2 - a_1) \in G_2 \cap G_{b_1}^{a_2-a_1}$ und weiter $G_2 \cap G_{b_1}^{a_2-a_1} = G_2 \cap (b_1 \parallel \overline{a_1 a_2}) \stackrel{b_1 \notin G_2}{=} \{b_2\}$, also zusammengefasst: $z + \rho(a_2 - z) \in \{b_2\}$ bzw. $b_2 = z + \rho(a_2 - z)$.
- Es ist $z + \rho(a_3 - z) = z + \rho(a_2 - z) + \rho(a_3 - a_2) = b_2 + \rho(a_3 - a_2) \in G_3 \cap G_{b_2}^{a_3-a_2}$ und weiter $G_3 \cap G_{b_2}^{a_3-a_2} = G_3 \cap (b_2 \parallel \overline{a_2 a_3}) \stackrel{b_2 \notin G_3}{=} \{b_3\}$, also zusammengefasst: $z + \rho(a_3 - z) \in \{b_3\}$ bzw. $b_3 = z + \rho(a_3 - z)$.
- Demzufolge ist $b_3 - b_1 = (z + \rho(a_3 - z) - (z + \rho(a_1 - z))) = \rho(a_3 - a_1)$ und weiter $K(b_3 - b_1) = K(\rho(a_3 - a_1)) = (K\rho)(a_3 - a_1) = K(a_3 - a_1)$.
- Schlußendlich ist $\overline{b_1 b_3} = G_{b_1}^{b_3-b_1} \parallel G_{a_1}^{a_3-a_1} = \overline{a_1 a_3}$.

Damit gilt in $\text{Aff}(KV)$ stets (AD).

2.20 (S)

In einem ADR gilt stets der *Kleine Affine Satz von Desargues* (Ad):

Sind G_1, G_2, G_3 drei verschiedene parallele Geraden und a_i, b_i für $i = 1, 2, 3$ Punkte, die $a_i, b_i \in G_i$ genügen, so folgt aus $\overline{a_1 a_2} \parallel \overline{b_1 b_2}$ und $\overline{a_2 a_3} \parallel \overline{b_2 b_3}$ auch stets $\overline{a_3 a_1} \parallel \overline{b_3 b_1}$.

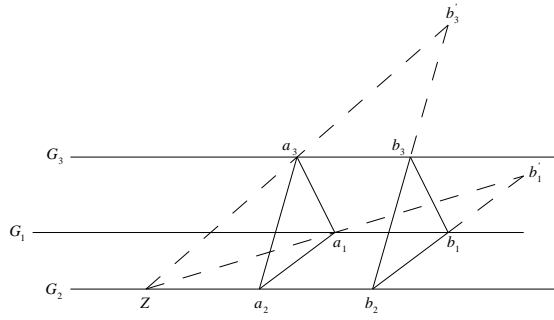


Abbildung 2.5: Zum Beweis des Kleinen Affinen Satz von Desargues

Beweis Sei $(\mathcal{P}, \mathcal{G}, \parallel)$ ein ADR und seien G_1, G_2, G_3 Geraden und a_i, b_i für $i = 1, 2, 3$ Punkte, die die Voraussetzungen von (Ad) erfüllen.

- Nach (2.13) gilt $G_1 \cap G_2 = G_2 \cap G_3 = G_3 \cap G_1 = \{\}$ woraus $a_1 \neq a_2 \neq a_3 \neq a_1$ und $b_1 \neq b_2 \neq b_3 \neq b_1$ sowie $a_i \notin G_j$ für $i \neq j$ folgt.
- Im Fall $a_1 = a_2$ läßt sich folgern:

- Es gilt $a_2 = \overline{a_1 a_2} \cap G_2 = (a_1 \parallel \overline{a_1 a_2}) \cap G_2 \stackrel{\overline{a_1 a_2} \parallel \overline{b_1 b_2}}{=} (b_1 \parallel \overline{b_1 b_2}) \cap G_2 = \overline{b_1 b_2} \cap G_2 = b_2$, also $a_2 = b_2$.
- Es gilt weiter $a_3 = \overline{a_2 a_3} \cap G_3 = (a_2 \parallel \overline{a_2 a_3}) \cap G_3 \stackrel{\overline{a_2 a_3} \parallel \overline{b_2 b_3}}{=} (b_3 \parallel \overline{b_2 b_3}) \cap G_3 = \overline{b_2 b_3} \cap G_3 = b_3$, also $a_3 = b_3$.

Aus $a_1 = b_1$ erhält man also $\overline{a_3 a_1} = \overline{b_3 b_1}$ bzw. $\overline{a_3 a_1} \parallel \overline{b_3 b_1}$.

- Analog zeigt man $\overline{a_3 a_1} = \overline{b_3 b_1}$, falls $a_2 = b_2$ oder $a_3 = b_3$.
- Sei ab hier also $a_i \neq b_i$ für $i = 1, 2, 3$ vorausgesetzt.
- Gilt $a_3 \in \overline{a_1 a_2}$, so folgt $\overline{a_1 a_2} \stackrel{[I_1]}{=} \overline{a_2 a_3} \stackrel{[I_1]}{=} \overline{a_3 a_1}$.
 - Damit und nach Voraussetzung ergibt sich $\overline{b_1 b_2} \parallel \overline{a_1 a_2} = \overline{a_2 a_3} \parallel \overline{b_2 b_3}$, woraus folgt $\overline{b_1 b_2} \parallel \overline{b_2 b_3}$.
 - Man sieht also, daß $\overline{b_1 b_2} = \overline{b_2 b_3} \stackrel{[I_1]}{=} \overline{b_3 b_1}$, bzw. $\overline{a_3 a_1} = \overline{a_1 a_2} \parallel \overline{b_1 b_2} = \overline{b_3 b_1}$.
 - Kurz gesagt: $\overline{a_3 a_1} \parallel \overline{b_3 b_1}$, falls $a_3 \in \overline{a_1 a_2}$.
- Wir dürfen ab hier außer $a_i \neq b_i$ für $i = 1, 2, 3$ auch noch $a_3 \notin \overline{a_1 a_2}$ voraussetzen.
- Es ist $\overline{a_1 a_2} \parallel \overline{b_1 b_2}$ und $\overline{a_2 a_3} \parallel \overline{b_2 b_3} \stackrel{[EP]}{=} (b_2 \parallel \overline{a_2 a_3})$.
Nach (Sax)* folgt $(b_1 \parallel \overline{a_3 a_1}) \cap \overline{b_2 b_3} =: b'_3 \in \mathcal{P} \setminus \overline{b_1 b_2}$.
- Hieraus lesen wir ab $b'_3 \neq b_1$ und $\overline{b'_3 b_1} = (b_1 \parallel \overline{a_3 a_1}) \parallel \overline{a_3 a_1}$
 $\overline{b'_3 b_1} \cap \overline{b_1 b_2} = \{b_1\} \rightsquigarrow b'_3 \in \overline{b_2 b_3}$
- Angenommen $b'_3 \in G_3$, dann wäre, da $G_3 = \overline{a_3 b_3}$, $\{a_3, b_3, b'_3\}$ ein Dreieck.
- Angenommen $b'_3 = b_2$, dann wäre $\overline{a_1 a_3} \parallel \overline{b'_3 b_1} = \overline{b_2 b_1} \parallel \overline{a_2 a_1}$ und es wäre $a_3 \in \overline{a_3 a_1} = \overline{a_2 a_1}$ q.e.a.
- Daher muß $b'_3 \neq b_2$ sein.
Demzufolge ist $\overline{b_2 b'_3} = \overline{b_3 b'_3}$ bzw. $\overline{b_3 b'_3} \parallel \overline{b_2 b'_3}$, woraus nach (Sax)* wiederum folgt, daß $(b_2 \parallel \overline{b_3 a_3}) \cap (b'_3 \parallel \overline{b'_3 a_3}) =: z \in \mathcal{P} \setminus \overline{b_2 b'_3}$.

