

Lösungen der Übungsaufgaben zum Kompendium der diskreten Mathematik (Bernd Baumgarten, De Gruyter, 2014) – Kapitel 7: Algebra –

Bitte beachten Sie:

- Versuchen Sie stets, die Aufgabe zunächst selbst zu lösen! Das Anschauen einer gelösten Übungsaufgabe *ohne vorherigen eigenen ernsthaften Bearbeitungsversuch* nützt Ihnen hinsichtlich des Lernerfolgs oft nicht mehr als der Genuss einer Tasse Kaffee: Es erzeugt vorübergehend ein angenehmes Gefühl.
- Zu jeder Aufgabe kann es verschiedene korrekte Lösungen bzw. Lösungswege und für jede Lösung mehrere Schreibweisen geben. Daher sind die in der Folge vorgestellten Lösungen durchweg nur als Beispiele zu verstehen.
- Zusätzliche Erklärungen stehen in eckigen Klammern [...].
- Auch in Übungsaufgaben können Fehler stecken. Bitte beachten Sie die Errata-Datei auf <http://www.bernd-baumgarten.de/>.

7.1 Verknüpfungen: Assoziativität, Kommutativität, neutrales Element

Es ist jeweils eine Verknüpfungstafel für eine zweistellige Operation \circ angegeben:

a) $\begin{array}{c|cc} \circ & a & b \\ \hline a & b & a \\ \hline b & a & a \end{array}$ b) $\begin{array}{c|cc} \circ & a & b \\ \hline a & a & a \\ \hline b & b & b \end{array}$ c) $\begin{array}{c|cc} \circ & a & b \\ \hline a & b & a \\ \hline b & b & a \end{array}$ auch:
+ auf natürl. Zahlen > 0

d) Man braucht für die Gegenbeispiele jeweils mindestens zwei Elemente.

- [(a) Kommutativität sieht man an der Symmetrie der Tafel bzgl. der Diagonalen.
 $a \circ (a \circ b) = a \circ a = b \neq a = b \circ b = (a \circ a) \circ b$.
Bekannte *nicht* komm. und nicht assoz. Beispiele: Subtraktion und Potenzierung.
- (b) Assoziativität folgt daraus, dass das linke Argument das Ergebnis bestimmt.
 $a \circ b = a \neq b = b \circ a$.
Andere Beispiele: A^* mit der Verkettung von Wörtern, sofern $|A| > 1$.
- (c) Die Operation in der Tabelle hat *weder Links- noch Rechtsneutrales*, denn dessen Zeile bzw. Spalte müsste mit der Kopfzeile für die rechten Argumente bzw. mit der Randspalte für die linken Argumente übereinstimmen. Ebenfalls: + auf \mathbb{N} .
- (d) Eine Verknüpfung auf einer einelementigen Menge $\{a\}$ ist wegen $a \circ a = a$ assoziativ, kommutativ und hat das neutrale Element a .]

7.2 Potenzmenge als Gruppe

Δ ist assoziativ:

Seien M_1, M_2 und M_3 Teilmengen von M , $x \in M$, und A_i die Aussage $x \in M_i$. Dann gilt

$$x \in (M_i \Delta M_k) \Leftrightarrow \neg(A_i \leftrightarrow A_k) \Leftrightarrow (\neg A_i \leftrightarrow A_k) \Leftrightarrow A_i \leftrightarrow A_k$$

mit dem Junktor \leftrightarrow aus Tab. 4.6. im Kapitel Logik, 4.1.7. Diese Äquivalenzen ergeben sich leicht aus der Übereinstimmung der Wahrheitswertverläufe. Somit bedeutet

$$x \in (M_1 \Delta M_2) \Delta M_3 \text{ dasselbe wie } (A_1 \leftrightarrow A_2) \leftrightarrow A_3, \text{ und}$$

$$x \in M_1 \Delta (M_2 \Delta M_3) \text{ dasselbe wie } A_1 \leftrightarrow (A_2 \leftrightarrow A_3), \text{ und}$$

die logische Äquivalenz der beiden rechten logischen Terme folgt aus dem idenischen Wahrheitswertverlauf in der Wahrheitstafel:

A_1	A_2	A_3	$A_1 \leftrightarrow A_2$	$(A_1 \leftrightarrow A_2) \leftrightarrow A_3$	$A_2 \leftrightarrow A_3$	$A_1 \leftrightarrow (A_2 \leftrightarrow A_3)$
W	W	W	F	W	F	W
W	W	F	F	F	W	F
W	F	W	W	F	W	F
W	F	F	W	W	F	W
F	W	W	W	F	F	F
F	W	F	W	W	W	W
F	F	W	F	W	W	W
F	F	F	F	F	F	F

Da also die Mengen $(M_1 \Delta M_2) \Delta M_3$ und $M_1 \Delta (M_2 \Delta M_3)$ dieselben Elemente haben, stimmen sie überein, d.h. Δ ist assoziativ.

[\leftrightarrow ist in der Informatik auch als XOR (exclusive or, entweder/oder) bekannt. Man beachte, dass $(A \leftrightarrow B) \leftrightarrow C$ nicht „entweder A oder B oder C“ bedeutet, da die Formel auch dann wahr ist, wenn alle drei Aussagevariablen wahr sind.]

Ein anderer Weg zum Beweis der Assoziativität von Δ verwendet die Tatsache, dass, wenn wir mit den Wahrheitswerten 1 für wahr und 0 für falsch arbeiten, sowie mit den Indikatorfunktionen

$$I_A(x) = \begin{cases} 1 & \text{wenn } x \in A \\ 0 & \text{sonst} \end{cases}$$

sich dann ergibt $I_{A \Delta B} = I_A + I_B$, allerdings mit 0, 1 und + interpretiert in \mathbb{Z}_2 . Die Assoziativität von Δ ergibt sich dann aus der Assoziativität der Addition in \mathbb{Z}_2 .]

Δ ist kommutativ:

Dies folgt aus der Kommutativität von \cup und \cap :

$$A \Delta B = (A \cup B) \setminus (A \cap B) = (B \cup A) \setminus (B \cap A) = B \Delta A.$$

Es gibt ein neutrales Element bezüglich Δ :

... nämlich die leere Menge, denn

$$\emptyset \Delta A = A \Delta \emptyset = (A \cup \emptyset) \setminus (A \cap \emptyset) = A \setminus \emptyset = A.$$

Es gibt zu jedem $A \in \mathbf{P}(M)$ ein Inverses bezüglich Δ :

... nämlich dieselbe Menge, denn

$$A \Delta A = (A \cup A) \setminus (A \cap A) = A \setminus A = \emptyset.$$

7.3 Nichtkommutative Gruppen

- a) Seien $a, b \in G$ mit $ab \neq ba$ (Verknüpfungszeichen weggelassen). Es kann nicht $a = e$ sein, denn $eb = be = b$, analog auch nicht $b = e$. Es kann auch nicht $a = b$ sein, denn sonst wäre $ba = aa = ab$.

Also sind a, b und e drei verschiedene Elemente. Es kann nicht $ab = a$ sein; sonst gilt (mit $\dots \circ a$) $aba = aa$ und (mit $a^{-1} \circ \dots$) $ba = a = ab$, im Widerspruch zur Voraussetzung $ab \neq ba$. Also ist $ab \neq a$. Analog zeigt man $ab \neq b$, $ba \neq a$ und $ba \neq b$. Auch muss $ab \neq e$ sein, denn sonst wäre $b = a^{-1}$ und $ba = e = ab$. Analog zeigt man $ba \neq e$. Also sind e, a, b, ab und ba fünf verschiedene Elemente.

- b) Tatsächlich sind Gruppen mit einer Primzahl als Mächtigkeit stets abelsch, so dass eine nichtkommutative Gruppe sogar mindestens 6 Elemente haben muss, und eine solche gibt es: die symmetrische Gruppe S_3 .

- c) i. Die sechs Permutationen von $\{1, 2, 3\}$ sind $id, (12), (13), (23), (123)$ und (132) . Hierbei ist z.B. $(12) \circ (13) \neq (13) \circ (12)$, denn z.B. angewendet auf 2 (hintere Permutation zu-erst) ergibt sich links 1 und rechts 3.

Geometrisch können wir die Permutationen als Bewegungen eines gleichseitigen Papp-Dreiecks auffassen, dessen Ecken im Uhrzeigersinn mit 1, 2 und 3 beschriftet sind (Urbild: Welche Ecke lag hier? Bild: Welche liegt nach der Bewegung hier?):

- id Stillstand
- (12) bzw. $(13), (23)$ Spiegelung s_3 bzw. s_2, s_1 an der Symmetrieachse durch 3 bzw. 1, 2
- (123) bzw. (132) Drehung d um 120° bzw. $d \circ d$ um 240° im Uhrzeigersinn.

So geschrieben sieht die Verknüpfungstafel der Gruppe wie folgt aus (hintere Bewegung (Kopfzeile) zuerst):

\circ	id	s_1	s_2	s_3	d	d^2
id	id	s_1	s_2	s_3	d	d^2
s_1	s_1	id	d	d^2	s_2	s_3
s_2	s_2	d^2	id	d	s_3	s_1
s_3	s_3	d	d^2	id	s_1	s_2
d	d	s_3	s_1	s_2	d^2	id
d^2	d^2	s_2	s_3	s_1	id	d

- ii. Man kann an den zwei Polen zu stehen kommen und dort (zwar jeweils nur in einer Himmelsrichtung aber) entlang vier verschiedener Längengrade (0., 90., 180., 270.) in vier verschiedene Richtungen schauen. Das ergibt acht verschiedene Positionen, die nach den Bewegungen Stillstand, L, LL, LLL, V, VL, VLL bzw. VLLL erreicht werden. Die Verknüpfungstafel entspricht der der Bewegungen eines Papp-Quadrats, bis es mit „sich selbst zur Deckung kommt“ (ähnlich wie beim Dreieck in c.i). Eine dritte dazu isomorphe Gruppe ist die der Isomorphismen eines ungerichteten zyklischen Graphen mit vier Knoten.

7.4 Einseitig neutrale und inverse Elemente

Wir lassen das Operationszeichen weg.

- a) Sei c Linksinverses vom Linksinversen b von a (bezüglich des Linksneutralen e), so dass (#) $ba = e = cb$ gilt. Dann folgt der Reihe nach wegen Linksneutralität von e , (#), Assoziativität, (#), Assoziativität, Linksneutralität von e , (#):

$$ab = (ea)b = ((cb)a)b = ((c(ba))b = (ce)b = c(eb) = cb = e \quad (\circ)$$

b ist wegen (\circ) (ganz links = ganz rechts) auch rechtsinvers zu a .

- b) Ferner folgt der Reihe nach wegen (#), Assoziativität, (\circ) , Linksneutralität von e :

$$ae = a(ba) = (ab)a = ea = a. \quad (\bullet)$$

Da dies mit beliebigen $a \in G$ geht, ist e wegen (\bullet) auch linksneutral.

7.5 Gruppenhomomorphismen

- 1) Der Reihe nach wegen/weil der Definition der Hintereinanderausführung $g \circ f$, f Homomorphismus ist, g Homomorphismus ist, sowie der Definition der Hintereinanderausführung gilt:

$$[g \circ f](a \circ_1 b) = g(f(a \circ_1 b)) = g(f(a) \circ_2 f(b)) = g(f(a)) \circ_3 g(f(b)) = [g \circ f](a) \circ_3 [g \circ f](b)$$

- 2) Sind $c, d \in G$, so existieren wegen Surjektivität $a, b, p \in G$ mit $f(a) = c$, $f(b) = d$ und $f(p) = c \circ d$. Nach der Definition der Umkehrabbildung folgt daraus $f^{-1}(c) = a$, $f^{-1}(d) = b$ und $f^{-1}(cd) = p$.

Wegen Homomorphie gilt $f(a \circ b) = f(a) \circ f(b) = c \circ d = f(p)$, wegen Injektivität also auch $a \circ b = p$. Daraus folgt $f^{-1}(c \circ d) = p = a \circ b = f^{-1}(c) \circ f^{-1}(d)$.

- 3) Wegen (1) ist die Hintereinanderausführung eine Verknüpfung auf $\text{Aut}(G, G)$, und sie ist wie bei allen Abbildungen assoziativ. Neutrales Element ist id_G , denn $\text{id}_G \circ f = f \circ \text{id}_G = f$. Die inverse Abbildung ist wegen $f^{-1} \circ f = f \circ f^{-1} = \text{id}_G$ auch Inverses in der – wie sich dadurch zeigt – Gruppe $\text{Aut}(G, G)$.

7.6 Kommutativität und Untergruppen

- a) Man kann zeigen, dass \tilde{K} das neutrale Element sowie Produkte und Inverse seiner Elemente enthält. Unter Verwendung des Untergruppen-Kriteriums in Satz 7.7 kann man auch kürzer so vorgehen:

Seien $x, y \in \tilde{K}$ und $a \in G$. Wir wollen zeigen, dass $xy^{-1}a = axy^{-1}$ (und damit $xy^{-1} \in \tilde{K}$). Das Verknüpfungszeichen und zahlreiche Klammern sind weggelassen, e ist das neutrale Element von G :

Wegen $x, y \in \tilde{K}$ gilt $ax = xa = x(ea) = x(y^{-1}y)a = xy^{-1}(ya) = xy^{-1}(ay)$, woraus durch Multiplikation des ersten und des letzten Terms von rechts mit y^{-1} wie gewünscht folgt: $axy^{-1} = xy^{-1}a$.

b) $\mathbb{Z}_2 \times S_3$ hat 12 Elemente. Ist 0 das neutrale Element von \mathbb{Z}_2 und id_3 das von $\mathbb{Z}_2 \times S_3$, so besteht das Zentrum weder aus der ganzen Gruppe noch nur aus dem neutralen Element $(0, id_3)$, denn

- $(0, (23))$ kommutiert nicht mit allen Elementen, z.B. ist $(0, (23))(0, (13)) = (123) \neq (132) = (0, (13))(0, (23))$, und
- $(1, id_3)$ kommutiert mit allen Elementen, denn $(1, id_3)(x, y) = (1+x, y) = (x+1, y) = (x, y)(1, id_3)$.

[Jedes Produkt einer abelschen Gruppe mit mehr als einem Element und einer nicht kommutativen Gruppe hat auf diese Weise ein nichttriviales Zentrum.]

Die Symmetriegruppe eines Quadrats mit den im Uhrzeigersinn mit 1 bis 4 nummerierten Ecken besteht aus allen Hintereinanderausführungen (beispielsweise) der Drehung d um 90° im Uhrzeigersinn und einer Spiegelung s an der zu 1-2 parallelen Symmetrieachse („Spiegelung 1-2“). So entstehen 8 verschiedene Bewegungen (auch als Permutation der Ecken geschrieben):

Stillstand	e	id	Spiegelung 1-2	s	$(14)(23)$
Drehung 90°	d	(1234)	Spiegelung 2-4	sd	(13)
Drehung 180°	d^2	$(13)(24)$	Spiegelung 2-3	sd^2	$(12)(34)$
Drehung 270°	d^3	(1432)	Spiegelung 1-3	sd^3	(24)

Man erstellt – z.B. durch Betrachtung der Permutationswirkung – leicht eine Verknüpfungstafel, an der man abliest [Symmetrie bzgl. Diagonale? Spalte = Zeile?]:

- Nicht alles kommutiert miteinander, denn z.B. gilt $sd = (13) \neq (24) = ds$.
- Genau e und d^3 kommutieren mit allen 8 Gruppenelementen und bilden so das Zentrum.

7.7 Untergruppen und Homomorphismen

a) Bildmenge $f(U)$ ist Untergruppe von H :

Nach dem Untergruppen-Kriterium von Satz 7.7 ist zu zeigen:

(#) Für beliebige $a, b \in U$ gilt $f(a)[f(b)]^{-1} \in f(U)$.

Aus Satz 7.7 wissen wir, dass $ab^{-1} \in U$. Nach den Homomorphismus-Eigenschaften in Satz 7.4 gilt $f(ab^{-1}) = f(a)f(b^{-1}) = f(a)[f(b)]^{-1}$, insgesamt also (#).

b) Urbildmenge $f^{-1}(V)$ ist Untergruppe von G :

Nach dem Untergruppen-Kriterium von Satz 7.7 ist zu zeigen:

(o) Für beliebige $a, b \in G$ mit $f(a), f(b) \in V$ gilt $ab^{-1} \in f^{-1}(V)$, d.h. $f(ab^{-1}) \in V$.

Nach Satz 7.4 gilt $f(ab^{-1}) = f(a)f(b^{-1}) = f(a)[f(b)]^{-1}$. Aus Satz 7.7 folgt $f(a)[f(b)]^{-1} \in V$, insgesamt also (o).

c) Surjektivität, Injektivität und die Untergruppen $\text{im}(f)$ und $\text{ker}(f)$:

Der Zusammenhang zwischen Surjektivität und $\text{im}(f)$ ergibt sich unmittelbar aus den Definitionen beider Begriffe.

f ist nicht injektiv \Rightarrow Es existieren $a, b \in G$ mit $a \neq b$ und $f(a) = f(b)$.

$\Rightarrow ab^{-1} \neq e$ [sonst mit $\circ b: a = b!$] und

$$f(ab^{-1}) = f(a)f(b^{-1}) = f(a)[f(b)]^{-1} \neq e'$$

[sonst mit $\circ f(b): f(a) = f(b)$]

$\Rightarrow \text{ker}(f) \neq \{e\}$

$\text{ker}(f) \neq \{e\} \Rightarrow$ Es existiert $a \in G$ mit $a \neq e$ und $f(a) = f(e)$.

$\Rightarrow f$ ist nicht injektiv.

7.8 Gruppen-Antiisomorphismen

$inv : g \mapsto g^{-1}$ leistet das Gewünschte:

inv ist ein „Antihomorphismus“:

$$inv(g_1 \circ g_2) = (g_1 \circ g_2)^{-1} = g_1^{-1} g_2^{-1} = inv(g_1) \circ inv(g_2).$$

inv ist bijektiv:

$g = inv(g^{-1})$, also ist inv surjektiv,

und $inv(g_1) = inv(g_2) \Rightarrow g_1 = (g_1^{-1})^{-1} = (g_2^{-1})^{-1} = g_2$, also ist inv injektiv.