- Wegen $b_2 \in G_2$ und $\overline{b_3 a_3} = G_3 \parallel G_2$, gilt $(b_2 \parallel \overline{b_3 a_3}) = G_2$, d.h. $z \in G_2$.
- Angenommen $z = a_2$.
Dann wäre $b_3 \in \overline{z a_3} = \overline{a_2 a_3} \parallel \overline{b_2 b_3} \ni b'_3$ bzw. $\overline{a_2 a_3} = \overline{b_2 b_3}$. Weiterhin wäre
 $a_2 = \overline{a_2 a_3} \cap G_2 = \overline{b_2 b_3} \cap G_2 = b_2$ q.e.a.
Demzufolge muß $z \neq a_2$ gelten.
- Angenommen $z = b_2$.
Dann wäre $\overline{b_2 a_3} = \overline{z a_3} = \overline{b'_3 a_3} = \overline{b_2 b_3}$ bzw. $a_3 = \overline{b'_3 a_3} \cap G_3 = \overline{b_2 b_3} \cap G_3 = b_3$
q.e.a.
Demzufolge muß $z \neq b_2$ gelten.
- Aus $\overline{z a_2} = G_2 = \overline{z b_2}$ folgt $\overline{z a_2} \parallel \overline{z b_2}$ und, da $a_2 \in \overline{z a_2}$, es folgt nach (Sax)*
 $(z \parallel \overline{z a_1}) \cap (b_2 \parallel \overline{a_2 a_1}) =: b'_1 \in \mathcal{P} \setminus z b_2$.
- Es ist $(z \parallel \overline{z a_1}) = \overline{z a_1}$ und $(b_2 \parallel \overline{a_2 a_1}) = \overline{b_2 b_1}$, woraus $b'_1 = \overline{z a_1} \cap \overline{b_2 b_1}$ folgt.
- Die Geraden $\overline{z a_1}$, $\overline{z a_2}$ und $\overline{z a_3}$ erfüllen zusammen mit den Punkten
 a_1, a_2, a_3, b'_1, b_2 und b'_3 die Voraussetzungen von (Ad).
Demnach gilt $\overline{a_3 a_1} \parallel \overline{b'_3 b'_1} \parallel \overline{b'_3 b_1}$, bzw. $\overline{b'_3 b'_1} \parallel \overline{b'_3 b_1}$ und es folgt nach (2.13)
 $\overline{b'_3 b'_1} = \overline{b'_3 b_1}$.
- Weiterhin ist $b'_1 \in \overline{b'_3 b'_1} \cap \overline{b_1 b_2} = \overline{b'_3 b_1} \cap \overline{b_1 b_2} = \{b_1\} \rightsquigarrow b'_1 = b_1$
- $G_1 = \overline{a_1 b_1} = \overline{a_1 b'_1} = \overline{z a_1}$, woraus folgt $z \in G_1 \cap G_2 = \{z\}$ q.e.a.
- Daher muß $b'_3 \in G_3$ sein, d.h. $b'_3 \in \overline{b_2 b_3} \cap G_3 = \{b_3\}$, was bedeutet, daß $b'_3 = b_3$.
- Damit haben wir: $\overline{b_3 b_1} = \overline{b'_3 b_1} \parallel \overline{a_3 a_1}$.

Es gilt somit der Kleine Affine Satz von Desargues (Ad).

2.21 (D)

Ein IR $(\mathcal{P}, \mathcal{G})$ heißt *trivial*, wenn gilt: $(\mathcal{P}, \mathcal{G})$ besitzt kein Dreieck.

Warum trivial? Ist $(\mathcal{P}, \mathcal{G})$ ein trivialer IR, so gilt

entweder $|\mathcal{P}| < 2 \xrightarrow{[I_2]} \mathcal{G} = \{z\} \rightsquigarrow (\mathcal{P}, \mathcal{G}) \stackrel{[I_1]}{=} (\mathcal{P}, \{z\})$,

oder es gilt $|\mathcal{P}| \geq 2$: Sei dann $G \in \mathcal{G}$ beliebig vorgegeben. Nach $[I_1]$ und $[I_2]$ wäre dann $G = \overline{pq}$ mit $p, q \in \mathcal{G}$ und $p \neq q$. Sei weiterhin ein $x \in \mathcal{P}$ beliebig vorgegeben. Angenommen $x \in G$, dann wäre $\{p, q, x\} \in \mathcal{P}$ ein Dreieck q.e.a. (wir gehen von einem trivialen IR aus). Daher folgt aus $x \in \overline{pq}$, daß $G = \mathcal{P}$ und weiter $(\mathcal{P}, \mathcal{G}) = (\mathcal{P}, \{\mathcal{P}\})$, d.h. \mathcal{P} ist die einzige Gerade des IR $(\mathcal{P}, \mathcal{G})$.

2.22 (S) Existenz und Eindeutigkeit des vierten Schnittpunktes in einem Paralleogramm

Ist $\{a, b, c\} \subset \mathcal{P}$ ein Dreieck eine AR $(\mathcal{P}, \mathcal{G}, \parallel)$, so gilt

$$(c \parallel \overline{ab}) \cap (b \parallel \overline{ac}) =: d$$

mit eindeutig bestimmtem $d \in \mathcal{P}$

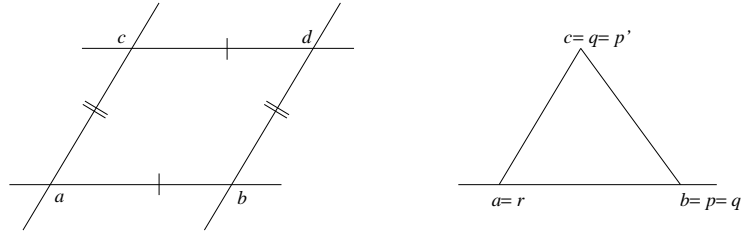


Abbildung 2.6: Eindeutigkeit eines Parallelogramms

Beweis Sei $\{a, b, c\} \subset \mathcal{P}$ ein beliebig vorgegebenes Dreieck eines AR $(\mathcal{P}, \mathcal{G}, \parallel)$.

- Setze $a =: r, b =: q', c =: q =: p'$.
- Dann ist $\overline{pq} = \overline{bc} = \overline{p'q'}$ bzw. $\overline{pq} \parallel \overline{p'q'}$ und $r \notin \overline{pq}$.
- Nach (Sax) ist dann $(p' \parallel \overline{pr}) \cap (q' \parallel \overline{qr}) =: d \in \mathcal{P}$ eindeutig bestimmt.
- $(p' \parallel \overline{pr}) = (c \parallel \overline{ab})$ und $(q' \parallel \overline{qr}) = (b \parallel \overline{ac})$ folgt die Behauptung.

2.23 (D+S)

- (a) Ist $(\mathcal{P}, \mathcal{G})$ ein IR und $a \in \mathcal{P}$, so heißt $\langle a \rangle := \{G \in \mathcal{G} \mid a \in G\}$ das *Geradenbündel durch a*.
- (b) Ist $(\mathcal{P}, \mathcal{G}, \parallel)$ ein nicht trivialer AR, so gilt $|\langle a \rangle| \geq 3$ für alle $a \in \mathcal{P}$.

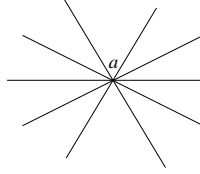


Abbildung 2.7: Geradenbündel

Beweis

- (a) Definition, nicht beweisbar.
- (b) Sei $(\mathcal{P}, \mathcal{G}, \parallel)$ ein nicht trivialer AR und $a \in \mathcal{P}$ beliebig vorgegeben.
- Dann existiert ein $b \in \mathcal{P} \setminus \{a\}$.
 - Angenommen $\overline{ab} \supset \mathcal{P}$, dann wäre $(\mathcal{P}, \mathcal{G})$ trivial q.e.a.; daher existiert ein $c \in \mathcal{P} \setminus \overline{ab}$.
 - Damit ist $\overline{ab} \neq \overline{ac}$ und $(c \parallel \overline{ab}) \cap (b \parallel \overline{ac}) \stackrel{(2.22)}{=} d \in \mathcal{P}$ ist eindeutig bestimmt.
 - Angenommen $d \in \overline{ab}$, dann würde aus $d \in \overline{ab} \cap (c \parallel \overline{ab})$ nach (2.13) folgen, daß $\overline{ab} = (c \parallel \overline{ab})$, bzw. daß $c \in \overline{ab}$ q.e.a.; daher ist $d \notin \overline{ab}$ und es folgt $\overline{ad} \neq \overline{ab}$.
 - Angenommen $d \in \overline{ac}$, dann würde aus $d \in \overline{ac} \cap (b \parallel \overline{ac})$ nach (2.13) folgen, daß $\overline{ac} = (b \parallel \overline{ac})$, bzw. daß $b \in \overline{ac}$ q.e.a.; daher ist $d \notin \overline{ac}$ und es folgt $\overline{ac} \neq \overline{ad}$.
 - Wir haben gezeigt, daß $\overline{ab} \neq \overline{ac} \neq \overline{ad} \neq \overline{ab}$, also $|\{\overline{ab}, \overline{ac}, \overline{ad}\}| = 3$.

Hieraus folgt die Behauptung $|\langle a \rangle| \geq 3$.

2.24 (S+D)

In einem AR $(\mathcal{P}, \mathcal{G}, \parallel)$ mit $\mathcal{G} \neq \{\}$ gilt für alle $G, H \in \mathcal{G}$

$$|G| = |H| =: \text{ord}(\mathcal{P}, \mathcal{G}, \parallel)$$

und es heißt $\text{ord}(\mathcal{P}, \mathcal{G}, \parallel)$ die *Ordnung des AR* $(\mathcal{P}, \mathcal{G}, \parallel)$.

Beweis Seien $G, H \in \mathcal{G}$ mit $G \neq H$ beliebig vorgegeben. Dann ist entweder $G \parallel H$ (Fall I) oder $G \nparallel H$ (Fall II).