7.9 Gruppen endlicher Ordnung

Unter den Potenzen $g^0 := e, g^1 := g, g^2 := g \circ g, \dots$ muss es Wiederholungen – also i, k mit $k > i$ und $g^i = g^k$ – geben (Schubfachprinzip, sonst wäre die Gruppe nicht endlich). Unter den k mit $k > i$ und $g^i = g^k$ gibt es ein kleinstes, k_i . Nach Multiplikation der Elemente $g^i, g^{i+1}, \dots, g^{k_i}$ mit $(g^i)^{-1}$ erhalten wir die Elemente $e, g^1, \dots, g^{k_i-i} = e$, die bis auf das erste und letzte, sämtlich voneinander verschieden sind. Mit $n := k_i - i$ bildet $U := \{e, g^1, \dots, g^{n-1}\}$ eine Untergruppe der Ordnung n von G , denn (da $g^n = e$, also $g^x = e g^x = g^n g^x = g^{n+x}$):

Sind $0 \leq r, s \leq n-1$, also $g^r, g^s \in U$, so ist

$$g^r (g^s)^{-1} = \begin{cases} g^{r-s}, & 0 \leq r-s \leq n-1, & \text{wenn } r \geq s \\ g^{n+r-s}, & 0 \leq n+r-s \leq n-1 & \text{wenn } r < s \end{cases} \in U,$$

also das Untergruppen-Kriterium erfüllt.

Nach dem Satz von Lagrange ist n Teiler von $|G|$, weshalb eine natürliche Zahl m mit $n \cdot m = |G|$ existiert. Also ist $g^{|G|} = g^{n \cdot m} = (g^n)^m = e^m = e$.

7.10 Bewegungsgruppe eines Tetraeders

Bei einer Bewegung des regelmäßigen Tetraeders bis zur Deckungsgleichheit kann jede der vier Ecken $f(1) = 1, 2, 3$ oder 4 an die Positionen der ursprünglichen Ecke 1 zu liegen kommen. Für das gegenüberliegende Dreieck gibt es dann genau drei mögliche Positionen, die sich um eine Drehung um die Achse (Ecke $f(1)$) – (Schwerpunkt des aktuellen Dreiecks 234) unterscheiden. Die sind z.B. beschrieben durch $f(2)$. Das sind zusammen $4 \cdot 3$, also 12 Bewegungen, entsprechend 12 der 24 möglichen Permutationen.

Die *Symmetriegruppe* (oder Bewegungsgruppe) dieses Polyeders ist hier also (im Gegensatz zur Symmetriegruppe des räumlich bewegbaren regelmäßigen Dreiecks) verschieden von der *symmetrischen Gruppe* (bestehend aus den Permutationen der Eckennummern). Das liegt an der sog. *Chiralität*: Der gespiegelte Tetraeder kann nicht in sein Original gedreht werden. Er kann aber seinerseits 12 Positionen einnehmen, entsprechend den anderen 12 Permutationen.

[Dies hängt mit der Existenz einer „Schraubrichtung“ zusammen: Ein Durchlaufen der Ecken des abgebildeten Tetraeders ist eine rechtsschraubende Bewegung. Wären die Nummern $2, 3, 4$ gegen den Uhrzeigersinn angeordnet, ergäbe sich eine linksschraubende Bewegung.]

Die Transformation in einen gespiegelten (linksschraubenden) Tetraeder kann entlang der Symmetrieebenen durch die sechs Kanten erfolgen. Eine solche Spiegelung vertauscht die zwei Ecken, die außerhalb der Ebene liegen, entspricht also genau einer der sechs möglichen Transpositionen $(12), (13), (14), (23), (24), (34)$. So wird (34) von der Spiegelung an der Symmetrieebene durch die Kante 12 bewirkt. Eine anschließende weitere Transposition spiegelt den Tetraeder wieder ins Original (wenn auch i.a. in anderer Lage). Jede Permutation ist aber Produkt von Transpositionen (Satz 3.10). Also entsprechen die Permutationen, die den gespiegelten Tetraeder positionieren, den ungeraden Permutationen, und die reinen *Bewegungen* entsprechen den *geraden* Permutationen.

[Dies alles ist hier wenig formal unterfüttert, da das geometrische Handwerkszeug, wie zu Beginn von Kapitel 7 erläutert, ausgeklammert bleibt.]

7.11 Endomorphismenringe

a) Die Ringeigenschaften der Endomorphismen von $(G, +) - \text{Endo}(G)$ – mit punktweiser Addition und Hintereinanderausführung \circ :

- $+$ ist Verknüpfung auf $\text{Endo}(G)$, denn mit f und g aus $\text{Endo}(G)$ ist $f + g$
 - Abbildung von G nach G ,
denn für $x \in G$ ist mit $f(x)$ und $g(x)$ auch $f(x) + g(x)$ in G ,
 - und auch Homomorphismus,
denn für f und g aus $\text{Endo}(G)$ sowie $x \in G$ gilt

$$(f + g)(x + y) = f(x + y) + g(x + y) = (f(x) + f(y)) + (g(x) + g(y))$$

$$= (f(x) + g(x)) + (f(y) + g(y)) = (f + g)(x) + (f + g)(y),$$
 wobei beim Übergang vom Ende der ersten Zeile zum Anfang der zweiten die Assoziativität und Kommutativität von $+$ in G genutzt werden
- Mit der Verknüpfung $+$ bildet $\text{Endo}(G)$ eine abelsche Gruppe:
 - $+$ ist assoziativ,
denn wegen der Assoziativität von $+$ in G gilt für alle $x \in G$

$$((f + g) + h)(x) = (f + g)(x) + h(x) = (f(x) + g(x)) + h(x)$$

$$= f(x) + (g(x) + h(x)) = f(x) + (g + h)(x) = (f + (g + h))(x).$$
 - $+$ ist kommutativ,
auf analoge Weise wegen der Kommutativität von $+$ in G .
 - Neutrales Element ...
ist die konstante Abbildung auf das neutrale Element 0 von G , nennen wir es ebenfalls 0 , denn für alle $x \in G$ gilt

$$(f + 0)(x) = f(x) + 0(x) = f(x) + 0 = f(x),$$
 also $f + 0 = f$, und z.B. wegen Kommutativität auch $0 + f = f$.
 - Die $+$ -Inverse zu f ...
ist $-f$, definiert durch $(-f)(x) := -f(x)$, letzteres das Inverse zu $f(x)$ in G mit seiner Gruppenoperation $+$, denn für alle $x \in G$ ist

$$(f + (-f))(x) = f(x) + (-f)(x) = f(x) + (-f(x)) = 0 = 0(x).$$
- Die G -Endomorphismen bilden mit \circ eine Halbgruppe:
 - \circ ist Verknüpfung auf $\text{Endo}(G)$,
denn mit f und g aus $\text{Endo}(G)$ bildet $g \circ f$ natürlich selbst G in G ab und ist als Hintereinanderausführung zweier Gruppenhomomorphismen auf $(G, +)$ ebenfalls einer.
 - \circ ist assoziativ
wegen der Assoziativität der Hintereinanderausführung von Abbildungen.
- Die Distributivgesetze gelten für \circ und $+$ wegen

$$(f \circ (g + h))(x) = f((g + h)(x)) = f(g(x) + h(x)) = f(g(x)) + f(h(x))$$

$$= (f \circ g)(x) + (f \circ h)(x) = ((f \circ g) + (f \circ h))(x)$$
 und

$$((f + g) \circ h)(x) = (f + g)(h(x)) = f(h(x)) + g(h(x))$$

$$= (f \circ h)(x) + (g \circ h)(x) = ((f \circ h) + (g \circ h))(x)$$

[Die Begründungen sind sehr einfach. Die Hauptarbeit ist, an alles zu denken!]

- b)
- f = Multiplikation mit 2,
 - g = Multiplikation mit 3,
 - $f + g$ = Multiplikation mit 5,
 - $f \circ g$ = Multiplikation mit 6.

- (c) Da die 1- bis 3-elementigen Gruppen alle zyklisch sind, jedes ihrer Elemente also eine Potenz $e^n = e \circ \dots \circ e$ (n -mal, $0 \leq n < |G|$), sind deren Endomorphismen durch das Bild von e bestimmt, können also nur von der Art f_n sein.

Die im Tipp gezeigte (sog. Klein'sche) Vierergruppe ist nicht zyklisch. Wegen $1+1=0$ in \mathbb{Z}_2 gibt es an unterschiedlichen Vielfachen f_n nur f_0 und f_1 . Mit Linearer Algebra ergibt sich, dass die Multiplikation mit einer 2×2 -Matrix über \mathbb{Z}_2 ein $((\mathbb{Z}_2)^2, +)$ -Gruppenendomorphismus ist, dass es also mindestens 16 verschiedene (s.u.) Endomorphismen gibt. Also bleiben (mindestens) 14 Endomorphismen, die keinem f_n entsprechen, zum Beispiel

- die Vertauschung der Komponenten $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_2 \\ x_1 \end{pmatrix}$ und
- die Projektion auf die erste Komponente $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_1 \\ 0 \end{pmatrix}$.

[Da das Bild eines Vektors in $(\mathbb{Z}_2)^2$ bereits durch die (jeweils 4 möglichen) Bilder der erzeugenden Vektoren $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ und $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ festgelegt ist, kann es insgesamt auch nur

$4 \cdot 4 = 16$ Endomorphismen auf der Gruppe $((\mathbb{Z}_2)^2, +)$ geben. Also kann „mindestens“ oben entfallen]

7.12 Nullteiler und Einheiten im Ring

- a) Wir beweisen sogar: Ist $(R, +, \cdot)$ ein Ring mit Nullelement 0, dann gilt für alle $a \in R \setminus \{0\}$: a ist genau dann *kein* linker Nullteiler, wenn die Abbildung $f_a : x \mapsto a \cdot x$ von R nach R injektiv ist.

Sind $a \in R \setminus \{0\}$, $x, y \in R$ und a kein linker Nullteiler, dann folgt

$$\begin{aligned} a \cdot x = a \cdot y &\Rightarrow a \cdot (x - y) = a \cdot x - a \cdot y = 0 \Rightarrow a \text{ oder } x - y \text{ ist } 0 \text{ (aber } a \neq 0) \\ &\Rightarrow x - y = 0 \Rightarrow x = y, \text{ d.h. } f_a \text{ ist injektiv.} \end{aligned}$$

Ist $a \in R \setminus \{0\}$, und f_a injektiv, so kann a also kein linker Nullteiler sein, denn gäbe es ein $b \in R \setminus \{0\}$ mit $a \cdot b = 0$, so folgte daraus $a \cdot b = a \cdot 0$ und wegen der Injektivität von f_a $b = 0$ – ein Widerspruch.

- b) Sei R endlicher kommutativer Ring mit Eins (also per Def. $0 \neq 1$) und $T_R(0)$ die Menge der (echten wie trivialen) Nullteiler von R .

$R^* \cap T_R(0) = \emptyset$: Gäbe es ein $a \in R^* \cap T_R(0)$, so gäbe es in R ein $b \neq 0$ mit $a \cdot b \neq 0$ und ein c mit $c \cdot a = 1$, so dass $0 = c \cdot 0 = c \cdot (a \cdot b) = (c \cdot a) \cdot b = 1 \cdot b = b$ – ein Widerspruch.

$R^* \cup T_R(0) = R$: Nehmen wir das Gegenteil an: Es gibt ein $a \in R$, das weder Nullteiler noch Einheit ist. Dann ist die Multiplikation $f_a(x) = a \cdot x$, $f_a : R \rightarrow R$, nicht surjektiv, denn gäbe es ein $f_a(b) = a \cdot b = 1$ mit $f_a(b) = a \cdot b = 1$, so wäre a Einheit. Wegen der Endlichkeit von R (und des Schubfachprinzips, denn $|R|$ Bilder $f_a(x)$ sind auf $|f_a(R)| < |R|$ Plätze aufzuteilen) ist f_a nun auch nicht injektiv und nach (a) oben wäre a Nullteiler. Also ist die Annahme falsch und $R^* \cup T_R(0) = R$ wahr.

Insgesamt: $\{R^*, T_R(0)\}$ ist eine Partition von R .

7.13 Ringe und Homomorphismen

Seien $(R, +, \cdot)$ und (Q, \oplus, \otimes) Ringe, U ein Unterring von R und V ein Unterring von Q . man beachte, dass dann U eine Untergruppe von $(R, +)$ und V eine Untergruppe von (Q, \oplus) ist.

- a) Bildmenge $f(U)$ ist Unterring von Q :
 Nach Satz 7.8 ist $f(U)$ Untergruppe von (Q, \oplus) , und nach Satz 7.7 gilt für $a, b \in U$:
 $f(a) - f(b) \in f(U)$. Ferner gilt $f(a) \otimes f(b) = f(a \cdot b)$ und nach Satz 7.14 $a \cdot b \in U$,
 also $f(a) \otimes f(b) = f(a \cdot b) \in f(U)$. Das Unterring-Kriterium von Satz 7.14 ist daher
 für $f(U)$ erfüllt.
- b) Urbildmenge $f^{-1}(V)$ ist Unterring von R :
 Nach Satz 7.8 ist $f^{-1}(V)$ Untergruppe von R , und nach Satz 7.7 gilt für
 $a, b \in f^{-1}(V)$: $a - b \in V$. Ferner gilt $f(a \cdot b) = f(a) \otimes f(b)$ und nach Satz 7.14
 $f(a) \otimes f(b) \in V$. Das Unterring-Kriterium von Satz 7.14 ist daher für $f^{-1}(V)$ erfüllt.

[Natürlich können auch unter Verwendung von weniger Sätzen die Unterring-Definitionen
 unmittelbar überprüft werden.]

7.14 Zerlegung eines Restklassenrings

[Wiederholte Addition des jeweiligen Einselementes, also von $(1,1) \in \mathbb{Z}_4 \times \mathbb{Z}_3$ bzw. $1 \in \mathbb{Z}_{12}$,
 zum jeweiligen Nullelement $(0,0)$ bzw. 0 ergibt – ebenso wie die in Satz 7.17 beschriebene
 Abbildung:]

(0,0)	(1,1)	(2,2)	(3,0)	(0,1)	(1,2)	(2,0)	(3,1)	(0,2)	(1,0)	(2,1)	(3,2)
0	1	2	3	4	5	6	7	8	9	10	11

7.15 Produktkörper

Die Antwort ist: Es geht nicht.

Im Produktring $K_1 \times K_2$ gilt $(0,1) \cdot (1,0) = (0,0)$, und $(0,0)$ ist sein Nullelement. Im Körper
 K_1 bzw. K_2 gilt $0 \neq 1$ und damit im Produktring $(1,0) \neq (0,0)$. Also sind in $K_1 \times K_2$ $(0,1)$
 und $(1,0)$ echte Nullteiler. Wäre $K_1 \times K_2$ ein Körper, hätte er aber wegen der Abgeschlossen-
 heit eines Körpers abzüglich seines Nullelementes gegenüber der Multiplikation (2. Körpereigenschaft!) *keine* Nullteiler.

7.16 Endliche Körper

[\mathbb{Z}_2 eignet sich nicht, da dort $1 = -1$ gilt und damit -1 die Wurzel 1 hat.

\mathbb{Z}_3 eignet sich, da dort $2 = -1$, aber $0 \cdot 0 = 0$ und $1 \cdot 1 = 2 \cdot 2 = 1$ gilt, so dass -1 keine Quadratwurzel hat.]

Wir nehmen $K = \{(a,b) \mid a,b \in \mathbb{Z}_3\}$ als Menge mit der komponentenweisen Addition und (analog zu den komplexen Zahlen) der Multiplikation

$(a_1, b_1) \cdot (a_2, b_2) := (a_1 \cdot a_2 - b_1 \cdot b_2, a_1 \cdot b_2 + b_1 \cdot a_2)$, alles modulo 3 gerechnet, und schreiben $a + b \cdot i$ für (a,b) etc., so dass $i^2 = -1$ gilt. Zunächst ist K (wie jedes Gruppenprodukt) mit $+$ eine kommutative Gruppe. Die Multiplikation

- ist assoziativ:

$$\begin{aligned} ((a_1, b_1) \cdot (a_2, b_2)) \cdot (a_3, b_3) &= (a_1 \cdot a_2 - b_1 \cdot b_2, a_1 \cdot b_2 + b_1 \cdot a_2) \cdot (a_3, b_3) \\ &= ((a_1 \cdot a_2 - b_1 \cdot b_2) \cdot a_3 - (a_1 \cdot b_2 + b_1 \cdot a_2) \cdot b_3, \\ &\quad (a_1 \cdot a_2 - b_1 \cdot b_2) \cdot b_3 + a_3 \cdot (a_1 \cdot b_2 + b_1 \cdot a_2)) \\ &= (a_1 a_2 a_3 - b_1 b_2 a_3 - a_1 b_2 b_3 - b_1 a_2 b_3, \\ &\quad a_1 a_2 b_3 - b_1 b_2 b_3 + a_1 b_2 a_3 + b_1 a_2 a_3) \\ &= (a_1, b_1) \cdot (a_2 \cdot a_3 - b_2 \cdot b_3, a_2 \cdot b_3 + b_2 \cdot a_3) \\ &= (a_1, b_1) \cdot ((a_2, b_2) \cdot (a_3, b_3)) \end{aligned}$$

- ist kommutativ:

$$\begin{aligned} (a_1, b_1) \cdot (a_2, b_2) &= (a_1 \cdot a_2 - b_1 \cdot b_2, a_1 \cdot b_2 + b_1 \cdot a_2) \\ &= (a_2 \cdot a_1 - b_2 \cdot b_1, a_2 \cdot b_1 + b_2 \cdot a_1) \\ &= (a_1, b_1) \cdot (a_2, b_2) \end{aligned}$$

- hat das Einselement 1, d.h. $1 + 0 \cdot i$, d.h. $(1,0)$:

$$\begin{aligned} (a, b) \cdot (1, 0) &= (a \cdot 1 - b \cdot 0, a \cdot 0 + 1 \cdot b) \\ &= (a, b) \\ &= (1 \cdot a - 0 \cdot b, 0 \cdot a + b \cdot 1) \\ &= (1, 0) \cdot (a, b). \end{aligned}$$

- Das Inverse zu (a, b) ($\neq (0,0)$) ist – vgl. Übung 5.11.iv: $\left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \right)$.