- (I) • Es gilt $G \cap H = \{\}$. Wähle ein $g_0 \in G$ und ein $h_0 \in H$.
- Für $\varphi : \begin{cases} G \rightarrow H \\ g \mapsto (g \parallel \overline{g_0 h_0}) \cap H =: g^\varphi \end{cases}$ gilt $\varphi \in \text{Abb}(G, H)$.
- Für $\psi : \begin{cases} H \rightarrow G \\ h \mapsto (h \parallel \overline{g_0 h_0}) \cap G =: h^\psi \end{cases}$ gilt $\psi \in \text{Abb}(H, G)$.
- Sei $g \in G$ beliebig vorgegeben. Wähle es so, daß $g^\varphi =: h \in H$ und $h^\psi =: g' \in G$ mit $h \in (g \parallel \overline{g_0 h_0}) \stackrel{[\text{EP}]}{=} (h \parallel \overline{g_0 h_0}) \ni g'$.
- Damit ist $g' = h^\psi = (h \parallel \overline{g_0 h_0}) \cap G = (g \parallel \overline{g_0 h_0}) \cap G = g$, also $g^{\varphi\psi} = g' = g$, woraus $\varphi\psi = \text{id}_G$ folgt.
- Analog erhält man $\psi\varphi = \text{id}_H$.
- Damit ist φ Bijektion von G auf H , d.h. $|G| = |H|$, falls $G \parallel H$.
- (II) • Im Fall $G \nparallel H$ wähle $g_0 =: l_0 \in G$.
- Setze $G \nparallel H \parallel (g_0 \parallel H) =: L$. Da \parallel transitiv ist, folgt $G \nparallel L$ bzw. $G \cap L = g_0 = l_0$.
- Setze $G \setminus \{g_0\} =: G_0$ und $L \setminus \{l_0\} =: L_0$, dann ist $G_0 \cap L_0 = \{\}$.
- Wähle $g_1 \in G_0, l_1 \in L_0$, dann ist $\{g_0 = l_0, g_1, l_1\} \subset \mathcal{P}$ ein Dreieck.
- (Sax)*: Für $\alpha : \begin{cases} G_0 \rightarrow L_0 \\ g \mapsto (g \parallel \overline{g_1 l_1}) \cap L_0 =: g^\alpha \end{cases}$ gilt $\alpha \in \text{Abb}(G_0, L_0)$.
- Für $\beta : \begin{cases} L_0 \rightarrow G_0 \\ l \mapsto (l \parallel \overline{g_1 l_1}) \cap G_0 =: l^\beta \end{cases}$ gilt ebenso $\beta \in \text{Abb}(L_0, G_0)$.
- Sei ein $g \in G_0$ beliebig vorgegeben. Wähle es so, daß $g^\alpha =: l \in L_0$ und daß $l^\beta =: \tilde{g} \in G_0$ mit $l \in (g \parallel \overline{g_1 l_1}) \stackrel{[\text{EP}]}{=} (l \parallel \overline{g_1 l_1}) \ni \tilde{g} = g$.
- Daraus folgt $\tilde{g} = l^\beta = (l \parallel \overline{g_1 l_1}) \cap G_0 = (g \parallel \overline{g_1 l_1}) \cap G_0 = g$, also $g^{\alpha\beta} = \tilde{g} = g$, bzw. $\alpha\beta = \text{id}_{G_0}$.
- Analog erhält man $\beta\alpha = \text{id}_{L_0}$.
- Damit ist α Bijektion von G_0 auf L_0 , d.h. $|G_0| = |L_0|$, woraus folgt $|G| = |G_0| + 1 = |L_0| + 1 = |L|$.
- Wegen $L \parallel H$ folgt mit Fall I $|G| = |L| = |H|$, falls $G \nparallel H$.

Damit ist $|G| = |H|$ für alle $G, H \in \mathcal{G}$.

2.25 (A)

Es seien A, B Mengen und $\varphi \in \text{Abb}(A, B), \psi \in \text{Abb}(B, A)$.

Zeige: Ist $\varphi\psi = \text{id}_A$ und $\psi\varphi = \text{id}_B$, so gilt $\varphi \in \text{Bij}(A, B)$.

Lösung

Seien $x_1, x_2 \in A$ mit $x_1^\varphi = x_2^\varphi =: y \in B$ beliebig vorgegeben. Dann ist

$$x_1 = x_1^{id_A} = x_1^{\varphi^\psi} = (x_1^\varphi)^\psi = (x_2^\varphi)^\psi = x_2^{\varphi^\psi} = x_2^{id_A} = x_2$$

Damit ist φ injektiv.

Sei $y \in B$ beliebig vorgegeben. Setze $y^\psi =: x \in A$. Dann ist

$$x^\varphi = (y^\psi)^\varphi = y^{\psi\varphi} = y^{id_B} = y$$

Damit ist φ surjektiv und somit auch bijektiv.

2.26 (D+A)

- (a) Sind A, B Mengen und $\alpha \in \text{Abb}(A, B)$, so ist $\tilde{\alpha} : \begin{cases} \text{Pot}(B) \rightarrow \text{Pot}(A) \\ y \mapsto y^{\tilde{\alpha}} := \{x \in A \mid x^\alpha \in y\} \end{cases}$
eine Abbildung von $\text{Pot}(B)$ nach $\text{Pot}(A)$, d.h. es gilt $\tilde{\alpha} \in \text{Abb}(\text{Pot}(B), \text{Pot}(A))$.

- (b) Beweise oder widerlege die folgende Behauptung:
Sind A, B Mengen und ist $\alpha \in \text{Abb}(A, B)$, so gilt für alle $A_1, A_2 \in \text{Pot}(A)$ und für alle $B_1, B_2 \in \text{Pot}(B)$ stets:

- (i) $(A_1 \cup A_2)^\alpha = A_1^\alpha \cup A_2^\alpha$
- (ii) $(A_1 \cap A_2)^\alpha = A_1^\alpha \cap A_2^\alpha$
- (iii) $(B_1 \cup B_2)^{\tilde{\alpha}} = B_1^{\tilde{\alpha}} \cup B_2^{\tilde{\alpha}}$
- (iv) $(B_1 \cap B_2)^{\tilde{\alpha}} = B_1^{\tilde{\alpha}} \cap B_2^{\tilde{\alpha}}$

Lösung

- (a) Definition

- (b) (i) • $A_1 \cup A_2 \supset \begin{Bmatrix} A_1 \\ A_2 \end{Bmatrix} \rightsquigarrow (A_1 \cup A_2)^\alpha = \begin{Bmatrix} A_1^\alpha \\ A_2^\alpha \end{Bmatrix}$
• Damit ist $(A_1 \cup A_2)^\alpha \supset A_1^\alpha \cup A_2^\alpha$
• Sei $y \in (A_1 \cup A_2)^\alpha$ beliebig vorgegeben. Dann existiert $x \in A_1 \cup A_2$:
 $x^\alpha = y$.
• Daraus folgt $\begin{cases} \text{entweder } x \in A_1 \rightsquigarrow x^\alpha = y \in A_1^\alpha \subset A_1^\alpha \cup A_2^\alpha \\ \text{oder } x \notin A_1 \rightsquigarrow x \in A_2 \rightsquigarrow x^\alpha = y \in A_2^\alpha \subset A_1^\alpha \cup A_2^\alpha \end{cases}$
• Damit folgt: $A_1^\alpha \cup A_2^\alpha \supset (A_1 \cup A_2)^\alpha$ und weiter

$$(A_1 \cup A_2)^\alpha = A_1^\alpha \cup A_2^\alpha$$

- (ii) • $\begin{Bmatrix} A_1 \supset A_1 \cap A_2 \rightsquigarrow A_1^\alpha \supset (A_1 \cap A_2)^\alpha \\ A_2 \supset A_1 \cap A_2 \rightsquigarrow A_2^\alpha \supset (A_1 \cap A_2)^\alpha \end{Bmatrix} \rightsquigarrow (A_1 \cap A_2)^\alpha \subset A_1^\alpha \cap A_2^\alpha$
• Aber: Sei $A_1 = \{1, 2\}$ $A_2 = \{3, 4\}$. Dann ist $A_1 \cap A_2 = \{\}$.
• Setze $x^\alpha = 1$ für $x = 1, 2, 3, 4$. Damit ist $A_1^\alpha \cap A_2^\alpha = \{1\} \neq \{\}$, aber
 $(A_1 \cap A_2)^\alpha = \{\}^\alpha = \{\}$, d.h die Behauptung (ii) ist falsch!