- Das Linksdistributivgesetz gilt ebenfalls:

$$\begin{aligned} (a_1, b_1) \cdot ((a_2, b_2) + (a_3, b_3)) &= (a_1, b_1) \cdot (a_2 + a_3, b_2 + b_3) \\ &= (a_1 \cdot (a_2 + a_3) - b_1 \cdot (b_2 + b_3), a_1 \cdot (b_2 + b_3) + b_1 \cdot (a_2 + a_3)) \\ &= (a_1 a_2 + a_1 a_3 - b_1 b_2 - b_1 b_3, a_1 b_2 + a_1 b_3 + b_1 a_2 + b_1 a_3) \\ &= (a_1 \cdot a_2 - b_1 \cdot b_2, a_1 \cdot b_2 + b_1 \cdot a_2) + (a_1 \cdot a_3 - b_1 \cdot b_3, a_1 \cdot b_3 + b_1 \cdot a_3) \\ &= (a_1, b_1) \cdot (a_2, b_2) + (a_1, b_1) \cdot (a_3, b_3) \end{aligned}$$

Wegen der Kommutativität reicht jeweils eine halbe Tabelle, hier rechts oben die Additions- und links unten in rot die Multiplikationsergebnisse:

	0	1	2	i	$1+i$	$2+i$	$2i$	$1+2i$	$2+2i$	plus
	0	1	2	i	$1+i$	$2+i$	$2i$	$1+2i$	$2+2i$	0
0	0	2	0	$1+i$	$2+i$	i	$1+2i$	$2+2i$	$2i$	1
1	0	1	1	$2+i$	i	$1+i$	$2+2i$	$2i$	$1+2i$	2
2	0	2	1	$2i$	$1+2i$	$2+2i$	0	1	2	i
i	0	i	$2i$	2	$2+2i$	$2i$	1	2	0	$1+i$
$1+i$	0	$1+i$	$2+2i$	$2+i$	$2i$	$1+2i$	2	0	1	$2+i$
$2+i$	0	$2+i$	$1+2i$	$2+2i$	1	i	i	$1+i$	$2+i$	$2i$
$2i$	0	$2i$	i	1	$1+2i$	$1+i$	2	$2+i$	i	$1+2i$
$1+2i$	0	$1+2i$	$2+i$	$1+i$	2	$2i$	$2+2i$	i	$1+i$	$2+2i$
$2+2i$	0	$2+2i$	$1+i$	$1+2i$	i	2	$2+i$	1	$2i$	
mal	0	1	2	i	$1+i$	$2+i$	$2i$	$1+2i$	$2+2i$	

[Man vervollständigt eine Spalte bzw. Zeile leicht, indem man sie bis zur Diagonale (also bis zum vorläufigen Abbruch) liest, von dort aus abbiegt und in der Zeile bzw. Spalte weiter liest.]

7.17 Satz von Wilson

In $\mathbb{Z}_p \setminus \{0\}$ kann es Elemente a geben, die von ihrem multiplikativen Inversen a^{-1} verschieden sind, d.h. mit $a \neq a^{-1}$. Für jede Teilmenge $M \subseteq \mathbb{Z}_p \setminus \{0\}$, die solch ein Paar $\{a, a^{-1}\}$, $a \neq a^{-1}$, enthält, gilt wegen $a \cdot a^{-1} = 1$:

$$\prod_{x \in M} x = (a \cdot a^{-1}) \cdot \prod_{x \in M \setminus \{a, a^{-1}\}} x = \prod_{x \in M \setminus \{a, a^{-1}\}} x.$$

Wenn man nun solange wie möglich solche Paare aus $\mathbb{Z}_p \setminus \{0\}$ herausstreicht, gilt, ohne dass sich das Produkt über die verbleibenden Elemente ändert, am Ende:

$$\prod_{x \in \mathbb{Z}_p \setminus \{0\}} x = \prod_{\substack{x \in \mathbb{Z}_p \setminus \{0\}, \\ x = x^{-1}}} x.$$

Für jedes der verbliebenen Elemente $x \in \mathbb{Z}_p \setminus \{0\}$ mit $x = x^{-1}$ gilt $x^2 = 1$, also auch

$$(x+1) \cdot (x-1) = x^2 - 1 = 0.$$

Da der Körper \mathbb{Z}_p aber (vgl. Lösung 7.15) keine echten Nullteiler hat, folgt für die $x \in \mathbb{Z}_p \setminus \{0\}$ mit $x = x^{-1}$, dass $x+1=0$ oder $x-1=0$ gilt. Es kann sich also nur um die Elemente 1 und -1 handeln, wobei die beiden in \mathbb{Z}_2 zusammenfallen, und das Produkt der beiden Elemente (oder das eine) ist auf jeden Fall -1 , also

$$\prod_{x \in \mathbb{Z}_p \setminus \{0\}} x = \prod_{\substack{x \in \mathbb{Z}_p \setminus \{0\}, \\ x = x^{-1}}} x = 1 \cdot (-1) = -1.$$

7.18 Schiefkörper

Vorab die unten benötigten Rechenregeln für Konjugation in \mathbb{C} , nämlich dass sie über Addition und Multiplikation distribuiert und selbstinvers ist ($x_i, y_i \in \mathbb{R}$):

$$\begin{aligned}\overline{(x_1 + y_1i) + (x_2 + y_2i)} &= \overline{(x_1 + x_2) + (y_1 + y_2)i} \\ &= \overline{(x_1 + x_2) - (y_1 + y_2)i} \\ &= \overline{(x_1 - y_1i) + (x_2 - y_2i)} \\ &= \overline{(x_1 + y_1i) + (x_2 + y_2i)}\end{aligned}$$

$$\begin{aligned}\overline{(x_1 + y_1i) \cdot (x_2 + y_2i)} &= \overline{(x_1x_2 - y_1y_2) + (x_1y_2 + y_1x_2)i} \\ &= \overline{(x_1x_2 - y_1y_2) - (x_1y_2 + y_1x_2)i} \\ &= \overline{(x_1 - y_1i) \cdot (x_2 - y_2i)} \\ &= \overline{(x_1 + y_1i) \cdot (x_2 + y_2i)}\end{aligned}$$

$$\begin{aligned}\overline{\overline{x_1 + y_1i}} &= \overline{x_1 - y_1i} \\ &= x_1 - (-y_1)i \\ &= x_1 + y_1i\end{aligned}$$

Zunächst ist $\mathbb{C} \times \mathbb{C}$ (wie jedes Gruppenprodukt) mit $+$ eine kommutative Gruppe. Die Multiplikation

- ist assoziativ:

$$\begin{aligned}((a_1, b_1) \cdot (a_2, b_2)) \cdot (a_3, b_3) &= (a_1 \cdot a_2 - b_1 \cdot \overline{b_2}, a_1 \cdot b_2 + b_1 \cdot \overline{a_2}) \cdot (a_3, \overline{b_3}) \\ &= ((a_1 \cdot a_2 - b_1 \cdot \overline{b_2}) \cdot a_3 - (a_1 \cdot b_2 + b_1 \cdot \overline{a_2}) \cdot \overline{b_3}, \\ &\quad (a_1 \cdot a_2 - b_1 \cdot \overline{b_2}) \cdot \overline{b_3} + (a_1 \cdot b_2 + b_1 \cdot \overline{a_2}) \cdot a_3) \\ &= (a_1 a_2 a_3 - a_1 b_2 \overline{b_3} - b_1 a_2 \overline{b_3} - b_1 b_2 a_3, \\ &\quad a_1 a_2 \overline{b_3} + a_1 b_2 a_3 + b_1 a_2 a_3 - b_1 b_2 \overline{b_3}) \\ &= (a_1 \cdot (a_2 \cdot a_3 - b_2 \cdot \overline{b_3}) - b_1 \cdot (a_2 \cdot \overline{b_3} + b_2 \cdot a_3), \\ &\quad a_1 \cdot (a_2 \cdot \overline{b_3} + b_2 \cdot a_3) + b_1 \cdot (a_2 \cdot a_3 - b_2 \cdot \overline{b_3})) \\ &= (a_1, b_1) \cdot (a_2 \cdot a_3 - b_2 \cdot \overline{b_3}, a_2 \cdot \overline{b_3} + b_2 \cdot a_3) \\ &= (a_1, b_1) \cdot ((a_2, b_2) \cdot (a_3, b_3))\end{aligned}$$

- ist *nicht* kommutativ, denn $(i, 0) \cdot (0, 1) = (0, i) \neq (0, -i) = (0, 1) \cdot (i, 0)$

- hat das Einselement $(1, 0)$:

$$\begin{aligned}(a, b) \cdot (1, 0) &= (a \cdot 1 - b \cdot 0, a \cdot 0 + b \cdot 1) \\ &= (a, b) \\ &= (1 \cdot a - 0 \cdot \overline{b}, 1 \cdot b + 0 \cdot \overline{a}) \\ &= (1, 0) \cdot (a, b).\end{aligned}$$

- Das multiplikative Inverse zu (a, b) ($\neq (0, 0)$) ist $\left(\frac{\overline{a}}{a \cdot \overline{a} + b \cdot \overline{b}}, \frac{-b}{a \cdot \overline{a} + b \cdot \overline{b}} \right)$, wobei in den Komponenten die komplexe Multiplikation hier ohne Punkt geschrieben ist:

$$(a, b) \cdot \left(\frac{\overline{a}}{a\overline{a} + b\overline{b}}, \frac{-b}{a\overline{a} + b\overline{b}} \right) = \left(\frac{a\overline{a} - b(-\overline{b})}{a\overline{a} + b\overline{b}}, \frac{a(-b) + b\overline{a}}{a\overline{a} + b\overline{b}} \right) = (1, 0)$$

- Das Links- und das Rechts-Distributivgesetz (was ja mangels Kommutativität nicht aus dem linken folgt) gelten ebenfalls:

$$\begin{aligned}
(a_1, b_1) \cdot ((a_2, b_2) + (a_3, b_3)) &= (a_1, b_1) \cdot (a_2 + a_3, b_2 + b_3) \\
&= (a_1(a_2 + a_3) - b_1 \overline{(b_2 + b_3)}, a_1(b_2 + b_3) + b_1 \overline{(a_2 + a_3)}) \\
&= (a_1 a_2 + a_1 a_3 - b_1 \overline{b_2} - b_1 \overline{b_3}, a_1 b_2 + a_1 b_3 + b_1 \overline{a_2} + b_1 \overline{a_3}) \\
&= (a_1 a_2 - b_1 \overline{b_2} + a_1 a_3 - b_1 \overline{b_3}, a_1 b_2 + b_1 \overline{a_2} + a_1 b_3 + b_1 \overline{a_3}) \\
&= (a_1 a_2 - b_1 \overline{b_2}, a_1 b_2 + b_1 \overline{a_2}) + (a_1 a_3 - b_1 \overline{b_3}, a_1 b_3 + b_1 \overline{a_3}) \\
&= ((a_1, b_1) \cdot (a_2, b_2)) + ((a_1, b_1) \cdot (a_3, b_3)) \\
((a_1, b_1) + (a_2, b_2)) \cdot (a_3, b_3) &= (a_1 + a_2, b_1 + b_2)(a_3, b_3) \\
&= ((a_1 + a_2)a_3 - (b_1 + b_2)\overline{b_3}, (a_1 + a_2)b_3 + (b_1 + b_2)\overline{a_3}) \\
&= (a_1 a_3 + a_2 a_3 - b_1 \overline{b_3} - b_2 \overline{b_3}, a_1 b_3 + a_2 b_3 + b_1 \overline{a_3} + b_2 \overline{a_3}) \\
&= (a_1 a_3 - b_1 \overline{b_3} + a_2 a_3 - b_2 \overline{b_3}, a_1 b_3 + b_1 \overline{a_3} + a_2 b_3 + b_2 \overline{a_3}) \\
&= (a_1 a_3 - b_1 \overline{b_3}, a_1 b_3 + b_1 \overline{a_3}) + (a_2 a_3 - b_2 \overline{b_3}, a_2 b_3 + b_2 \overline{a_3}) \\
&= ((a_1, b_1) \cdot (a_3, b_3)) + ((a_2, b_2) \cdot (a_3, b_3))
\end{aligned}$$

[Dieser Körper (bzw. ein dazu isomorpher) findet sich in der Literatur oder im Internet auch unter dem Namen *Quaternionenkörper*: Wenn man die obigen Elemente $(a + bi, c + di)$ als $a + bi + cj + dk$ schreibt, und j und k als weitere „ i -artige“ Zahlen mit der Multiplikationstafel

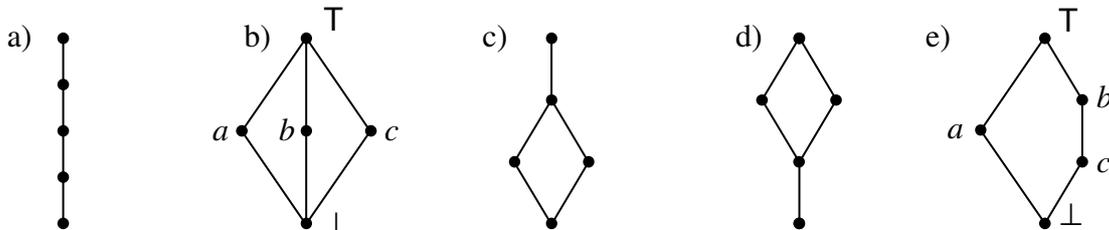
\cdot	i	j	k
i	-1	k	$-j$
j	$-k$	-1	i
k	j	$-i$	-1

behandelt, hat man den Übergang im Prinzip bewältigt.]

7.19 Kleine Verbände

Zunächst gibt es (wie bei allen endlichen Verbänden) ein größtes und ein kleinstes Element T und \perp – beide voneinander verschieden, damit es mehr als ein Element geben kann: Jetzt müssen nur noch drei Elemente dazwischen platziert werden (denn Infima und Suprema gibt es jetzt stets!), entweder

- alle drei untereinander geordnet (a) (kein Paar der drei unvergleichbar) oder
- alle drei paarweise unvergleichbar (b) oder
- genau ein Paar unvergleichbar und
 - das dritte Element darüber (c) oder
 - darunter (d) oder
- genau zwei Paare unvergleichbar (e):



(b) ist nicht distributiv: $a \sqcap (b \sqcap c) = a \sqcap \perp = a$
 $(a \sqcap b) \sqcap (a \sqcap c) = T \sqcap T = T$

(e) ist nicht distributiv: $b \sqcap (a \sqcap c) = b \sqcap T = b$
 $(b \sqcap a) \sqcap (b \sqcap c) = \perp \sqcap c = c$

7.20 Distributive Ungleichungen und Gleichungen in Verbänden

- a) Für die Verbandsordnung \leq gilt nach Abschnitt 3.6.4

$$x \sqcap y = \inf\{x, y\}, \quad x \sqcap y = x \Leftrightarrow x \leq y, \quad x \sqcup y = \sup\{x, y\}, \quad x \sqcup y = x \Leftrightarrow x \geq y.$$

Gemäß der Definition der unteren und oberen Schranken, insbesondere \inf und \sup , ist $a \sqcap b \leq a$ und $a \sqcap b \leq b \leq b \sqcup c$. Somit ist $a \sqcap b$ als untere Schranke von a und $b \sqcup c$ kleiner oder gleich der größten unteren Schranke (dem \inf) der beiden:

$$a \sqcap b \leq a \sqcap (b \sqcup c).$$

Entsprechend folgt aus $a \sqcap c \leq a$ und $a \sqcap c \leq c \leq b \sqcup c$, dass

$$a \sqcap c \leq a \sqcap (b \sqcup c).$$

Also ist $a \sqcap (b \sqcup c)$ als obere Schranke von $a \sqcap b$ und von $a \sqcap c$ größer oder gleich der kleinsten oberen Schranke (dem \sup) der beiden:

$$a \sqcap (b \sqcup c) \geq \sup\{a \sqcap b, a \sqcap c\} = (a \sqcap b) \sqcup (a \sqcap c).$$

Die andere Verbandsungleichung folgt analog (genauer: dual) zum Vorstehenden.

- b) „ \Rightarrow “: Gilt die erste Distributivitätsgleichung, so folgt wegen der Kommutativität und $a \sqcup (a \sqcap c) = a = (a \sqcup b) \sqcap a$ (nach den Absorptionsregeln)

$$\begin{aligned} a \sqcup (b \sqcap c) &= (a \sqcup (a \sqcap c)) \sqcap (b \sqcap c) && \text{Absorption oben links} \\ &= a \sqcup ((a \sqcap c) \sqcap (b \sqcap c)) && \text{Assoziativität} \\ &= a \sqcup ((a \sqcup b) \sqcap c) && \text{erste Distributivitätsgleichung} \\ &= ((a \sqcup b) \sqcap a) \sqcup ((a \sqcup b) \sqcap c) && \text{Absorption oben rechts} \\ &= (a \sqcup b) \sqcap (a \sqcup c) && \text{erste Distributivitätsgleichung} \end{aligned}$$

Die andere Richtung „ \Leftarrow “ folgt analog (genauer: dual) zum Vorstehenden.

7.21 Kürzungsregel in distributiven Verbänden

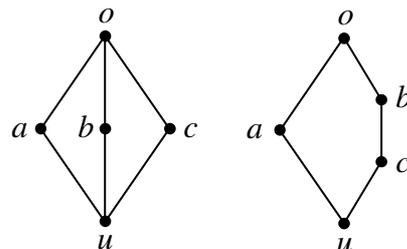
- a) Mit den Prämissen (P1, P2) der Kürzungsregel und unter Verwendung der Absorption (A), der Kommutativität (K), und der Distributivität (D) sehen wir:

$$a \stackrel{A}{=} a \sqcap (a \sqcup x) \stackrel{K}{=} a \sqcap (x \sqcup a) \stackrel{P1}{=} a \sqcap (x \sqcup b) \stackrel{D}{=} (a \sqcap x) \sqcup (a \sqcap b)$$

$$\stackrel{K}{=} (x \sqcap a) \sqcup (a \sqcap b) \stackrel{P2}{=} (x \sqcap b) \sqcup (a \sqcap b) \stackrel{D}{=} (x \sqcup a) \sqcap b \stackrel{P1}{=} (x \sqcup b) \sqcap b \stackrel{A,K}{=} b$$

- b) Wir verwenden die logische Kontraposition und zeigen, dass in nichtdistributiven Verbänden die Kürzungsregel verletzt ist. Ist V nicht distributiv, so existiert nach Satz 7.20 ein Unterverband einer der beiden

Formen rechts unten. In beiden (und damit in V) gilt $a \sqcap b = a \sqcap c (= u)$ und $a \sqcup b = a \sqcup c (= o)$, aber $b \neq c$. Die Kürzungsregel gilt hier also *nicht*.



7.22 Verbandshülle

- a) Ein Durchschnitt einer nichtleeren Menge von Unterverbänden eines Verbandes V ist selbst ein Unterverband von V , denn Assoziativität, Kommutativität und Absorption übertragen sich unmittelbar von den entsprechenden Eigenschaften in V .

Die Menge der X_0 enthaltenden Unterverbände von V enthält zumindest V , ist also nicht leer. Also ist

$$[X_0] := \bigcap \{U \mid X_0 \subseteq U, U \text{ Unterverband von } V\}$$

ein Verband und enthält alle Elemente von X_0 . Da er selbst unter den genannten U vorkommt, ist er selbst der kleinste dieser X_0 umfassenden Unterverbände, denn der Durchschnitt einer Mengenfamilie ist Teilmenge jeder einzelnen der geschnittenen Mengen.

- b) Die induktiv definierte Menge $\bigcup_{i=0,1,\dots} X_i$

- enthält X_0 , denn $X_0 \subseteq X_0 \cup \bigcup_{i=1,2,\dots} X_i = \bigcup_{i=0,1,\dots} X_i$
- ist Unterverband von V , denn Assoziativität, Kommutativität und Absorption übertragen sich unmittelbar von den entsprechenden Eigenschaften in V , und, wie man induktiv sofort beweist, ist sie abgeschlossen gegenüber den Verbandsoperationen:

Die Folge der X_i ist aufsteigend, $X_i \subseteq X_{i+1}$, so dass $X_i \cup X_k \subseteq X_{\max(i,k)}$

gilt. Sind $x, y \in \bigcup_{i=0,1,\dots} X_i$, dann gibt es i mit $x \in X_i$ und k mit $y \in X_k$,

und dann gilt $x \sqcap y, x \sqcup y \subseteq X_{\max(i,k)+1} \subseteq \bigcup_{i=0,1,\dots} X_i$.

- ist also Obermenge von $[X_0]$,
- muss aber auch Teilmenge von $[X_0]$ sein, da, wie man wiederum induktiv zeigt, für alle X_0 umfassenden Verbände U und alle $i \geq 0$ gilt: $X_i \subseteq U$:
 $X_0 \subseteq U$, und $X_i \subseteq U \Rightarrow X_{i+1} \subseteq U$, da jedes Element von $X_{i+1} \setminus X_i$ inf (\sqcap) oder sup (\sqcup) zweier Elemente von X_i , also auch von U , ist.

7.23 Lineare (Un-)Abhängigkeit

a) $1 \cdot (\mathbf{u} + \mathbf{v}) + (-1) \cdot (\mathbf{v} - \mathbf{w}) + (-1) \cdot (\mathbf{w} + \mathbf{u}) = \mathbf{u} + \mathbf{v} - \mathbf{v} + \mathbf{w} - \mathbf{w} - \mathbf{u} = \mathbf{0}$

b) $x(\mathbf{u} + \mathbf{v}) + y(\mathbf{v} + \mathbf{w}) + z(\mathbf{w} + \mathbf{u}) = \mathbf{0} \Rightarrow (x+z)\mathbf{u} + (x+y)\mathbf{v} + (y+z)\mathbf{w} = \mathbf{0}$

lineare Unabhängigkeit: \Rightarrow (i) $x+z=0$, (ii) $x+y=0$, (iii) $y+z=0$

(i)+(ii)-(iii), dann mal 1/2: $\Rightarrow x=0$

eingesetzt in (i) bzw. (ii): $\Rightarrow z=0, y=0$

... also $\{\mathbf{u} + \mathbf{v}, \mathbf{v} + \mathbf{w}, \mathbf{w} + \mathbf{u}\}$ linear unabhängig.

[Anders, mit mehr Handwerkszeug, aber nicht unbedingt schneller: Die lineare Abbildung A auf $[\{\mathbf{u}, \mathbf{v}, \mathbf{w}\}]$ mit $A(\mathbf{u}) := \mathbf{u} + \mathbf{v}$, $A(\mathbf{v}) := \mathbf{v} + \mathbf{w}$, $A(\mathbf{w}) := \mathbf{w} + \mathbf{u}$ (wieso gibt es

genau eine?) hat bezüglich der Basis $\{\mathbf{u}, \mathbf{v}, \mathbf{w}\}$ die Matrix $\begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$ mit der Determinante 1 und Rang 3, bildet also eine Basis auf eine Basis ab.]

7.24 Lineare (Un-)Abhängigkeit

Wegen Satz 7.21 und da $x^2 - 2x + 1$ eine Linearkombination von x^2 , x und 1 ist (oder direkt wegen $1 \cdot (x^2 - 2x + 1) - 1 \cdot x^2 + 2 \cdot x - 1 \cdot 1 = 0$), sind die vier Funktionen zusammen linear abhängig.

x^2 , x und 1 sind linear unabhängig, denn gibt es reelle Zahlen a , b und c derart, dass für alle reellen x $ax^2 + bx + c = 0$ gilt, so folgt daraus

mit $x = 0$: $c = 0$, also generell $ax^2 + bx = 0$, dann

mit $x = 1$: (i) $a + b = 0$ und

mit $x = -1$: (ii) $a - b = 0$, also auch

(i+ii)/2: $a = 0$ und

(i-ii)/2: $b = 0$.

[Nun kann man jeweils ähnlich die lineare Unabhängigkeit der drei anderen Dreierkombinationen zeigen, oder aber etwas allgemeiner so:]

Wäre $x^2 - 2x + 1$ zusammen mit zwei der drei Funktionen x^2 , x und 1 linear abhängig (#), so hätte man folgenden Fall:

Ein Vektor \mathbf{v}_4 ist „echte“ Linearkombination dreier anderer linear unabhängiger Vektoren $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ im reellen Vektorraum V ,

$$\mathbf{v}_4 = a_1 \mathbf{v}_1 + a_2 \mathbf{v}_2 + a_3 \mathbf{v}_3 \quad \text{mit} \quad a_1 \neq 0, a_2 \neq 0, a_3 \neq 0,$$

sowie wegen (#)

$$a_1 \mathbf{v}_1 + a_2 \mathbf{v}_2 + a_4 \mathbf{v}_4 = 0.$$

Und dieser Fall kann nie eintreten! – Warum? –:

Dann wäre $a_4 \neq 0$, denn sonst gälte $a_1 \mathbf{v}_1 + a_2 \mathbf{v}_2 = 0$, also wegen linearer Unabhängigkeit der beiden auch $a_1 = a_2 = 0$. Nun könnten wir durch a_4 dividieren und weiter schließen:

$$\frac{-a_1}{a_4} \mathbf{v}_1 + \frac{-a_2}{a_4} \mathbf{v}_2 = \mathbf{v}_4 = a_1 \mathbf{v}_1 + a_2 \mathbf{v}_2 + a_3 \mathbf{v}_3, \text{ so dass}$$

$$a_1(1 + 1/a_4) \mathbf{v}_1 + a_2(1 + 1/a_4) \mathbf{v}_2 + a_3 \mathbf{v}_3 = 0.$$

Lineare Unabhängigkeit der $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ ergäbe dann

$$a_1(1 + 1/a_4) = a_2(1 + 1/a_4) = a_3 = 0, \text{ im Widerspruch zu } a_3 \neq 0.$$

7.25 Lineare (Un-)Abhängigkeit

[Wir rechnen hier mit dem Zehnerlogarithmus. Es ginge auch mit anderen Basen.]

Zu Prüfung der linearen Unabhängigkeit gehen wir aus von 0 als Linearkombination von n Primzahllogarithmen, also

$$\sum_{i=1}^n \frac{a_i}{b_i} \cdot \log p_i = 0$$

mit n Primzahlen $p_i, 1 \leq i \leq n$, und n rationalen Zahlen, $a_i/b_i, 1 \leq i \leq n$, wobei alle $b_i \in \mathbb{N}$ und alle $a_i \in \mathbb{Z}$ sind.

Multipliziert mit dem kleinsten gemeinsamen Nenner der Brüche, $\text{kgV}\{b_1, \dots, b_n\}$, ergibt sich

$\sum_{i=1}^n c_i \cdot \log p_i = 0$ mit $c_i \in \mathbb{Z}$. Wir potenzieren 10 mit beiden Seiten: $\prod_{i=1}^n p_i^{c_i} = 1$. Wegen der Größe der absoluten Beträge müssen alle Faktoren 1, also alle c_i und damit alle $a_i/b_i, 1 \leq i \leq n$, null sein, insgesamt also die Primzahllogarithmen linear unabhängig.

7.26 Unendlichdimensionale Räume

- a) i) die Menge der Folgen f_i mit einer Eins an der i -ten Stelle und sonst nur Nullen, d.h. mit $(f_i)_k := \delta_{ik}$
- ii) die beiden Folgen f_u mit Einsen an den ungeraden und Nullen an den geraden Stellen bzw. f_g umgekehrt: $f_u := (1,0,1,0,1,\dots)$ und $f_g := (0,1,0,1,0,\dots)$
- b) i) $A: (a_1, a_2, a_3, a_4, \dots) \mapsto (a_2, a_3, a_4, a_5, \dots)$
- ii) $B: (a_1, a_2, a_3, a_4, \dots) \mapsto (0, a_1, a_2, a_3, \dots)$

Matrizen:

(i)
$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & \dots \\ 0 & 0 & 1 & 0 & 0 & \dots \\ 0 & 0 & 0 & 1 & 0 & \dots \\ 0 & 0 & 0 & 0 & 1 & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}, \text{ also } a_{ik} = \delta_{i+1,k}$$

(ii)
$$\begin{pmatrix} 0 & 0 & 0 & 0 & \dots \\ 1 & 0 & 0 & 0 & \dots \\ 0 & 1 & 0 & 0 & \dots \\ 0 & 0 & 1 & 0 & \dots \\ 0 & 0 & 0 & 1 & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}, \text{ also } a_{ik} = \delta_{i,k+1}$$

7.27 Geometrische Anwendung der reellen Zahlen als rationaler Vektorraum

Annahme (#): Eines der Quadrate hat eine irrationale Seitenlänge s .

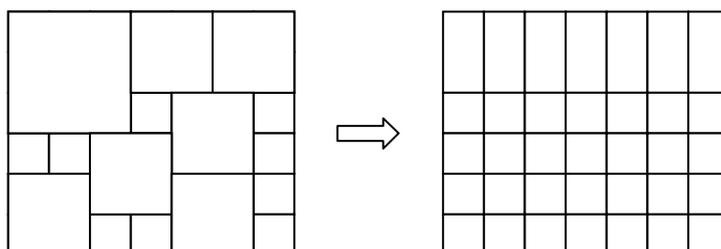
Da keine der Zahlen 1 und s ein rationales Vielfaches der anderen ist, sind die beiden im Vektorraum \mathbb{R} über dem Körper \mathbb{Q} linear unabhängig. Man kann laut Basisergänzungssatz $\{1, s\}$ zu einer Basis B von \mathbb{R} ergänzen. Jede reelle Zahl $\mathbf{r} \in \mathbb{R}$ ist dann eindeutige Linearkombination $\mathbf{r} = \sum_{i=1}^{n_{\mathbf{r}}} q_i \mathbf{b}_i$ mit einer von \mathbf{r} abhängigen Summandenzahl $n_{\mathbf{r}}$, endlich vielen Basisvektoren $\mathbf{b}_i \in B$ und rationalen Koeffizienten $q_i \neq 0$ für $i = 1, \dots, n_{\mathbf{r}}$. Infolgedessen ist

$$f: \begin{cases} \mathbb{R} & \rightarrow \mathbb{R} \\ \mathbf{r} & \mapsto \begin{cases} q_j & \text{wenn } \mathbf{b}_j = s \\ 0 & \text{wenn } s \notin \{\mathbf{b}_1, \dots, \mathbf{b}_{n_{\mathbf{r}}}\} \end{cases} \end{cases}$$

ein linearer Endomorphismus auf \mathbb{R} ist, der s auf 1 und alle anderen Basisvektoren in B auf 0 abbildet, also insbesondere $f(s) = 1, f(1) = 0$ erfüllt.

Jetzt sei auf den Rechtecken $r_{a \times b}$ mit Kantenlängen a und b definiert: $g(r_{a \times b}) := f(a) \cdot f(b)$. Man beachte, dass $g(r_{a \times b}) \geq 0$.

Wird ein großes Rechteck r (seitenparallel) in kleinere Rechtecke r_1, r_2, \dots, r_n zerschnitten, so kann man sich alle Schnitte als über das ganze r verlängert ausgeführt denken, wie in der folgenden Abbildung, so dass man durch erst waagrechte dann senkrechte Additionen erhält, dass $g(r) = \sum_{i=1}^n g(r_i)$.



Sind nun speziell q das Einheitsquadrat und q_1, q_2, \dots, q_n die Teilquadrate, jeweils q_i mit Seitenlänge s_i , darunter q_1 das mit Seitenlänge $s_1 = s$ aus (#), dann gilt

$$0 = f(1)^2 = g(q) = \sum_{i=1}^n g(q_i) \geq g(q_1) = f(s)^2 = 1,$$

was nicht sein kann. Also ist die Annahme (#) falsch.

7.28 Aufgespannte Untervektorräume

$\text{span}(M)$ bzw. $[M]$ ist die lineare Hülle von M , die Menge aller Linearkombinationen von Vektoren aus M . Und enthält wegen $\mathbf{v} = 1 \cdot \mathbf{v}$ natürlich alle Vektoren aus M .

a) Wir zeigen:

- (i) $[M]$ ist ein Untervektorraum von V , und
- (ii) jeder Untervektorraum U von V , der M umfasst, umfasst auch $[M]$.

Offensichtlich gilt (ii), da U als Untervektorraum jede Linearkombination seiner Vektoren enthält. Nun zu (i):

Im Folgenden seien alle $a_{ik} \in K$, alle $\mathbf{v}_{ik} \in M$ und alle $n_i \in \mathbb{N}$. Wir betrachten m Elemente von $[M]$, also Linearkombinationen

$$\sum_{k=1}^{n_1} a_{1k} \mathbf{v}_{1k}, \sum_{k=1}^{n_2} a_{2k} \mathbf{v}_{2k}, \dots, \sum_{k=1}^{n_m} a_{mk} \mathbf{v}_{mk}.$$

Diese denken wir uns jeweils derart umgeschrieben, dass in jeder der Summen die nicht vorkommenden \mathbf{v}_{ik} in Form von $0 \cdot \mathbf{v}_{ik}$ hinzu addiert werden („mit Nullvektoren aufgefüttert“), ohne dass sich der Wert der Summe ändert, so dass danach in jeder Summe alle \mathbf{v}_{ik} vorkommen. Diese \mathbf{v}_{ik} können wir nun als $\mathbf{v}_k, k=1, \dots, l$ linear aufzählen und die $[M]$ -Vektoren als Linearkombinationen $\mathbf{u}_j = \sum_{k=1}^l b_{jk} \mathbf{v}_k, j=1, \dots, m$, darstellen. Für eine Linearkombination $\sum_{j=1}^m c_{ij} \mathbf{u}_j$ dieser $[M]$ -Vektoren, gilt aber wegen der Rechengesetze in Körpern und Vektorräumen (insbesondere Distributivität(en) und Kommutativität(en))

$$\sum_{j=1}^m c_{ij} \mathbf{u}_j = \sum_{j=1}^m c_{ij} \left(\sum_{k=1}^l b_{jk} \mathbf{v}_k \right) = \sum_{k=1}^l \left(\sum_{j=1}^m c_{ij} b_{jk} \right) \mathbf{v}_k,$$

d.h. sie ist Element von $[M]$.

b) Wir zeigen:

- (i) $U_1 + U_2 \subseteq [U_1 \cup U_2]$,
- (ii) $[U_1 \cup U_2] \subseteq U_1 + U_2$.

(i) ... ist klar, da $\mathbf{u}_1 + \mathbf{u}_2$ mit $\mathbf{u}_i \in U_i$ eine Linearkombination $1 \cdot \mathbf{u}_1 + 1 \cdot \mathbf{u}_2$ von Vektoren aus $U_1 \cup U_2$ ist.

(ii): Wegen der Kommutativität der Vektoraddition können wir jedes $\mathbf{u} \in [U_1 \cup U_2]$, d.h. Linearkombination von Vektoren aus $U_1 \cup U_2$, aufspalten in den Anteil mit U_1 - und den mit U_2 - Vektoren:

$$\mathbf{u} = \sum_{i=1}^m a_i \mathbf{v}_i + \sum_{i=1}^n b_i \mathbf{w}_i \quad \text{mit } \mathbf{v}_i \in U_1, \mathbf{w}_i \in U_2; a_i, b_i \in K.$$

Wegen der Unterraumeigenschaft der U_i ist aber die linke Summe aus U_1 und die rechte aus U_2 , also $\mathbf{u} \in U_1 + U_2$.

7.29 Spann und Schnitt mehrerer Untervektorräume

Zunächst gehen wir der angedeuteten Frage nach einer *Verbandsstruktur* nach: In der Tat ist \subseteq eine Halbordnung auf der Menge der Untervektorräume eines Vektorraums V über einem Körper K , und diese bilden nach Abschnitt 3.6.4 einen Verband, da – wie inzwischen gezeigt – darin $U_1 + U_2$ das Supremum und $U_1 \cap U_2$ das Infimum zweier Unterräume U_1 und U_2 ist. Also fragt (a) nach der *Modularität* und (b/c) nach den *Distributivitätseigenschaften* dieses Verbandes.

a) Es gelte im Rest von (a) (#) $U_1 \subseteq U_3$.