- (iii) Die Behauptung ist wahr, der Beweis geht analog zu (i).

- (iv) Die Behauptung ist wahr, der Beweis geht analog zu (i).

2.27 (D+S)

Es sei $(P, \mathcal{G}, \parallel)$ ein IREP.

- (a) Eine Abbildung $\delta : \begin{cases} \mathcal{P} \rightarrow \mathcal{P} \\ x \mapsto x^\delta \end{cases}$ heißt *Dilatation*, wenn für alle $(p, q, G) \in \mathcal{P} \times \mathcal{P} \times \mathcal{G}$ mit $q \in (p \parallel G)$ gilt

$$q^\delta \in (p^\delta \parallel G)$$

- (b) Die Menge $\{\delta \in \text{Abb}(\mathcal{P}) \mid \delta \text{ ist Dilatation}\} =: \mathcal{D}$ bildet – Nacheinanderausführung von Abbildungen als Verknüpfung genommen – ein Monoid (\mathcal{D}, \cdot) mit $\text{id}_{\mathcal{P}}$ als neutralem Element.

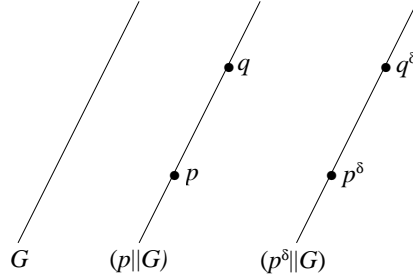


Abbildung 2.8: Dilatation

Beweis

- (a) Definition, nicht beweisbar.
- (b)
- Seien $\delta_1, \delta_2 \in \mathcal{D}$ beliebig vorgegeben.
Nach (a) ist $\delta_1 \cdot \delta_2 \in \text{Abb}(\mathcal{P})$. Ist auch $\delta_1 \cdot \delta_2 \in \mathcal{D}$?
 - Seien $(p, q, G) \in \mathcal{P} \times \mathcal{P} \times \mathcal{G}$ mit $q \in (p \parallel G)$ beliebig vorgegeben.
 - Da $\delta_1 \in \mathcal{D}$, ist $q^{\delta_1} \in (p^{\delta_1} \parallel G)$. Da auch $\delta_2 \in \mathcal{D}$, ist ebenso $(q^{\delta_1})^{\delta_2} \in ((p^{\delta_1})^{\delta_2} \parallel G)$.
 - Demzufolge ist $\delta_1 \cdot \delta_2 \in \mathcal{D}$ und (\mathcal{D}, \cdot) ist Untergruppoid von $(\text{Abb}(\mathcal{P}), \cdot)$.
 - $\mathcal{D} \subset \text{Abb}(\mathcal{P})$ und $(\text{Abb}(\mathcal{P}), \cdot)$ ist assoziativ. Nach (0.21) ist dann auch (\mathcal{D}, \cdot) assoziativ.
Damit ist (\mathcal{D}, \cdot) Unterhalbgruppe von $(\text{Abb}(\mathcal{P}), \cdot)$.
 - Es ist $q^{\text{id}_{\mathcal{P}}} = q \in (p \parallel G) = (p^{\text{id}_{\mathcal{P}}} \parallel G)$, daher ist $\text{id}_{\mathcal{P}} \in \mathcal{D}$.
Damit ist (\mathcal{D}, \cdot) Untermonoid von $(\text{Abb}(\mathcal{P}), \cdot)$, d.h. es gilt (b).

2.28 (S+D)

Es sei $(\mathcal{P}, \mathcal{G}, \parallel)$ ein nicht-trivialer IREP und $\delta \in \mathcal{D}$.

- (a) Ist δ nicht injektiv, so gilt $\mathcal{P}^\delta = \{x^\delta \mid x \in \mathcal{P}\} = \{a\}$ mit einem $a \in \mathcal{P}$.
- (b) Die Abbildung $\delta_a : \begin{cases} \mathcal{P} \rightarrow \mathcal{P} \\ x \mapsto x^{\delta_a} := a \text{ für alle } x \in \mathcal{P} \end{cases}$ ist für jedes $a \in \mathcal{P}$ eine Dilatation mit $\mathcal{P}^{\delta_a} = \{a\}$.

- (c) Die Elemente der Menge $\{\delta_a \mid a \in \mathcal{P}\} =: \Delta_0 \subset \mathcal{D}$ heißen *ausgeartete Dilatationen*
- (d) Zu beliebig vorgegebenen $p, q, a, b \in \mathcal{P}$ mit $p \neq q$ existiert im Fall $a = b$ genau eine Dilatation δ , die $p^\delta = a$ und $q^\delta = b$ genügt, nämlich $\delta_a \in \Delta_0$.