Wir zeigen links \subseteq rechts:

Ist $u_{13} \in U_1$ (also wegen (#) auch $u_{13} \in U_3$) und $u_{23} \in U_2 \cap U_3$, (also $u_{23} \in U_2$ und $u_{23} \in U_3$), so gilt [Merkregel: $u_{ik} \in U_i, U_k$]

- $u_{13} + u_{23} \in U_1 + U_2$ per Definition von $U_1 + U_2$ und
- $u_{13} + u_{23} \in U_3 + U_3 = U_3$, da U_3 Untervektorraum.

Wir zeigen rechts \subseteq links:

Gilt $u_{13} \in U_1$ (also wegen (#) auch wieder $u_{13} \in U_3$), $u_2 \in U_2$ und $u_{13} + u_2 \in U_3$, so gibt es ein $u_3 \in U_3$ mit $u_{13} + u_2 = u_3$, also auch $u_2 = u_3 - u_{13} \in U_3$, so dass $u_2 \in U_2 \cap U_3$ und schließlich $u_{13} + u_2 \in U_1 + (U_2 \cap U_3)$.

b) Die Gleichung gilt nicht:

[Es gilt zwar links \subseteq rechts:

Ist $u_1 \in U_1$ und $u_{23} \in U_2 \cap U_3$ (also $u_{23} \in U_2$ und $u_{23} \in U_3$), so gilt $u_1 + u_{23} \in U_1 + U_2, U_1 + U_3$, also $u_1 + u_{23} \in (U_1 + U_2) \cap (U_1 + U_3)$; das funktioniert analog mit \square, \sqcup, \leq in jeder Verbandsordnung.]

Es gilt aber *nicht* rechts \subseteq links:

Sind im $V = \mathbb{R}^3$ (über dem Körper \mathbb{R} und geschrieben mit Zeilenvektoren) $U_1 = [(1,0,0)]$, $U_2 = [(0,1,0), (0,0,1)]$ und $U_3 = [(1,1,0), (0,0,1)]$, so ist $(U_1 + U_2) \cap (U_1 + U_3) = V$ und $U_1 + (U_2 \cap U_3) = [(1,0,0), (0,0,1)]$, und z.B. $(0,1,0) \in (U_1 + U_2) \cap (U_1 + U_3) \setminus U_1 + (U_2 \cap U_3)$.

c) Die Gleichung gilt nicht:

[Es gilt zwar rechts \subseteq links:

Ist $u_{12} \in U_1 \cap U_2$ und $u_{13} \in U_1 \cap U_3$, so gilt $u_{12} + u_{13} \in U_1$, da U_1 Untervektorraum, und $u_{12} + u_{13} \in U_2 + U_3$ wegen +; das funktioniert mit analog mit \square, \sqcup, \leq in jeder Verbandsordnung.]

Es gilt aber *nicht* links \subseteq rechts:

Sind im \mathbb{R}^2 (über dem Körper \mathbb{R} und geschrieben mit Zeilenvektoren) $U_1 = [(1,1)]$, $U_2 = [(1,0)]$ und $U_3 = [(0,1)]$, so gilt $U_1 \cap (U_2 + U_3) = U_1 \cap \mathbb{R}^2 = U_1$ aber $(U_1 \cap U_2) + (U_1 \cap U_3) = \{(0,0)\} + \{(0,0)\} = \{(0,0)\}$.

7.30 Untervektorräume von Folgenräumen

Natürlich ist der Raum aller reellen Folgen mit der gliedweisen Addition bzw. Skalarmultiplikation als spezieller Raum von Abbildungen (Beispiel in 7.4.1) ein reeller Vektorraum. Zu zeigen ist jeweils, dass die angegebene Folgenmenge abgeschlossen unter Addition und unter Skalarmultiplikation ist, denn dann ist sie ein Untervektorraum.

- a) Seien (a_n) und (b_n) Nullfolgen, $r \in \mathbb{R} \setminus \{0\}$ und $\varepsilon > 0$. Dann existieren n_a, n_b derart, dass $\forall i \geq n_a |a_i| < \varepsilon/2$ und $\forall i \geq n_b |b_i| < \varepsilon/2$, also
- $$\forall i \geq \max(n_a, n_b) |a_i + b_i| \leq |a_i| + |b_i| < \varepsilon.$$

Ferner existiert n_r derart, dass $\forall i \geq n_r |a_i| < \varepsilon/|r|$, also

$$\forall i \geq n_a |r \cdot a_i| = |r| \cdot |a_i| < \varepsilon,$$

und für $r = 0$ ist ohnehin $(r \cdot a_n) = 0, 0, 0, \dots$, also Nullfolge.

Also sind $(a_n) + (b_n) = (a_n + b_n)$ und $(r \cdot a_n)$ Nullfolgen.

- b) Seien (a_n) und (b_n) konvergent gegen a bzw. b , $r \in \mathbb{R} \setminus \{0\}$ und $\varepsilon > 0$. Dann existieren n_a, n_b derart, dass

$$\forall i \geq n_a |a_i - a| < \varepsilon/2 \text{ und } \forall i \geq n_b |b_i - b| < \varepsilon/2, \text{ also}$$

$$\forall i \geq \max(n_a, n_b) |(a_i + b_i) - (a + b)| \leq |a_i - a| + |b_i - b| < \varepsilon.$$

Ferner existiert n_r derart, dass $\forall i \geq n_r |a_i| < \varepsilon/|r|$, also

$$\forall i \geq n_a |r \cdot a_i - r \cdot a| = |r| \cdot |a_i - a| < \varepsilon,$$

und für $r = 0$ ist ohnehin $(r \cdot a_n) = 0, 0, 0, \dots$, also konvergente Folge.

Also sind $(a_n) + (b_n) = (a_n + b_n)$ und $(r \cdot a_n)$ konvergente Folgen.

- c) Seien (a_n) und (b_n) beschränkt durch $|a_n| < a$ bzw. $|b_n| < b$, $r \in \mathbb{R}$. Dann gilt

$$\forall n |a_n + b_n| \leq |a_n| + |b_n| \leq a + b \quad \text{und}$$

$$\forall n |r \cdot a_n| = |r| \cdot |a_n| \leq r a$$

Also sind $(a_n) + (b_n) = (a_n + b_n)$ und $(r \cdot a_n)$ beschränkte Folgen.

- d) Seien (a_n) und (b_n) beschränkt durch $|a_n| \leq r_a \cdot n^{s_a}$ und $|b_n| < r_b \cdot n^{s_b}$, $r \in \mathbb{R}$. Dann gilt mit $q := r_a + r_b$, $s := \max(s_a, s_b)$:

$$\forall n |a_n + b_n| \leq |a_n| + |b_n| \leq r_a \cdot n^{s_a} + r_b \cdot n^{s_b} \leq q \cdot n^s$$

$$\forall n |r \cdot a_n| = |r| \cdot |a_n| \leq (r \cdot r_a) \cdot n^{s_a}$$

Also sind $(a_n) + (b_n) = (a_n + b_n)$ und $(r \cdot a_n)$ höchstens polynomial wachsend.

7.31 Lineare Abbildung aus der Analysis

- a) Zwecks Identifikation als Unterraum aller reellen Funktionen ist zu zeigen: Eine Summe zweier solchen Polynome bzw. ein skalares Vielfaches eines solchen Polynoms ist ebenfalls ein reelles Polynom zweiten Grades. Und dies sieht man leicht:

$$(a_1x^2 + b_1x + c_1) + (a_2x^2 + b_2x + c_2) = (a_1 + a_2)x^2 + (b_1 + b_2)x + (c_1 + c_2)$$

$$r \cdot (a_1x^2 + b_1x + c_1) = (r \cdot a_1)x^2 + (r \cdot b_1)x + (r \cdot c_1)$$

- b) Erinnerung: Wenn man die Vektoren als Spaltenvektoren darstellt, also $ax^2 + bx + c$ als $(c \ b \ a)^T$, dann liefert das Bild des i -ten Einheitsvektors die i -te Spalte der Abbildungsmatrix. Also liefern unten die Differenzierungsregeln links die Matrix rechts:

$$f' = 0, \quad x' = 1, \quad (x^2)' = 2x \quad \Longrightarrow \quad \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix}$$

7.32 Lineare Abbildungen

- a) Nach den Sätzen über Spaltenrang und Zeilenrang und Dimension ist der Spaltenrang einer Matrix gleich dem Zeilenrang.

Die Zeilen $a_{1\bullet}$ und $a_{2\bullet}$ von A (beispielsweise) sind linear unabhängig, denn aus $\lambda \cdot a_{1\bullet} + \mu \cdot a_{2\bullet} = (0,0,0)$ folgt wegen der ersten Komponenten $\lambda = 0$ und wegen der dritten Komponenten $\mu = 0$. Die dritte Zeile ist eine Linearkombination der ersten beiden: $2 \cdot a_{1\bullet} + 2 \cdot a_{2\bullet} = a_{3\bullet}$. Also ist $\text{rang}(A) = 2$.

Die Spalten von B sind linear unabhängig, denn aus $\lambda \cdot b_{\bullet 1} + \mu \cdot b_{\bullet 2} = (0,0,0)^T$ folgt wegen der zweiten Komponenten $\mu = 0$ und wegen der dritten Komponenten $\lambda = 0$. Also ist $\text{rang}(B) = 2$.

- b) Wir lösen $Ax = \mathbf{0}$:

$$\begin{array}{cccc|c} 1 & -1 & 0 & 1 & 0 & (1) \\ 0 & 1 & -1 & -1 & 0 & (2) \end{array}$$

[Die dritte Gleichung ist eine Linearkombination der beiden und daher redundant, d.h. Sie können sie mit benutzen, aber sie ändert nichts an den Ergebnissen.]

Nach der Wahl zweier Parameter $x_3 := s, x_4 := t$ liefert (2) $x_2 = s + t$ und dann (1)

$x_1 = x_2 - x_4 = s + t - t = s$, also

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = s \cdot \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix} + t \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \text{ bzw. } \ker(A) = \left[\begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} \right] \text{ mit der Basis } = \left\{ \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} \right\}.$$

$\ker(B)$ ergibt sich ähnlich. Eine schnellere Alternative bietet der Dimensionssatz der linearen Abbildungen:

$$\text{def}(B) = \dim(\mathbb{R}^2) - \text{rang}(B) = 2 - 2 = 0, \text{ also}$$

$$\ker(B) = \{\mathbf{0}\} \text{ mit der Basis } \emptyset.$$

[Vgl. 7.4.2: eine „leere Linearkombination“ mit 0 Summanden ergibt $\mathbf{0}$.]

- c) Bei der Multiplikation „Matrix mal Vektor, Ax “ wird $\sum x_i a_{\bullet i}$ berechnet. Daher besteht die Bildmenge aus allen Linearkombinationen der Matrixspalten, und jede maximale linear unabhängige Teilmenge dieser Spalten ist eine Basis des Bildraums. Diese Teilmenge enthält $\text{rang}(A)$ Vektoren.

Wegen der Nullkomponenten sind je zwei beliebigen Spalten von A bzw. B linear unabhängig, und wegen des bereits bekannten Ranges 2 bilden sie eine Basis des Bildraumes, z.B.

$$\text{bei } A: \left\{ \begin{pmatrix} 1 \\ 0 \\ 2 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix} \right\} \quad \text{bei } B: \left\{ \begin{pmatrix} 1 \\ 0 \\ 2 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix} \right\}$$

7.33 Hintereinander ausgeführte lineare Abbildungen

Additivität:	Multiplikativität:	Begründungen:
$(A \circ B)(\mathbf{v} + \mathbf{w}) = A(B(\mathbf{v} + \mathbf{w}))$	$(A \circ B)(k\mathbf{v}) = A(B(k\mathbf{v}))$	Definition von \circ
$= A(B(\mathbf{v}) + B(\mathbf{w}))$	$= A(kB(\mathbf{v}))$	Linearität von B
$= A(B(\mathbf{v})) + A(B(\mathbf{w}))$	$= kA(B(\mathbf{v}))$	Linearität von A
$= (A \circ B)(\mathbf{v}) + (A \circ B)(\mathbf{w})$	$= k(A \circ B)(\mathbf{v})$	Definition von \circ

7.34 Matrixprodukte

- a) Wir berechnen das Beispiel (a) ausführlich: In der 2×2 -Ergebnismatrix steht links oben (auf der Position (1,1)) das Ergebnis von (1. Spalte linke Matrix) \cdot (1. Spalte rechte Matrix), bzw. allgemein auf der Position (i,k) das Ergebnis von $(i.$ Zeile linke Matrix) \cdot $(k.$ Spalte rechte Matrix). Die Produktmatrix (oder das Matrixprodukt) ist also:

$$\begin{pmatrix} (1 \ -1 \ 2) \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix} & (1 \ -1 \ 2) \begin{pmatrix} -1 \\ 1 \\ 1 \end{pmatrix} \\ (-1 \ 0 \ 1) \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix} & (-1 \ 0 \ 1) \begin{pmatrix} -1 \\ 1 \\ 1 \end{pmatrix} \end{pmatrix}, \text{ bzw.}$$

$$\begin{pmatrix} 1 \cdot 1 + (-1) \cdot 1 + 2 \cdot (-1) & 1 \cdot (-1) + (-1) \cdot 1 + 2 \cdot 1 \\ (-1) \cdot 1 + 0 \cdot 1 + 1 \cdot (-1) & (-1) \cdot (-1) + 0 \cdot 1 + 1 \cdot 1 \end{pmatrix}, \text{ bzw. } \begin{pmatrix} -2 & 0 \\ -2 & 2 \end{pmatrix}.$$

(b) und (e) erfüllen nicht die notwendige Voraussetzung, dass die vordere Matrix so viele Spalten hat wie die hintere Zeilen.

- c) $\begin{pmatrix} 2 & -1 & 1 \\ 0 & -1 & 3 \\ -2 & 1 & -1 \end{pmatrix}$ f) $\begin{pmatrix} 1 & -1 & 1 \\ 2 & -2 & 2 \\ 3 & -3 & 3 \end{pmatrix} \leftarrow$ Die Spalten von links und Zeilen von rechts sind jeweils einsteilig; ihr Produkt ergibt sich einfach als Zahl \cdot Zahl, und dies 3×3 - also neunmal.

7.35 Matrixpotenzen

- a) Nach der Berechnung von $A^2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ a & 0 & 1 \end{pmatrix}$ vermuten wir, dass $A^n = A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ a & 0 & 1 \end{pmatrix}$ für

alle $n \in \mathbb{N}$ gilt. Gewissheit verschaffen wir uns durch vollständige Induktion:

1. Es gilt für $n = 1$, denn $A^1 := A$.
2. Wenn es für eine natürliche Zahl n gilt, dann folgt daraus:
 $A^{n+1} := A \cdot A^n = A^2 = A$, also die Gültigkeit für $n + 1$.
3. Also gilt es für alle $n \in \mathbb{N}$.

Ergebnis: $A^{100} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ a & 0 & 1 \end{pmatrix}$

- b) Nach der Berechnung von $B^2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & b^2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ vermuten wir, dass $B^n = \begin{pmatrix} 1 & 0 & 0 \\ 0 & b^n & 0 \\ 0 & 0 & 1 \end{pmatrix}$ für

alle $n \in \mathbb{N}$ gilt. Das beweisen wir wie oben durch vollständige Induktion.

Ergebnis: $B^{100} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & b^{100} & 0 \\ 0 & 0 & 1 \end{pmatrix}$

c) Wir berechnen

$$C^2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$

$$C^3 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

und erhalten $C^{100} = C^{99} \cdot C = (C^3)^{33} \cdot C = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} = C.$

d) Wir berechnen

$$D^2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & d \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & d \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & d \\ d & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$

$$D^3 = \begin{pmatrix} 0 & 0 & d \\ d & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & d \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} d & 0 & 0 \\ 0 & d & 0 \\ 0 & 0 & d \end{pmatrix} = d \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

und erhalten

$$D^{100} = D^{99} \cdot D = (D^3)^{33} \cdot D = \begin{pmatrix} d^{33} & 0 & 0 \\ 0 & d^{33} & 0 \\ 0 & 0 & d^{33} \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & d \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & d^{33} & 0 \\ 0 & 0 & d^{34} \\ d^{33} & 0 & 0 \end{pmatrix}$$

7.36 Produkte von Dreiecksmatrizen

- a) Das Produkt zweier Diagonalmatrizen AB ist auch eine Diagonalmatrix, denn dann treffen bei den Produkten „ $(AB)_{ik}$ = Zeile $a_{i\bullet}$ mal Spalte $b_{\bullet k}$ “ nur dann zwei von 0 verschiedene Faktoren aufeinander, wenn $i = k$.
- b) Das Produkt zweier oberer Dreiecksmatrizen AB ist auch eine Diagonalmatrix, denn dann treffen bei den Produkten „ $(AB)_{ik}$ = Zeile $a_{i\bullet}$ mal Spalte $b_{\bullet k}$ “ nur dann zwei von 0 verschiedene Faktoren aufeinander, wenn $i \leq k$.
- c) keine besondere (im Sinne von Diagonal- oder Dreiecks-):

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

- d) Transponieren macht aus oberen Dreiecksmatrizen untere und umgekehrt; Diagonalmatrizen (auf der Hauptdiagonalen) bleiben dabei unverändert. Es gilt $A^T B^T = (BA)^T$. Hätte AB eine dieser besonderen Formen, müsste bereits die Matrix BA eine haben – hat sie aber nicht.

7.37 Vektorkoordinaten, Basistransformation

Die Gleichung $\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = x \cdot \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix} + y \cdot \begin{pmatrix} 0 \\ 2 \\ 1 \end{pmatrix} + z \cdot \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix}$ entspricht

dem linearen Gleichungssystem
$$\begin{aligned} x + 3z &= 1 \\ 2x - 2y + 2z &= 1 \\ y + z &= 1 \end{aligned}$$

Wir lösen es – z.B. ähnlich wie beim Gauß'schen Verfahren (Normierung hier eingespart):

$$\begin{array}{lcl} 1 & 0 & 3 \mid 1 & (1) \\ 2 & -2 & 2 \mid 1 & (2) \\ 0 & 1 & 1 \mid 1 & (3) \\ \hline 0 & 2 & 4 \mid 1 & (4) := 2 \cdot (1) - (2) \\ 0 & 0 & 2 \mid -1 & (5) := (4) - 2 \cdot (3) \end{array}$$

Rückrechnung mit (5), (3), (1) ergibt:

$$z = -1/2, \quad y = 1 - z = 3/2, \quad x = 1 - 3z = 5/2, \quad \text{also} \quad \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = \frac{5}{2} \cdot \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix} + \frac{3}{2} \cdot \begin{pmatrix} 0 \\ 2 \\ 1 \end{pmatrix} - \frac{1}{2} \cdot \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix}.$$

7.38 Basisergänzung und Basistransformation

- a) Da ja auch die dritten und vierten Komponenten der von einer Basis zu erzeugenden Vektoren „irgendwoher“ kommen müssen, versuchen wir es mit dem dritten und vierten der angebotenen Vektoren, also insgesamt mit

$$\mathbf{b}_1 = \begin{pmatrix} 1 \\ 2 \\ 0 \\ 0 \end{pmatrix}, \quad \mathbf{b}_2 = \begin{pmatrix} 2 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad \mathbf{b}_3 = \begin{pmatrix} 1 \\ 0 \\ -1 \\ 0 \end{pmatrix}, \quad \mathbf{b}_4 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix}.$$

0 als Linearkombination $x_1 \mathbf{b}_1 + x_2 \mathbf{b}_2 + x_3 \mathbf{b}_3 + x_4 \mathbf{b}_4$ der \mathbf{b}_i , also

$$x_1 \begin{pmatrix} 1 \\ 2 \\ 0 \\ 0 \end{pmatrix} + x_2 \begin{pmatrix} 2 \\ 1 \\ 0 \\ 0 \end{pmatrix} + x_3 \begin{pmatrix} 1 \\ 0 \\ -1 \\ 0 \end{pmatrix} + x_4 \begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix},$$

entspricht dem Gleichungssystem $x_1 + 2x_2 + x_3 + x_4 = 0$ usw. – in Kurznotation:

$$\begin{array}{lcl} 1 & 2 & 1 & 1 \mid 0 & (1) \\ 2 & 1 & 0 & 0 \mid 0 & (2) \\ 0 & 0 & -1 & 0 \mid 0 & (3) \\ 0 & 0 & 0 & -1 \mid 0 & (4) . \end{array}$$

Rückrechnung mit (4), (3) ergibt: $x_4 = 0, x_3 = 0$. Eingesetzt in (1) und (2):

$$\begin{array}{lcl} 1 & 2 & \mid 0 & (1') \\ 2 & 1 & \mid 0 & (2') \end{array}$$

$2 \cdot (1') - (2')$ ergibt $x_1 = 0$, und eingesetzt in (2') folgt $x_2 = 0$. Also sind die vier Vektoren linear unabhängig.

Nach dem Basisergänzungssatz können wir die vier um b weitere Vektoren ergänzen zu einer Basis B des Raumes \mathbb{R}^4 , der aber auch mit $E_4 = \{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \mathbf{e}_4\}$ eine Basis aus

vier Vektoren hat. Nach dem Dimensionssatz muss B ebenfalls aus vier Vektoren bestehen. Also war $b = 0$, und $\{\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \mathbf{b}_4\}$ bildet bereits selbst eine Basis.

b) (Bitte Korrektur des Aufgabentextes beachten!)

Gesucht: t_{ik} derart, dass $\mathbf{e}_k = \sum_{i=1}^4 t_{ik} \mathbf{b}_i = t_{1k} \mathbf{b}_1 + t_{2k} \mathbf{b}_2 + t_{3k} \mathbf{b}_3 + t_{4k} \mathbf{b}_4$. Für $k = 1, 2, 3, 4$ ist dies jeweils ein Gleichungssystem

$$t_{1k} \begin{pmatrix} 1 \\ 2 \\ 0 \\ 0 \end{pmatrix} + t_{2k} \begin{pmatrix} 2 \\ 1 \\ 0 \\ 0 \end{pmatrix} + t_{3k} \begin{pmatrix} 1 \\ 0 \\ -1 \\ 0 \end{pmatrix} + t_{4k} \begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \text{ bzw. } = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \text{ kurz:}$$

$$\begin{array}{cccc|cccc} 1 & 2 & 1 & 1 & 1 & 0 & 0 & 0 & (1) \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & (2) \\ 0 & 0 & -1 & 0 & 0 & 0 & 1 & 0 & (3) \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 & (4) \end{array}$$

Die vier Gleichungssysteme für die jeweils vier Koeffizienten in $s_{\bullet k}$ unterscheiden sich nur in den rechten Seiten; ihr Lösungsweg ist aber durch die linken Seiten bestimmt. Daher können wir die vier Gleichungssysteme simultan lösen, z.B. hier durch ein erweitertes Gauß'schen Verfahren mit (a) vier rechten Seiten gleichzeitig und (b) einer anschließenden Überführung der Dreiecksmatrix in eine Diagonalmatrix. [Es werden zuerst von links nach rechts unter der Hauptdiagonalen Nullen erzeugt, anschließend von rechts nach links oberhalb der Hauptdiagonalen.]:

$$\begin{array}{cccc|cccc} 1 & 2 & 1 & 1 & 1 & 0 & 0 & 0 & (1a) = (1) \\ 0 & 1 & 1 & 1 & 1 & -1 & 0 & 0 & (2a) = (1) - (2) \\ 0 & 0 & -1 & 0 & 0 & 0 & 1 & 0 & (3a) = (3) \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 & (4a) = (4) \\ \hline 1 & 2 & 1 & 1 & 1 & 0 & 0 & 0 & (1b) = (1a) \\ 0 & 1 & 1 & 1 & 1 & -1 & 0 & 0 & (2b) = (1a) - (2a) \\ 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & (3b) = -(3a) \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & (4b) = -(4a) \\ \hline 1 & 2 & 1 & 0 & 1 & 0 & 0 & 1 & (1c) = (1b) - (4b) \\ 0 & 1 & 1 & 0 & 1 & -1 & 0 & 1 & (2c) = (2b) - (4b) \\ 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & (3c) = (3b) \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & (4c) = (4b) \\ \hline 1 & 2 & 0 & 0 & 1 & 0 & 1 & 1 & (1d) = (1c) - (3c) \\ 0 & 1 & 0 & 0 & 1 & -1 & 1 & 1 & (2d) = (2c) - (3c) \\ 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & (3d) = (3c) \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & (4d) = (4c) \\ \hline 1 & 0 & 0 & 0 & -1 & 2 & -1 & -1 & (1e) = (1d) - 2(2d) \\ 0 & 1 & 0 & 0 & 1 & -1 & 1 & 1 & (2e) = (2d) \\ 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 & (3e) = (3d) \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & (4e) = (4d) \end{array}$$

Die Koeffizienten in $\mathbf{e}_k = t_{1k} \mathbf{b}_1 + t_{2k} \mathbf{b}_2 + t_{3k} \mathbf{b}_3 + t_{4k} \mathbf{b}_4$ sind die Komponenten von $t_{\bullet k}$, der k -ten Spalte der rechten Matrix im letzten Block, so dass

$$(t_{ik}) = \begin{pmatrix} -1 & 2 & -1 & -1 \\ 1 & -1 & 1 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \text{ und letztlich: } \begin{array}{l} \mathbf{e}_1 = -\mathbf{b}_1 + \mathbf{b}_2 \\ \mathbf{e}_2 = 2\mathbf{b}_1 - \mathbf{b}_2 \\ \mathbf{e}_3 = -\mathbf{b}_1 + \mathbf{b}_2 - \mathbf{b}_3 \\ \mathbf{e}_4 = -\mathbf{b}_1 + \mathbf{b}_2 - \mathbf{b}_4 \end{array}$$

- c) Die einfacher zu erlangende Matrix ist die der Transformation (s_{ik}) von E_4 nach B , woraus wir dann die Matrix (u_{ik}) der Basistransformation von B nach E_4 durch Inversion $(u_{ik}) = (s_{ik})^{-1}$ erhalten (Satz 7.40). Von (s_{ik}) wissen wir: $\mathbf{b}_k = \sum_{i=1}^4 s_{ik} \mathbf{e}_i$, d.h. der k -te Spaltenvektor der Basis B bildet die k -te Spalte $s_{\bullet k}$ von ...

$$(s_{ik}) = \begin{pmatrix} 1 & 2 & 1 & 1 \\ 2 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

Wie in Abschnitt 7.4.5 erläutert, führen wir zur Inversion ein erweitertes Gauß'sches Verfahren mit (a) vier rechten Seiten gleichzeitig und (b) einer anschließenden Überführung der Dreiecksmatrix in eine Diagonalmatrix durch. Das haben wir aber mit (s_{ik}) auf der ersten linken Seite ja bereits in (b) durchgeführt:

$$(u_{ik}) = (t_{ik}) = \begin{pmatrix} -1 & 2 & -1 & -1 \\ 1 & -1 & 1 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

- d) Man kann an Abb. 7.7 ablesen, und $(A\mathbf{e}_j)_i = \sum_{k=1}^4 a_{ik} (\mathbf{e}_j)_k = \sum_{k=1}^4 a_{ik} \delta_{jk} = a_{ij} = (a_{\bullet j})_i$ zeigt: Die Matrix von A bezüglich $E_4 = \{\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3, \mathbf{e}_4\}$ als Basis im Definitions- und Zielraum hat als Spalten die Bilder der Basisvektoren, lautet also

$$(a_{ik}) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Nach Satz 7.41 ist die Matrix (a'_{ik}) von A bezüglich B im Def.- und Zielraum

$$(a'_{ik}) = (s_{ik})(a_{ik})(t_{ik}) = \begin{pmatrix} 1 & 2 & 1 & 1 \\ 2 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} -1 & 2 & -1 & -1 \\ 1 & -1 & 1 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix},$$

errechnet sich also zu

$$\begin{pmatrix} 1 & 2 & 1 & 1 \\ 2 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & -1 \\ -1 & 2 & -1 & -1 \\ 1 & -1 & 1 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 3 & -2 & -2 \\ -1 & 2 & -1 & -3 \\ -1 & 1 & -1 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

7.39 Matrixgleichungen

a) Ist $(x_{ik}) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ die gesuchte Matrix (liest sich leichter), so ist

$(x_{ik})^2 = \begin{pmatrix} aa+bc & ba+bd \\ ac+cd & bc+dd \end{pmatrix}$, so dass wir folgendes Gleichungssystem lösen wollen:

$$aa+bc = 1 \quad (1)$$

$$ba+bd = 2 \quad (2)$$

$$ac+cd = 0 \quad (3)$$

$$bc+dd = 1 \quad (4)$$

Aus (3) folgt: $a = -d$ oder $c = 0$. Im Falle $a = -d$ gälte aber nach (2): $0 = 2$ – der Fall scheidet also aus, d.h. $c = 0$. Mit (1) folgt dann $a^2 = 1$, also $a = 1$ oder $a = -1$, und mit (4) $d^2 = 1$, also $d = 1$ oder $d = -1$. Wegen (2) muss $a \neq -d$ sein; also bleibt
 $a = d = 1$ (und wegen (2) $b = 1$) oder
 $a = d = -1$ (und wegen (2) $b = -1$).

Entweder prüfen wir nun, ob das Gleichungssystem bzw. $(x_{ik})^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ in beiden

Fällen erfüllt ist (ja, ist es), oder wir stellen fest, dass aus $(x_{ik})^2 = A$ auch

$(-x_{ik})^2 = ((-1)(x_{ik}))^2 = (x_{ik})^2 = A$ folgt und prüfen nur einen der beiden Fälle.

$(x_{ik})^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ hat also die Lösungen $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ und $\begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}$.

b) Die Matrixgleichung entspricht der Gleichungssystemen für die drei Spalten $x_{\bullet k}$ der gesuchten Matrix (x_{ik}) – alle mit den gleichen Koeffizienten, aber jeweils mit anderer rechter Seite, der k -ten Spalte der rechten Matrix. Wir können daher mit den drei rechten Seiten gleichzeitig operieren, wenn wir die linke Seite in normierte Stufenform (schattiert) bringen:

$$\begin{array}{ccc|ccc} 1 & 1 & 0 & 2 & -1 & 1 & (1) \end{array}$$

$$\begin{array}{ccc|ccc} 0 & 1 & 1 & 1 & 0 & 1 & (2) \end{array}$$

$$\begin{array}{ccc|ccc} 1 & 0 & 1 & 1 & 1 & 2 & (3) \end{array}$$

$$\begin{array}{ccc|ccc} 0 & 1 & -1 & 1 & -2 & -1 & (4) = (1) - (3) \end{array}$$

$$\begin{array}{ccc|ccc} 0 & 0 & 2 & 0 & 2 & 2 & (3a) = (2) - (4) \end{array}$$

$$\begin{array}{ccc|ccc} 0 & 0 & 1 & 0 & 1 & 1 & (3b) = (3a) / 2 \end{array}$$

Rückrechnung für $x_{\bullet k}$ aus der normierten Staffelform, also aus (3b), (2) und (1), mit der k -ten rechten Seite – und die lautet $(2 \ 1 \ 0)^T$ für $k = 1$, $(-1 \ 0 \ 1)^T$ für $k = 2$, $(1 \ 1 \ 1)^T$ für $k = 3$ – ergibt für ...

$$k = 1: x_{31} = 0, \quad x_{21} = 1 - x_{31} = 1, \quad x_{11} = 2 - x_{21} = 1;$$

$$k = 2: x_{32} = 1, \quad x_{22} = 0 - x_{32} = -1, \quad x_{12} = -1 - x_{22} = 0;$$

$$k = 3: x_{33} = 1, \quad x_{23} = 1 - x_{33} = 0, \quad x_{13} = 1 - x_{23} = 1.$$

$$(x_{ik}) = \begin{pmatrix} 1 & 0 & 1 \\ 1 & -1 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$

- c) Die Seiten der Matrixgleichung können wir transponieren, müssen dabei aber die beiden multiplizierten Matrizen nicht nur transponieren, sondern auch vertauschen. Bezeichnen wir die Transponierte von (x_{ik}) als (y_{ik}) , können wir dann analog zu (b) vorgehen und erhalten Gleichungssysteme für die drei Spalten $y_{\bullet k}$ der gesuchten Matrix (y_{ik}) – alle mit den gleichen Koeffizienten, aber jeweils mit anderer rechter Seite, der k -ten Spalte der rechten Matrix. Wir können daher wieder mit den drei rechten Seiten gleichzeitig operieren, wenn wir die linke Seite in normierte Stufenform (schat- tiert) bringen:

$$\begin{array}{l} \begin{array}{ccc|ccc} 1 & 0 & 1 & 2 & 1 & 1 \end{array} & (1) \\ \begin{array}{ccc|ccc} 1 & 1 & 0 & -1 & 0 & 1 \end{array} & (2) \\ \begin{array}{ccc|ccc} 0 & 1 & 1 & 1 & 1 & 2 \end{array} & (3) \\ \begin{array}{ccc|ccc} 0 & -1 & 1 & 3 & 1 & 0 \end{array} & (4) = (1) - (2) \\ \begin{array}{ccc|ccc} 0 & 0 & 2 & 4 & 2 & 2 \end{array} & (3a) = (3) + (4) \\ \begin{array}{ccc|ccc} 0 & 0 & 1 & 2 & 1 & 1 \end{array} & (3b) = (3a) / 2 \end{array}$$

Rückrechnung für $y_{\bullet k}$ aus der normierten Staffelform, also aus (3b), (3) und (1), mit der k -ten rechten Seite – und die lautet $(2 \ 1 \ 2)^T$ für $k=1$, $(1 \ 1 \ 1)^T$ für $k=2$, $(1 \ 2 \ 1)^T$ für $k=3$ – ergibt für ...

$$\begin{array}{l} k=1: \quad y_{31} = 2, \quad y_{21} = 1 - y_{31} = -1, \quad y_{11} = 2 - y_{31} = 0; \\ k=2: \quad y_{32} = 1, \quad y_{22} = 1 - y_{32} = 0, \quad y_{12} = 1 - y_{32} = 0; \\ k=3: \quad y_{33} = 1, \quad y_{23} = 2 - y_{33} = 1, \quad y_{13} = 1 - y_{33} = 0. \end{array}$$

$$(y_{ik}) = \begin{pmatrix} 0 & 0 & 0 \\ -1 & 0 & 1 \\ 2 & 1 & 1 \end{pmatrix}, \quad (x_{ik}) = \begin{pmatrix} 0 & -1 & 2 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

7.40 Matrix-Rang

Da keine Zeile Vielfaches einer anderen ist, also keine 2 zusammen bereits linear abhängigen Zeilen existieren, ist jede von ihnen eine Linearkombination der anderen beiden. Wir können z.B. ansetzen: Zeile 1 = $x \cdot$ Zeile 2 + $y \cdot$ Zeile 3, spaltenweise interpretiert also:

$$\begin{array}{l} x + y = 2 \quad (1) \\ y = -1 \quad (2) \\ x + 2y = 1 \quad (3) \end{array},$$

wobei natürlich eine (beliebige) Gleichung entbehrlich ist, aber auch nicht schadet. Aus (2) folgt $y = -1$, und mit (1) folgt $x = 2 - y = 3$, d.h.

$$(2 \ -1 \ 1) = 3 \cdot (1 \ 0 \ 1) - (1 \ 1 \ 2).$$

7.41 Gleichungssysteme

- a) $(1) + (2) \Rightarrow x_2 = 1$; eingesetzt in (1) oder (2) $\Rightarrow x_1 = -1$.
b) Überführung in normierte Staffelform:

$$\begin{array}{l} \begin{array}{ccc|c} 1 & 2 & 1 & 1 \end{array} & (1) \\ \begin{array}{ccc|c} -1 & 1 & 2 & 2 \end{array} & (2) \\ \hline \begin{array}{ccc|c} 0 & 3 & 3 & 3 \end{array} & (3) = (1) + (2) \\ \begin{array}{ccc|c} 0 & 1 & 1 & 1 \end{array} & (4) = (3) / 3 \end{array}$$

Rückrechnung: (4) mit $x_3 := t \in \mathbb{R}$ als Parameter liefert $x_2 = 1 - t$, eingesetzt in (1):
 $x_1 = 1 - 2x_2 - x_3 = t - 2$.