Beweis

- (a)
- Ist $\delta \in \mathcal{D}$ nicht injektiv, so wähle $p, q \in \mathcal{P}$ mit $p \neq q$ und $p^\delta = q^\delta =: a$.
 - Sei $x \in \mathcal{P} \setminus \overline{pq}$ beliebig vorgegeben.
 - Setze $\overline{px} =: G$ und $\overline{qx} =: H$. Dann ist nach [EP] $x \in \overline{px} = (p \parallel G)$ bzw. $x \in \overline{qx} = (q \parallel H)$.
 - Da $\delta \in \mathcal{D}$, folgt $\left\{ \begin{array}{l} x^\delta \in (p^\delta \parallel G) = (a \parallel G) \\ x^\delta \in (q^\delta \parallel H) = (a \parallel H) \end{array} \right\}$. Daher ist $x^\delta \in (a \parallel G) \cap (a \parallel H) =: D \supset \{a\}$.
 - Angenommen $|D| > 1$. Nach $[I_1]$ wäre dann $(a \parallel G) = (a \parallel H)$, also $G \parallel (a \parallel G) = (a \parallel H) \parallel H$ bzw. $G \parallel H$. Nach (2.13) wäre damit $G = H = \overline{pq}$ und, da $x \in G$, auch $x \in \overline{pq}$. q.e.a. Daher ist $|D| \leq 1$.
 - Folglich ist $\mathcal{D} = \{a\}$ und weiter $x^\delta = a$ für alle $x \in \mathcal{P} \setminus \overline{pq}$.
 - Bis hierher haben wir gezeigt: $x^\delta = a$ für alle $x \in \mathcal{P} \setminus \overline{uv}$, falls für $u, v \in \mathcal{D}$ $u \neq v$ und $u^\delta = v^\delta = a$ gilt.
 - Wähle ein $r \in \mathcal{P} \setminus \overline{pq}$ (möglich, da $(\mathcal{P}, \mathcal{G})$ ein nicht-trivialer IR ist). Dann ist $r^\delta = a = p^\delta$, d.h. es gilt $y^\delta = a$ für alle $y \in \mathcal{P} \setminus \overline{pr}$.
 - Wegen $r \notin \overline{pq}$ gilt $\overline{pr} \neq \overline{pq}$ und nach $[I_1]$ folgt $\overline{pr} \cap \overline{pq} = p$.
 - Damit ist $x^\delta = a$ für alle $x \in \overline{pq} \setminus \{p\}$ und es folgt, da $p^\delta = a$, daß $\mathcal{P}^\delta := \{x^\delta \mid x \in \mathcal{P}\} = \{a\}$, d.h. es gilt (a).
- (b)
- Sei $a \in \mathcal{P}$ beliebig vorgegeben.
 - Setze $\delta_a : \begin{cases} \mathcal{P} \rightarrow \mathcal{P} \\ x \mapsto x^{\delta_a} := a \forall x \in \mathcal{P} \end{cases}$, dann ist $\mathcal{P}^{\delta_a} = \{a\}$.
 - Seien $(p, q, G) \in \mathcal{P} \times \mathcal{P} \times \mathcal{G}$ mit $q \in (p \parallel G)$ beliebig vorgegeben.
 - Es ist $q^{\delta_a} = a \in (a \parallel G) \stackrel{p^\delta = a}{=} (p^\delta \parallel G)$. Nach (2.27) folgt daraus $\delta_a \in \mathcal{D}$, d.h. es gilt (b).
- (c) Definition, nicht beweisbar.
- (d)
- Seien $p, q \in \mathcal{P}$ mit $p \neq q$ und $a \in \mathcal{P}$ beliebig vorgegeben.
 - Setze $\{\delta \in \mathcal{D} \mid p^\delta = q^\delta = a\} : \mathcal{D}_a$. Nach (b) ist dann $\delta_a \in \mathcal{D}_a$.
 - Sei umgekehrt $\delta_a \in \mathcal{D}_a$ beliebig vorgegeben.
 - δ ist nicht injektiv und es folgt $\mathcal{P}^\delta = \{x^\delta \mid x \in \mathcal{P}\} \stackrel{(a)}{=} \{p^\delta\} = \{a\}$, d.h. $x^\delta = a \forall x \in \mathcal{P}$, also $\delta = \delta_a$. Damit ist $\mathcal{D}_a \subset \{\delta_a\}$.
 - Folglich ist $\mathcal{D}_a = \{\delta_a\}$, d.h. es gilt (d).

2.29 (S)

It $(\mathcal{P}, \mathcal{G}, \parallel)$ ein nicht-trivialer IREP und sind $p, q; p'q' \in \mathcal{P}$ beliebig vorgegebene Punkte, die $p \neq q$ und $p' \neq q'$ genügen, so gilt stets:

(+) Es gibt höchstens eine Dilatation δ , die $p^\delta = p'$ und $q^\delta = q'$ genügt.

Existiert eine solche Dilatation, so gilt

- (i) $\overline{pq} \parallel \overline{p'q'}$
- (ii) $\delta \in \text{Bij}(\mathcal{P})$
- (iii) $(p \parallel G)^\delta = \{x^\delta \mid x \in (p \parallel G)\} = (p^\delta \parallel G) \in \mathcal{G}$ für alle $(p, G) \in \mathcal{P} \times \mathcal{G}$.
- (iv) Die Umkehrabbildung δ^{-1} ist ebenfalls eine Dilatation mit $(r \parallel G)^{\delta^{-1}} = (r^{\delta^{-1}} \parallel G)$ für alle $(r, G) \in \mathcal{P} \times \mathcal{G}$.

Beweis

- Sei $(\mathcal{P}, \mathcal{G}, \parallel)$ ein nicht-trivialer IREP, δ eine beliebig vorgegebene Dilatation, die $p^\delta = p'$ und $q^\delta = q'$ genügt, und seien $p, q; p'q' \in \mathcal{P}$ beliebig vorgegebene Punkte, die $p \neq q$ und $p' \neq q'$ genügen.
- Es gilt $q \in \overline{pq} = (p \parallel \overline{pq})$ und damit $q' = q^\delta \in (p^\delta \parallel \overline{pq}) = (p' \parallel \overline{pq})$, da δ Dilatation ist. Damit ergibt sich Aussage (i).
- $p^\delta \supset \{p^\delta, q^\delta\} = \{p', q'\}$. Daher ist $|p^\delta| > 1$ und δ ist injektiv.
- Sei $x \in \mathcal{P} \setminus \overline{pq}$ beliebig vorgegeben.
Da δ Dilatation ist, folgt aus $\left\{ \begin{array}{l} x \in \overline{px} = (p \parallel \overline{px}) \\ x \in \overline{qx} = (q \parallel \overline{qx}) \end{array} \right\}$, daß $\left\{ \begin{array}{l} x^\delta \in (p^\delta \parallel \overline{px}) = (p' \parallel \overline{px}) \\ x^\delta \in (q^\delta \parallel \overline{qx}) = (q' \parallel \overline{qx}) \end{array} \right\}$. (Sax)* besagt dann, daß $x^\delta = (p' \parallel \overline{px}) \cap (q' \parallel \overline{qx}) \in \mathcal{P} \setminus \overline{p'q'}$.
- Damit ist x^δ für alle $x \in \mathcal{P} \setminus \overline{pq}$ durch $p, q; p'q'$ eindeutig bestimmt und es ist $x^\delta \in \mathcal{P} \setminus \overline{p'q'}$.
Daraus folgt: $\delta|_{\mathcal{P} \setminus \overline{pq}}$ ist injektive Abbildung von $\mathcal{P} \setminus \overline{pq}$ nach $\mathcal{P} \setminus \overline{p'q'}$ und durch $p, q; p'q'$ eindeutig bestimmt.
- Sei $y \in \mathcal{P} \setminus \overline{p'q'}$ vorgegeben.
- Nach (Sax)* ist $(p \parallel \overline{p'y}) \cap (q \parallel \overline{q'y}) =: x \in \mathcal{P} \setminus \overline{pq}$ eindeutig bestimmt und $\overline{px} \stackrel{[I_2]}{=} (p \parallel \overline{p'y}) \parallel \overline{p'y}$.
- Analog: $\overline{qx} \stackrel{[I-2]}{=} (q \parallel \overline{q'y}) \parallel \overline{q'y}$
- Demnach ist $x^\delta = (p' \parallel \overline{px}) \cap (q' \parallel \overline{qx}) \stackrel{[\text{EP}]}{=} (p' \parallel \overline{p'y}) \cap (q' \parallel \overline{q'y}) = y$.
- Damit ist $\delta|_{\mathcal{P} \setminus \overline{pq}}$ eine Bijektion von $\mathcal{P} \setminus \overline{pq}$ auf $\mathcal{P} \setminus \overline{p'q'}$ und $\delta|_{\mathcal{P} \setminus \overline{pq}}$ ist durch $p, q; p'q'$ eindeutig bestimmt.
- Wähle ein $r \in \mathcal{P} \setminus \overline{pq}$ (möglich, da $(\mathcal{P}, \mathcal{G}, \parallel)$ nicht-trivial). Dann ist $r^\delta =: r' \neq p'$ und $r' \notin \overline{p'q'}$.
- $p, r; p', r' \in \mathcal{P}$ genügen daher $p \neq r$ und $p' \neq r'$ und $p^\delta = p'$ sowie $r^\delta = r'$.