Die Lösungsmenge ist beschrieben durch $x_1 = t - 2, x_2 = 1 - t, x_3 = t, t \in \mathbb{R}$.

[bzw. $\{ (t - 2, 1 - t, t) \mid t \in \mathbb{R} \}$]

7.42 Gleichungssysteme

[Die $m \times n$ -Koeffizientenmatrix (a_{ik}) , eines Gleichungssystems $Ax = y$ ist in normierter Stufenform, wenn in jeder Zeile (von links gezählt) die erste von 0 verschiedene Komponente den Wert 1 hat und unter ihr in der Matrix nur Nullen stehen. Die separate rechte Seite, die abgetrennte $(n+1)$ -te Spalte (b_i) mit m Komponenten, unterliegt keiner solchen Einschränkung.]

1. \langle Numerische Erfassung der Form der Matrix \rangle
Zeilenzahl m , Spaltenzahl n , spezielle Spaltenindizes k_i und höchster interessierender Zeilenindex max sind wie folgt definiert:
Die in der $m \times n$ -Koeffizientenmatrix (a_{ik}) in ihrer jeweiligen Zeile führenden Einsen stehen an Stellen a_{ik_i} in den Zeilen $i = 1$ bis max .
 \langle Daher gilt $max \leq m$, $k_{i+1} > k_i$, und eventuellen (a_{ik}) -Zeilen mit Nummern $i > max$ bestehen nur aus Nullen. \rangle
2. Gibt es ein $i > max$ mit $y_i \neq 0$, so schreibe „Die Lösungsmenge ist leer.“, und die Berechnung endet.
 \langle Denn dann ergibt die linke Seite der i . Gleichung 0, die rechte nicht – ein Widerspruch. \rangle
3. \langle Es gibt also kein $i > max$ mit $y_i \neq 0$. Dann rechnen wir ab der Zeile $i := max$, der untersten Nicht-0-Zeile, zurück. Die „letzte Bezugsspalte“ wird fiktiv auf $n+1$ gesetzt. \rangle
Schreibe: „Lösungsmenge ist die Menge aller Wertekombinationen x_1, x_2, \dots, x_n , $n =$ “; Schreibe n ; Schreibe: „mit “;
 $i := max$; $l := n+1$;
4. \langle Die $x_k, k_i < k < l$, werden im Weiteren als Parameter verwendet. \rangle
Für $x_k, k = k_i + 1, \dots, l-1$ schreibe „ $x_k \in \mathbb{R}$, “ (k spezifiziert).
5. Berechne x_{k_i} aus der $x_{k_i} := b_i - \sum_{k=k_i+1}^n a_{ik} x_k$ (erhalten aus Zeile i des Gleichungssystems) Zeile als Linearkombination von 1 und den bisherigen Parametern,
$$x_{k_i} = c_i + \sum_{\substack{k=k_i+1 \\ P(k)}}^n d_{ik} x_k, \quad (\text{Gl. } k_i \text{ neu})$$
wobei $P(k)$ bedeutet: k ist keines der k_i . Dies geschieht, indem die x_{k_i} mit höherem i durch die rechte Seite ihrer jeweiligen (Gl. k_i neu) ersetzt werden.
6. Schreibe die Gleichung (Gl. k_i neu) mit „konkreten Werten“ sowohl für k_i als auch für die Produkte auf der rechten Seite; Schreibe „ , “
7. Falls $i = 1$:
 - Schreibe für alle $k_i - 1 \geq k \geq 2$, „ $x_k \in \mathbb{R}$, “ (k spezifiziert);
 - Falls $k_i \geq 2$: Schreibe „ $x_1 \in \mathbb{R}$ “;
 - Schreibe „ } “;
 - Die Berechnung endet.
8. \langle Noch ist $i > 1$ \rangle
 $l := k_i$; $i := i - 1$; mache weiter bei (4).

Test mit einem konkreten Gleichungssystem:

$$\begin{array}{cccc|c} 0 & 1 & -1 & 2 & 1 & | & 1 \\ 0 & 0 & 0 & 1 & -1 & | & 2 \\ 0 & 0 & 0 & 0 & 0 & | & 0 \end{array}$$

Schritt	Wirkung (u.a. Textausgabe) + ggf. <Kommentar>
1:	$m = 3, n = 5, k_1 = 2, k_2 = 4, \max = 2$
2 -, 3:	Lösungsmenge ist die Menge aller Wertekombinationen $x_1, x_2, \dots, x_n, n = 5$ mit $i = 2$ (daher z.Z. auch $k_i = 4$), $l = 6$
4:	<k wird durchlaufen von $k_i + 1 = 5$ bis $l - 1 = 5$.> $x_5 \in \mathbb{R}$,
5:	$x_4 = 2 + x_5$
6:	$x_4 = 2 + x_5$,
7 -, 8:	$l = 4, i = 1$ (daher z.Z. auch $k_i = 2$)
4:	<k wird durchlaufen von $k_i + 1 = 3$ bis $l - 1 = 3$.> $x_3 \in \mathbb{R}$,
5:	$x_2 = 1 + x_3 - 2x_4 - x_5 = 1 + x_3 - 2 \cdot (2 + x_5) - x_5 = -3 + x_3 - 3x_5$
6:	$x_2 = -3 + x_3 - 3x_5$,
7:	$x_1 \in \mathbb{R}$ }

Prüfung, dass die berechnete Lösungsmenge wirklich *nur* Lösungen enthält.

$$0x_1 + x_2 - x_3 + 2x_4 + x_5 = -3 + x_3 - 3x_5 - x_3 + 4 + 2x_5 + x_5 = 1 \quad \text{OK}$$

$$0x_1 + 0x_2 + 0x_3 + x_4 - x_5 = 2 + x_5 - x_5 = 2 \quad \text{OK}$$

Dies beweist aber nicht, dass die Menge *alle* Lösungen umfasst.

7.43 Wirtschaftsmathematik (Bitte korrigierte Aufgabenstellung beachten!)

Die Anzahlen der 1-, 2-, 5-DM-Münzen können wir anschaulich x_1, x_2, x_5 nennen, wobei wir x_5 als 3. Komponente des Lösungsvektors behandeln. Die Aufgabenstellung liefert je eine lineare Gleichung bezüglich Anzahl, Gewicht, und Wert:

$$x_1 + x_2 + x_5 = 30$$

$$5x_1 + 7x_2 + 10x_5 = 200$$

$$x_1 + 2x_2 + 5x_5 = 61$$

Wir bringen das System (frei nach Gauß) in Staffelform

$$\begin{array}{ccc|c} 1 & 1 & 1 & | & 30 & (1) \end{array}$$

$$\begin{array}{ccc|c} 5 & 7 & 10 & | & 200 & (2) \end{array}$$

$$\begin{array}{ccc|c} 1 & 2 & 5 & | & 61 & (3) \end{array}$$

$$\begin{array}{ccc|c} 0 & 1 & 4 & | & 31 & (2a) := (3) - (1) \end{array}$$

$$\begin{array}{ccc|c} 0 & 2 & 5 & | & 50 & (3a) := (2) - 5(1) \end{array}$$

$$\begin{array}{ccc|c} 0 & 0 & 3 & | & 12 & (3b) := 2(2a) - (3a) \end{array}$$

$$\begin{array}{ccc|c} 0 & 0 & 1 & | & 4 & (3c) := (3b) / 3 \end{array}$$

und rechnen zurück: $x_5 = 4, x_2 = 31 - 4 \cdot 4 = 15, x_1 = 30 - 15 - 4 = 11$.

7.44 Matrizenvektorräume

Wenn (a_{ik}) und (b_{ik}) magische Quadrate mit Zeilen-, Spalten- und Diagonalsumme a bzw. b sind und r ist eine reelle Zahl, so gilt für die Zeilensummen von $(a_{ik} + b_{ik})$

$$(a_{i1} + b_{i1}) + (a_{i2} + b_{i2}) + (a_{i3} + b_{i3}) = (a_{i1} + a_{i2} + a_{i3}) + (b_{i1} + b_{i2} + b_{i3}) = a + b$$

und für die Spaltensummen:

$$(a_{1k} + b_{1k}) + (a_{2k} + b_{2k}) + (a_{3k} + b_{3k}) = (a_{1k} + a_{2k} + a_{3k}) + (b_{1k} + b_{2k} + b_{3k}) = a + b$$

und für die Hauptdiagonale:

$$(a_{11} + b_{11}) + (a_{22} + b_{22}) + (a_{33} + b_{33}) = (a_{11} + a_{22} + a_{33}) + (b_{11} + b_{22} + b_{33}) = a + b$$

und für die Nebendiagonale:

$$(a_{31} + b_{31}) + (a_{22} + b_{22}) + (a_{13} + b_{13}) = (a_{31} + a_{22} + a_{13}) + (b_{13} + b_{22} + b_{31}) = a + b.$$

Ähnlich folgt für die Zeilen-, Spalten- und Diagonalsummen von $r(a_{ik})$, dass sie alle $r \cdot a$ ergeben:

$$r \cdot a_{i1} + r \cdot a_{i2} + r \cdot a_{i3} = r \cdot (a_{i1} + a_{i2} + a_{i3}) = r \cdot a$$

$$r \cdot a_{1k} + r \cdot a_{2k} + r \cdot a_{3k} = r \cdot (a_{1k} + a_{2k} + a_{3k}) = r \cdot a$$

$$r \cdot a_{11} + r \cdot a_{22} + r \cdot a_{33} = r \cdot (a_{11} + a_{22} + a_{33}) = r \cdot a$$

$$r \cdot a_{31} + r \cdot a_{22} + r \cdot a_{13} = r \cdot (a_{31} + a_{22} + a_{13}) = r \cdot a$$

Das sind also auch magische Quadrate. Damit erfüllen die magischen Quadrate das Kriterium für Untervektorräume, dass Summen und skalare Vielfache von Vektoren aus ihnen auch darin liegen.

Die jeweils 8 identischen Summen (für 3 Zeilen, 3 Spalten, 2 Diagonalen) eines magischen Quadrats liefern per Vergleich mit der Summe der ersten Zeile 7 Gleichungen:

$$a_{11} + a_{12} + a_{13} - a_{21} - a_{22} - a_{23} = 0$$

$$a_{11} + a_{12} + a_{13} - a_{31} - a_{32} - a_{33} = 0$$

$$a_{11} + a_{12} + a_{13} - a_{11} - a_{12} - a_{13} = 0$$

$$a_{11} + a_{12} + a_{13} - a_{21} - a_{22} - a_{23} = 0$$

$$a_{11} + a_{12} + a_{13} - a_{31} - a_{32} - a_{33} = 0$$

$$a_{11} + a_{12} + a_{13} - a_{11} - a_{22} - a_{33} = 0$$

$$a_{11} + a_{12} + a_{13} - a_{31} - a_{22} - a_{13} = 0$$

Betrachten wir die Matrixkomponenten a_{ik} zeilenweise als Unbekannte $x_{3(i-1)+k}$ von x_1 bis x_9 aufgezählt, so erhalten wir die Koeffizientenmatrix des Gleichungssystems für diese Unbekannten, die wir dann lösen:

$$\begin{array}{l}
1 \ 1 \ 1 \ -1 \ -1 \ -1 \ 0 \ 0 \ 0 \ | \ 0 \quad (1) \\
1 \ 1 \ 1 \ 0 \ 0 \ 0 \ -1 \ -1 \ -1 \ | \ 0 \quad (2) \\
0 \ 1 \ 1 \ -1 \ 0 \ 0 \ -1 \ 0 \ 0 \ | \ 0 \quad (3) =: (3a) \\
1 \ 0 \ 1 \ 0 \ -1 \ 0 \ 0 \ -1 \ 0 \ | \ 0 \quad (4) \\
1 \ 1 \ 0 \ 0 \ 0 \ -1 \ 0 \ 0 \ -1 \ | \ 0 \quad (5) \\
0 \ 1 \ 1 \ 0 \ -1 \ 0 \ 0 \ 0 \ -1 \ | \ 0 \quad (6) =: (6a) \\
1 \ 1 \ 0 \ 0 \ -1 \ 0 \ -1 \ 0 \ 0 \ | \ 0 \quad (7) \\
\hline
0 \ 0 \ 0 \ 1 \ 1 \ 1 \ -1 \ -1 \ -1 \ | \ 0 \quad (2a) := (2) - (1) =: (2b) =: (2c) \\
0 \ -1 \ 0 \ 1 \ 0 \ 1 \ 0 \ -1 \ 0 \ | \ 0 \quad (4a) := (4) - (1) \\
0 \ 0 \ -1 \ 1 \ 1 \ 0 \ 0 \ 0 \ -1 \ | \ 0 \quad (5a) := (5) - (1) = (5b) \\
0 \ 0 \ -1 \ 1 \ 0 \ 1 \ -1 \ 0 \ 0 \ | \ 0 \quad (7a) := (7) - (1) = (7b) \\
\hline
0 \ 0 \ 1 \ 0 \ 0 \ 1 \ -1 \ -1 \ 0 \ | \ 0 \quad (4b) := (4a) + (3a) \\
0 \ 0 \ 0 \ 1 \ -1 \ 0 \ 1 \ 0 \ -1 \ | \ 0 \quad (6b) := (6a) - (3a) =: (6c) \\
\hline
0 \ 0 \ 0 \ 1 \ 1 \ 1 \ -1 \ -1 \ -1 \ | \ 0 \quad (5c) := (5b) + (4b) = (2c!) \\
0 \ 0 \ 0 \ 1 \ 0 \ 2 \ -2 \ -1 \ 0 \ | \ 0 \quad (7c) := (7b) + (4b) \\
\hline
0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ | \ 0 \quad (5d) := (2c) - (5c) \\
0 \ 0 \ 0 \ 0 \ -2 \ -1 \ 2 \ 1 \ 0 \ | \ 0 \quad (6d) := (6c) - (2c) \\
\hline
0 \ 0 \ 0 \ 0 \ 1 \ -1 \ 1 \ 0 \ -1 \ | \ 0 \quad (7d) := (2c) - (7c) \\
0 \ 0 \ 0 \ 0 \ 0 \ -3 \ 4 \ 1 \ -2 \ | \ 0 \quad (6e) := 2(7d) + (6d) \\
0 \ 0 \ 0 \ 0 \ 0 \ 1 \ -4/3 \ -1/3 \ 2/3 \ | \ 0 \quad (6e') := (6e) / (-3)
\end{array}$$

Rückrechnung:

$$\begin{array}{l}
(6e') \quad a_{23} = \frac{4}{3}a_{31} + \frac{1}{3}a_{32} - \frac{2}{3}a_{33}, \\
(7d) \quad a_{22} = a_{23} - a_{31} + a_{33}, \\
(2c) \quad a_{21} = -a_{22} - a_{23} + a_{13} + a_{23} + a_{33}, \\
(4b) \quad a_{13} = -a_{23} + a_{31} + a_{32}, \\
(3a) \quad a_{12} = -a_{13} + a_{21} + a_{31}, \\
(1) \quad a_{11} = -a_{12} - a_{13} + a_{21} + a_{22} + a_{23}
\end{array}$$

Mit $(x_7, x_8, x_9) = \dots$ (a) $(3,0,0)$, (b) $(0,3,0)$, (c) $(0,0,3)$ ergeben sich die Matrizen

$$\begin{pmatrix} 2 & 2 & -1 \\ -2 & 1 & 4 \\ 3 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 2 & -1 & 2 \\ 1 & 1 & 1 \\ 0 & 3 & 0 \end{pmatrix}, \quad \begin{pmatrix} -1 & 2 & 2 \\ 4 & 1 & -2 \\ 0 & 0 & 3 \end{pmatrix}.$$

Mithilfe der letzten Zeilen sieht man leicht, dass sie linear unabhängig sind. Durch Einsetzen in die Rückrechnungsgleichungen kann man zeigen, dass sich jede Lösung als Linearkombination der drei Matrizen darstellen lässt. Also bilden sie eine Basis des damit dreidimensionalen Vektorraums der reellwertigen magischen Quadrate.

[Es gibt „schönere“ Basen, in deren drei Matrizen alle Koeffizienten, 0, 1 oder -1 sind. Übungshalber könnte man jetzt noch ein klassisches magisches Quadrat aus den natürlichen Zahlen 1 bis 9 als Linearkombination der drei „Basismatrizen“ darstellen.]