- Damit ist $\delta|_{\mathcal{P} \setminus \overline{p\overline{r}}}$ eine Bijektion von $\mathcal{P} \setminus \overline{p\overline{r}}$ auf $\mathcal{P} \setminus \overline{p'r'}$ und $\delta|_{\mathcal{P} \setminus \overline{p\overline{r}}}$ ist durch $p, r; p'r'$ eindeutig bestimmt.
- Nach $[I_1]$ folgt aus $\left\{ \begin{array}{l} r \notin \overline{pq} \\ r' \notin \overline{p'q'} \end{array} \right\}$, daß $\left\{ \begin{array}{l} \overline{pq} \cap \overline{p\overline{r}} = p \\ \overline{p'q'} \cap \overline{p'r'} = p' \end{array} \right\}$ und weiter, daß $\overline{pq} \setminus \{p\} \subset \mathcal{P} \setminus \overline{p\overline{r}}$.
- Sei $y \in \overline{p'q'} \setminus \{p'\}$ beliebig vorgegeben, dann existiert ein $x \in \mathcal{P} \setminus \overline{p\overline{r}} : a^\delta = y$.
- Damit ist δ surjektive Abbildung von \mathcal{P} auf \mathcal{P} und es folgt Aussage (ii).
- Mit den bisherigen Aussagen wird ferner gezeigt, daß δ durch $p, q, r; p'q', r'$ bereits eindeutig bestimmt ist. Weiterhin ist r' durch $p, q; p'q'$ bereits eindeutig bestimmt.
Folglich ist δ durch $p, q; p'q'$ bereits eindeutig bestimmt, d.h. die Kernaussage (+) ist bewiesen.
- Sei $(p, G) \in \mathcal{P} \times \mathcal{G}$ und $x \in (p \parallel G)$ beliebig vorgegeben.
- Da δ eine Dilatation ist, folgt $x^\delta \in (p^\delta \parallel G)$ und weiter $(p^\delta \parallel G) \supset (p \parallel G)^\delta$ für alle $(p, G) \in \mathcal{P} \times \mathcal{G}$.
- Wegen (ii) existiert zu δ eine Umkehrabbildung δ^{-1} . Ist diese ebenfalls eine Dilatation?
- Sei $(p, q, G) \in \mathcal{P} \times \mathcal{P} \times \mathcal{G}$ mit $q \in (p \parallel G)$ beliebig vorgegeben.
- Dann folgt $\left\{ \begin{array}{l} \text{entweder } p = q : \quad q^{\delta^{-1}} = p^{\delta^{-1}} \in (p^{\delta^{-1}} \parallel G) \\ \text{oder } p \neq q : \quad (p \parallel G) = \overline{pq} ; \quad q^{\delta^{-1}} \neq p^{\delta^{-1}} \\ \quad \text{und } q^{\delta^{-1}} \in \overline{p^{\delta^{-1}} q^{\delta^{-1}}} = (p^{\delta^{-1}} \parallel \overline{p^{\delta^{-1}} q^{\delta^{-1}}}) \end{array} \right.$
- Damit ist $q = q^{\delta^{-1}\delta} \in \left((p^{\delta^{-1}})^\delta \parallel \overline{p^{\delta^{-1}} q^{\delta^{-1}}} \right) = \left(p \parallel \overline{p^{\delta^{-1}} q^{\delta^{-1}}} \right) = \overline{pq} = (p \parallel G)$,
also $\overline{p^{\delta^{-1}} q^{\delta^{-1}}} \parallel \left(p \parallel \overline{p^{\delta^{-1}} q^{\delta^{-1}}} \right) = (p \parallel G)$.
- Da \parallel transitiv ist, folgt $\overline{p^{\delta^{-1}} q^{\delta^{-1}}} \parallel G$ und weiter $q^{\delta^{-1}} \in \left(p^{\delta^{-1}} \parallel \overline{p^{\delta^{-1}} q^{\delta^{-1}}} \right) = \left(p^{\delta^{-1}} \parallel G \right)$.
- Es gilt also in jedem Fall $q^{\delta^{-1}} \in (p^{\delta^{-1}} \parallel G)$, d.h. δ^{-1} ist Dilatation mit $p'^{\delta^{-1}} = p$ und $q'^{\delta^{-1}} = q$ sowie $p' \neq q'; p \neq q$.
- Folglich ist $(r^{\delta^{-1}} \parallel G) \supset (r \parallel G)^{\delta^{-1}}$ für alle $(r, G) \in \mathcal{P} \times \mathcal{G}$.
- $(p \parallel G) = (p^{\delta\delta^{-1}} \parallel G) \supset (p^\delta \parallel G)^{\delta^{-1}} \rightsquigarrow (p \parallel G)^\delta \supset (p^\delta \parallel G)^{\delta^{-1}\delta} = (p \parallel G)^\delta \supset (p \parallel G)^\delta$
- Damit ist

$$(p \parallel G)^\delta = (p^\delta \parallel G) \in G$$
 für alle $(p, G) \in \mathcal{P} \times \mathcal{G}$, d.h. Aussage (iii) ist gezeigt.
- Angewandt auf δ^{-1} statt auf δ ergibt sich analog:

$$(p \parallel G)^{\delta^{-1}} = (p^{\delta^{-1}} \parallel G) \in G$$
 für alle $(p, G) \in \mathcal{P} \times \mathcal{G}$, was Aussage (iv) beweist.

2.30 ...

An dieser Stelle endet meine Mitschrift.

Korrekturen

Bisher wurde in diesem Dokument folgende Korrekturen vorgenommen:

Vers.- Nr.	Datum	Art der Änderung
2,7	08.03.03	Die beiden alten Skripte wurden in ein neues zusammengeführt, im Layout überarbeitet, im Satz vereinheitlicht und mit Inhalts- und Abbildungsverzeichnis sowie einem Index versehen.

Abbildungsverzeichnis

1.1	Punkte in der Ebene bzw. im Raum	49
1.2	Zur Definition der Verbindungsgeraden	60
1.3	Dreieck	64
1.4	Zur Definition der Halbgeraden	65
1.5	Konvexe Hüllen im \mathbb{R}^2	69
1.6	Konvexe Hülle im \mathbb{R}^3	70
1.7	Zur Definition der Senkrechten	74
1.8	Zur Definition des Winkels	76
1.9	Skizze zu Aufgabe 1.51	80
2.1	Zum Euklidischen Parallelaxiom	89
2.2	Zum Schnittaxiom	89
2.3	Zum (erweiterten) Schnittaxiom (Sax)*	92
2.4	Zum Affinen Satz von Desargues	93
2.5	Zum Beweis des Kleinen Affinen Satz von Desargues	94
2.6	Eindeutigkeit eines Parallelogramms	96
2.7	Geradenbündel	96
2.8	Dilatation	99

Index

- Äquivalenzklasse, 87
- Äquivalenzrelation, 86
- Abbildung, 7
 - Schreibweisen, 8
 - skalarprodukttreue, 53
- abelsch
 - DVAG, 32
- abelsches Gruppoid, 14
- Abstand
 - euklidischer A. zweier Punkte, 50
 - zwischen Mengen, 77
- abstandstreu, 52
- ADR, 92
- affine Geometrie, 90
 - Grundmenge der, 62
- affiner Desarguesscher Raum, 92
- affiner Raum, 89
- antisymmetrisch, 86
- assoziativ, 12
- Assoziativgesetz, 12
- Beklammerung, 13
- Bewegung, 52
- Bijektion, 7
 - abstandstreue, 52
- binomische Formel, 33
- Bogenmaß, 76
- Cauchy-Schwartzsche Ungleichung, 50
- Cosinus, 77
- Dilatation, 99
 - ausgeartete, 100
- distributive Verknüpfung abelscher Gruppen, 28
- duale Schreibweise, 8
- DVAG, 28
 - duale, 30
 - kommutative, 32
 - Matrizen-, 36
 - nullteilerfreie, 32
- Einheit, 16
 - engruppe, 23
- Einheitengruppe, 23
- Einheitsvektor, 56
- Element
 - neutrales, 8
- EP, 88
- Euklidischer Vektorraum, 42
- EVR, 42
 - kanonischer n-dimensionaler, 42
- Exponentialschreibweise, 8
- Funktionsschreibweise, 7
- Gerade, 85
 - Bündel, 96
 - Halb-, 65
 - Verbindungs-, 85
- Gruppe, 21
 - abelsche
 - distributive Verknüpfung, 28
 - der Bewegungen des metrischen Raumes, 52
 - Halb-, 12
 - mit neutralem Element, 15
 - Unter-, 25
 - zyklische, 72
- Gruppoid, 8
 - abelsches, 14
 - additiv geschriebenes, 23
 - assoziatives, 12
 - kommutatives, 14
 - mit neutralem Element, 10
 - multiplikativ geschriebenes, 23
 - Unter-, 8
- Hülle, 67
 - konvexe, 68
 - Operator, 72
- Hüllensystem, 67
- Halbgerade, 65
- Halbgruppe, 12
- Hilbertraum, 43
- Inverse, 16, 18
- Inzidenzraum, 85
 - mit euklidischem Parallelenaxiom, 88
- \mathbb{IR} , 85

- kollinear, 88
 - trivialer, 95
- IREP, 88
- K-Vektorraum, 41
- Körper, 28
 - der ganzen Zahlen, 29
- kartesisches Produkt, 7
- Klasse
 - Äquivalenz-, 87
 - Parallel-, 88
- Klasseneinteilung, 86
- Klasseneiteilung
 - induzierte, 87
- kollinear, 88
- kommutativ, 14
 - DVAG, 32
- Kommutativgesetz, 14
- kongruent modulo, 88
- konvex, 65
- konvexe Hülle, 68
- Kroneckersymbol, 56
- Lot
 - gerade, 76
 - Fußpunkt des, 76
- Mächtigkeit, 87
- Matrix, 35
 - Matrizen-DVAG, 36
 - transponierte, 35
- Menge
 - konvexe, 65
- Mengen
 - Standardbezeichnungen, 7
- metrischer Raum, 51
- Mittelpunkt einer Strecke, 63
- modulo, 88
- Monoid, 15
- n-eck, 88
- neutrales Element, 8
- Norm, 50
 - Euklidische, 50
- nullteilerfrei, 32
- Ordnung, 97
- Ordnungsrelation, 86
- parallel, 88
- Parallele, 88
- Parallelnaxiom, euklidisches, 88
- Produkt
 - kartesisches, 7
- Punkt, 50, 85

- Raum
 - affiner, 89
 - affiner Desarguesscher, 92
 - metrischer, 51
- reeller Vektorraum, 42
- reflexiv, 86
- Relation, 86
 - Äquivalenz-, 86
 - Ordnungs-, 86
- Ring, 28
 - der ganzen Zahlen, 29
 - verallgemeinerter, 28
- Schnittaxiom, 89
- Schreibweise
 - duale, 8
 - Exponential-, 8
 - Funktions-, 8
- Schwerpunkt eines Dreiecks, 64
- skalarprodukttreu, 53
- Sphäre, 59
- Standardbeklammernung, 13
- Standardbezeichnungen, 7
- symmetrisch, 86
- transitiv, 86
- Translationsgruppe, 53
- trivial, 95
- trivialer IR, 95
- Untergruppe, 25
- Untergruppenkriterium, 25
- Untergruppoid, 8
- Untervektorraum, 69
- UVR, 69
- Vektor
 - Einheits-, 56
- Vektorraum, 41
 - affine Geometrie über, 90
 - Euklidischer, 42
 - normierter, 50
 - reeller, 42
 - Unter-, 69
- Verbindungsgerade, 60
- Verbindungsstrecke, 63
- Verknüpfung
 - ditributive V. abelscher Gruppen, 28
- Winkel
 - Cosinus, 77
 - zwischen zwei Geraden, 77