7.45 Matrixinverse

a) Wir müssen die Rechenregeln (Addition, Multiplikation modulo 5) in \mathbb{Z}_5 beachten:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

i. Entweder wir entdecken, dass der Matrixrang nur 1 ist (z.B. wegen der Determinante 0 oder weil die zweite Zeile das 2-fache der ersten ist) und sie daher *nicht* invertiert werden kann, oder wir berechnen die Inverse nach Rezept, und die Berechnung bricht wegen Unlösbarkeit ab:

$$\begin{array}{l} 2 \quad 3 \quad | \quad 1 \quad 0 \quad (1) \\ 4 \quad 1 \quad | \quad 0 \quad 1 \quad (2) \\ \hline 1 \quad 4 \quad | \quad 3 \quad 0 \quad (1') = (1) / 2 = 3(1), \text{ denn } 2^{-1} = 3 \\ 0 \quad 0 \quad | \quad 2 \quad 1 \quad (2') = (2) - 4(1') \end{array}$$

Gleichung (2') mit der ersten rechten Seite impliziert $0 = 2$. Das Gleichungssystem ist also widersprüchlich.

ii. $\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} 4 & 3 \\ 3 & 4 \end{pmatrix}$, denn nach Rezept in Abschnitt 7.4.5, modifiziert:

$$\begin{array}{l} 2 \quad 1 \quad | \quad 1 \quad 0 \quad (1) \\ 1 \quad 2 \quad | \quad 0 \quad 1 \quad (2) \\ \hline 1 \quad 3 \quad | \quad 3 \quad 0 \quad (1') = (1) / 2 = 3(1), \text{ denn } 2^{-1} = 3 \\ 0 \quad 1 \quad | \quad 3 \quad 4 \quad (2') = (1') - (2) \\ 1 \quad 0 \quad | \quad 4 \quad 3 \quad (1'') = (1') - 3(2) \\ 0 \quad 1 \quad | \quad 3 \quad 4 \quad (2'') = (1') - (2) \end{array}$$

b) i. $\begin{pmatrix} 2 & 3 \\ 4 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} -0,1 & 0,3 \\ 0,4 & -0,2 \end{pmatrix}$, denn nach dem Rezept in Abschnitt 7.4.5, modif.:

$$\begin{array}{l} 2 \quad 3 \quad | \quad 1 \quad 0 \quad (1) \\ 4 \quad 1 \quad | \quad 0 \quad 1 \quad (2) \\ \hline 1 \quad 1,5 \quad | \quad 0,5 \quad 0 \quad (1') = (1) / 2 \\ 0 \quad -5 \quad | \quad -2 \quad 1 \quad (2') = (2) - 4(1') \\ 0 \quad 1 \quad | \quad 0,4 \quad -0,2 \quad (2'') = (2') / (-5) \\ 1 \quad 0 \quad | \quad -0,1 \quad 0,3 \quad (1'') = (1') - (3/2)(2'') \\ 0 \quad 1 \quad | \quad 0,4 \quad -0,2 \quad (2'') = (2') / (-5) \end{array}$$

ii. $\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} 2/3 & -1/3 \\ -1/3 & 2/3 \end{pmatrix}$, denn nach dem Rezept in Abschnitt 7.4.5, modif.

$$\begin{array}{l} 2 \quad 1 \quad | \quad 1 \quad 0 \quad (1) \\ 1 \quad 2 \quad | \quad 0 \quad 1 \quad (2) \\ \hline 0 \quad 3 \quad | \quad -1 \quad 2 \quad (1') = 2(2) - (1) \\ 0 \quad 1 \quad | \quad -1/3 \quad 2/3 \quad (1'') = (1') / 3 \\ 1 \quad 0 \quad | \quad 2/3 \quad -1/3 \quad (2'') = (2) - 2(1'') \\ 0 \quad 1 \quad | \quad 0,4 \quad -0,2 \quad (1''') \end{array}$$

- c) Entweder wir entdecken, dass der Matrixrang nur 1 ist (z.B. wegen der Determinante 0 oder weil die zweite Zeile das $(1/2 - i/2)$ -fache der ersten ist) und sie daher *nicht* invertiert werden kann, oder wir berechnen die Inverse nach Rezept, und die Berechnung bricht wegen Unlösbarkeit ab:

$$\begin{array}{ccc|cc} 1+i & 2 & | & 1 & 0 & (1) \\ 1 & 1-i & | & 0 & 1 & (2) \\ \hline 1 & 1-i & | & (1-i)/2 & 0 & (1') = (1) \times (1-i)/2 \\ 0 & 0 & | & -(1-i)/2 & 1 & (2') = (2) - (1') \end{array}$$

Gleichung (2') mit der ersten zweiten Seite (1) impliziert $0 = 1$. Das Gleichungssystem ist also widersprüchlich.

7.46 Mengensysteme als Vektorräume

- a) Lösungsidee: Im Beispiel 1 des Abschnitts 7.4.1 sahen wir, dass die Abbildungen einer Menge M in den Körper \mathbb{Z}_2 mit der punktweisen Addition und Skalarmultiplikation einen Vektorraum \mathbb{Z}_2^M bilden. Jeder Abbildung $f: M \rightarrow \mathbb{Z}_2$ entspricht genau eine Teilmenge $f^{-1}(\{1\})$ von M (der sog. **Träger** $\text{supp}(f)$ von f), und umgekehrt jedem $A \subseteq M$ mittels $f(x) := 1 \Leftrightarrow x \in A$ (0 sonst, die sog. **charakteristische Abbildung** χ_A von A) genau eine Abbildung von M in \mathbb{Z}_2 . Dabei entspricht wegen der Rechenregeln modulo 2 der Summe $f + g: M \rightarrow K$ zweier solcher Abbildungen als deren Trägermenge die symmetrischen Differenz der Trägermengen von f und g :

$$\begin{aligned} \text{supp}(f + g) &= \text{supp}(f) \Delta \text{supp}(g), \text{ weil} \\ (f + g)(x) = 1 &\Leftrightarrow (f(x) = 1 \wedge g(x) = 0) \vee (f(x) = 0 \wedge g(x) = 1) \\ &\Leftrightarrow x \in \text{supp}(f) \setminus \text{supp}(g) \vee x \in \text{supp}(g) \setminus \text{supp}(f) \\ &\Leftrightarrow x \in \text{supp}(f) \Delta \text{supp}(g) \end{aligned}$$

$$\chi_{A \Delta B} = \chi_A + \chi_B \text{ (ähnlich)}$$

Der $\mathbf{0}$ in \mathbb{Z}_2^M entspricht \emptyset in $\mathbf{P}(M)$, denn $\text{supp}(\mathbf{0}) = \emptyset$.

Auch die Skalarmultiplikationen entsprechen einander:

$$\begin{aligned} \text{supp}(0 \cdot f) &= \text{supp}(0\text{-Abbildung}) = \emptyset = 0 \cdot \text{supp}(f) \\ \text{supp}(1 \cdot f) &= \text{supp}(f) = 1 \cdot \text{supp}(f) \end{aligned}$$

Daher übertragen sich alle algebraischen Eigenschaften von \mathbb{Z}_2^M mit der punktweisen Addition und Skalarmultiplikation auf $\mathbf{P}(M)$ mit der symmetrischen Differenz Δ als Addition und der angegebenen Skalarmultiplikation. Insbesondere werden alle Vektorraumkriterien auch von $\mathbf{P}(M)$ erfüllt.

[Natürlich könnte man alle Kriterien auch „zu Fuß“ nachprüfen, was aber wahrscheinlich weniger Aha-Momente erzeugt.]

- b) Sind A und B endliche Teilmengen von M , dann auch $A + B (= A \Delta B)$ und sämtliche skalaren Vielfachen, $0 \cdot A (= \emptyset)$ und $1 \cdot A (= A)$. Das Standard-Untervektorraum-Kriterium ist erfüllt.

- c) Beispielsweise sind $\{\{1\}, \{2\}, \{3\}\}$ und $\{\{1,2\}, \{1,3\}, \{1,2,3\}\}$ zwei Basen, die keinen Basisvektor gemeinsam haben:

$\{\{1\}, \{2\}, \{3\}\}$ spannt $\mathbf{E}(\{1,2,3\})$ auf, denn für $i \neq k$ ist $\{i, k\} = \{i\} \Delta \{k\} = \{i\} + \{k\}$, und $\{1,2,3\} = \{1\} + \{2\} + \{3\}$. Diese drei Vektoren sind linear unabhängig, denn $x_1\{1\} + x_2\{2\} + x_3\{3\}$ ist die Menge derjenigen i mit $x_i = 1$ also $x_i \neq 0$, kann also nur dann $\mathbf{0}$, d.h. \emptyset , sein, wenn $x_i = 0$ für $i = 1, 2, 3$.

$\{\{1,2\}, \{1,3\}, \{1,2,3\}\}$ spannt ebenfalls $\mathbf{E}(\{1,2,3\})$ auf, da die vorigen Basisvektoren als Linearkombinationen darstellbar sind:

$\{1\} = \{1,2,3\} + \{2,3\} = \{1,2,3\} + (\{1,2\} + \{1,3\})$, $\{2\} = \{1,2,3\} + \{1,3\}$, $\{3\} = \{1,2,3\} + \{1,2\}$. Also müssen die drei Vektoren linear unabhängig sein – sonst wäre die Dimension von $\mathbf{E}(\{1,2,3\})$ kleiner als 3. Also ist $\{\{1,2\}, \{1,3\}, \{1,2,3\}\}$ ebenfalls Basis von $\mathbf{E}(\{1,2,3\})$.

- d) f_{\emptyset} erfüllt $f_{\emptyset}(0A) = f_{\emptyset}(\emptyset) = 0f_{\emptyset}(A)$ und $f_{\emptyset}(1A) = f_{\emptyset}(A) = 1f_{\emptyset}(A)$. Also ist f_{\emptyset} genau dann Homomorphismus (d.h. linear), wenn $f_{\emptyset}(A+B) = f_{\emptyset}(A) + f_{\emptyset}(B)$.

Ist f_{\emptyset} linear, so gilt für beliebige $a, b \in M$:

$$f(a) = f(b) \Rightarrow f_{\emptyset}(\{a\} + \{b\}) = f_{\emptyset}(\{a\}) + f_{\emptyset}(\{b\}) = \mathbf{0} = \emptyset,$$

Im Falle $f(a) = f(b)$ müssen also $f_{\emptyset}(\{a\} \Delta \{b\})$ und damit $\{a\} \Delta \{b\}$ und somit insbesondere $\{a\} \setminus \{b\}$ leer sein, was heißt: $a = b$. Ist also f_{\emptyset} linear, so ist f injektiv.

Nehmen wir nun umgekehrt für endliche $A, B \subseteq M$ an: $f_{\emptyset}(A+B) \neq f_{\emptyset}(A) + f_{\emptyset}(B)$.

Wegen $f_{\emptyset}(A) \Delta f_{\emptyset}(B) \subseteq f_{\emptyset}(A \Delta B)$, was man leicht nachprüft (s.u.: #), muss ein $y \in f_{\emptyset}(A \Delta B)$ existieren, das nicht in $f_{\emptyset}(A) \Delta f_{\emptyset}(B)$ liegt. Dann existiert ein $x \in A \Delta B$ mit $f(x) \notin f_{\emptyset}(A) \Delta f_{\emptyset}(B)$. Ist $x \in A \setminus B$, so muss es ein $x' \in B \setminus A$ geben, also $x' \neq x$, das „das $f(x)$ aus $f_{\emptyset}(A)$ auslöscht“, d.h. mit $f(x') = f(x)$.

Analoges folgt wenn $x \in B \setminus A$. Zusammengefasst gilt: Ist f_{\emptyset} nicht linear, so ist f nicht injektiv. Insgesamt gilt also: f injektiv $\Leftrightarrow f_{\emptyset}$ linear.

Nachtrag #:

$$\begin{aligned} z \in f_{\emptyset}(A) \Delta f_{\emptyset}(B) \\ \Rightarrow (\exists a \in A z = f(a) \wedge \neg \exists b \in B z = f(b)) \vee (\exists b \in B z = f(b) \wedge \neg \exists a \in A z = f(a)) \\ \Rightarrow \exists a \in A \setminus B z = f(a) \vee \exists b \in B \setminus A z = f(b) \\ \Rightarrow z \in f_{\emptyset}(A \Delta B) \end{aligned}$$

- e) Nach 7.4.4 gilt für die gesuchte 3×2 -Matrix (a_{ik}) : $g_{\emptyset}(\mathbf{b}_k) = \sum_{i=1}^3 a_{ik} \mathbf{c}_i$.

Nun ist $g_{\emptyset}(\mathbf{b}_1) = g_{\emptyset}(\{1\}) = \{a\} = \{a, b, c\} \Delta \{b, c\} = \{a, b, c\} \Delta (\{a, b\} \Delta \{a, c\}) = \mathbf{c}_1 + \mathbf{c}_2 + \mathbf{c}_3$ und $g_{\emptyset}(\mathbf{b}_2) = g_{\emptyset}(\{2\}) = \{b\} = \{a, b, c\} \Delta \{a, c\} = \mathbf{c}_2 + \mathbf{c}_3$, also

$$(a_{ik}) = \begin{pmatrix} 1 & 0 \\ 1 & 1 \\ 1 & 1 \end{pmatrix}.$$

- f) Mit Argumenten wie in (c) oben zeigt man leicht, dass die einelementigen Mengen $\{m\}$, $m \in M$, eine Basis von $\mathbf{E}(M)$ bilden.

Für jedes lineare Funktional $A: \mathbf{E}(M) \rightarrow \mathbb{Z}_2$ und jedes $N \in \mathbf{E}(M)$ ist dann

$$A(N) = \sum_{x \in N} A(\{x\}), \quad (\#)$$

so dass mit $M_A := \{y \in M \mid A(y) = 1\}$ für lineare Funktionale gilt: $A, B: \mathbf{E}(M) \rightarrow \mathbf{Z}_2$ und Skalare $k \in \mathbf{Z}_2$ gilt

$$M_{A+B} = M_A \Delta M_B = M_A + M_B, \quad M_{kA} = \begin{cases} \text{wenn } k=0: \emptyset \\ \text{wenn } k=1: M \end{cases} = k \cdot M_A.$$

Mit (#) zeigt man leicht, dass die Abbildung $A \mapsto M_A$ nicht nur, wie gerade gesehen linear, sondern auch bijektiv, also ein Vektorraumisomorphismus zwischen $\mathbf{E}(M)^*$ und $\mathbf{P}(M)$ über \mathbf{Z}_2 ist.

[Übrigens besagt $A(N)$, ob $|N \cap M_A|$ – eine natürliche Zahl – gerade (Ergebnis 0) oder ungerade (Ergebnis 1) ist.]

- g) Jeder Vektorraum hat eine Basis, und eine Basis von $\mathbf{P}(M)$ erlaubt, jede Teilmenge von M als Linearkombination der Basisvektoren darzustellen. Die Basisvektoren sind auch Teilmengen von M , und ihre Linearkombinationen sind endliche Δ -Ketten dieser „Basismengen“. Keine der Basismengen ist Linearkombination, d.h. endliche Δ -Kette, anderer Basismengen.

7.47 Determinantenberechnung

Seien $\mathbf{v}_k = a_{\bullet k}$ die Spalten der $n \times n$ -Matrix (a_{ik}) . Zu \mathbf{v}_{k_0} werde eine Linearkombination der anderen Zeilen addiert – ohne Beschränkung der Allgemeinheit eine Linearkombination *aller* anderen Zeilen, ggf. mit etlichen Nullen als Koeffizienten. Wegen der spaltenweisen Linearität gilt dann

$$\begin{aligned} & f(\mathbf{v}_1, \dots, \mathbf{v}_{k_0-1}, \mathbf{v}_{k_0} + \sum_{m \neq k_0} \lambda_m \mathbf{v}_m, \mathbf{v}_{k_0+1}, \dots, \mathbf{v}_n) \\ &= f(\mathbf{v}_1, \dots, \mathbf{v}_{k_0-1}, \mathbf{v}_{k_0}, \mathbf{v}_{k_0+1}, \dots, \mathbf{v}_n) + f(\mathbf{v}_1, \dots, \mathbf{v}_{k_0-1}, \sum_{m \neq k_0} \lambda_m \mathbf{v}_m, \mathbf{v}_{k_0+1}, \dots, \mathbf{v}_n) \\ &= f(a_{ik}) + \sum_{m \neq k_0} \lambda_m \cdot f(\mathbf{v}_1, \dots, \mathbf{v}_{k_0-1}, \mathbf{v}_m, \mathbf{v}_{k_0+1}, \dots, \mathbf{v}_n) \end{aligned}$$

Aber alle oben zu $f(a_{ik})$ addierten Summanden sind f -Bilder von Matrizen mit zwei identischen Spalten, haben also nach Satz 7.44 den Wert null.

7.48 Determinantenberechnung

- a) Wir entwickeln (vgl. Satz 7.43) zuerst nach der letzten Spalte, dann nach der ersten, da dies die Anzahl der Summanden klein hält; zuletzt verwenden wir die Sarrus-Regel mit den Diagonalen:

$$\begin{vmatrix} 1 & 0 & 1 & 0 \\ 0 & -1 & -1 & 0 \\ 0 & 1 & 2 & 0 \\ 1 & 0 & 0 & 1 \end{vmatrix} = 1 \cdot \begin{vmatrix} 1 & 0 & 1 \\ 0 & -1 & -1 \\ 0 & 1 & 2 \end{vmatrix} = 1 \cdot 1 \cdot \begin{vmatrix} -1 & -1 \\ 1 & 2 \end{vmatrix} = -2 - (-1) = -1$$

- b) Die zweite Zeile ist die Hälfte der Summe von Zeile 1 und Zeile 3, d.h. wir können diese Hälfte von Zeile 2 subtrahieren, ohne, dass sich die Determinante ändert. Wenn wir nach der entstehenden Nullzeile als neuer Zeile 2 entwickeln (Satz 7.43), ergibt sich das Ergebnis: 0.

7.49 Permutationsmatrizen

Die Permutationsmatrix können wir uns durch Permutation der Spalten aus der Einheitsmatrix erzeugen. Diese Permutation ist als Produkt einer Folge von Transpositionen, also Vertauschungen zweier Spalten, darstellbar [auf viele Arten, aber das schadet nicht]. Durch jede einzelne Transposition wird wegen des Alternierens (Satz 7.46) der Wert der Determinante der Matrix (ursprünglich 1) mit -1 multipliziert – insgesamt so oft, wie die Anzahl der Transpositionen in der Folge beträgt. Genauso ist aber das Vorzeichen der Permutation definiert.

7.50 Bilinearformen

Zunächst zeigt man leicht, dass $b: V \times W \rightarrow K$ genau dann Bilinearform ist, wenn für alle $\mathbf{v}_0 \in V$ die Zuordnung $\mathbf{w} \mapsto b(\mathbf{v}_0, \mathbf{w})$ ein lineares Funktional auf W und für alle $\mathbf{w}_0 \in W$ die Zuordnung $\mathbf{v} \mapsto b(\mathbf{v}, \mathbf{w}_0)$ ein lineares Funktional auf V ist. (#) Das bedeutet kurz gesagt Linearität im ersten und im zweiten Argument.

a) Da jeder Vektor aus V bzw. W Linearkombination der \mathbf{b}_i bzw. \mathbf{c}_k ist, definiert

$$b\left(\sum_{i=1}^n x_i \mathbf{b}_i, \sum_{k=1}^m y_k \mathbf{c}_k\right) := \sum_{i=1}^n x_i \sum_{k=1}^m y_k a_{ik} \quad \text{eine Bilinearform auf } V \times W :$$

Es gilt

$$\begin{aligned} & b\left(\sum_{i=1}^n x_i \mathbf{b}_i + \sum_{i=1}^n x'_i \mathbf{b}_i, \sum_{k=1}^m y_k \mathbf{c}_k\right) \\ &= b\left(\sum_{i=1}^n (x_i + x'_i) \mathbf{b}_i, \sum_{k=1}^m y_k \mathbf{c}_k\right) \\ &= \sum_{i=1}^n (x_i + x'_i) \sum_{k=1}^m y_k a_{ik} \\ &= \sum_{i=1}^n x_i \sum_{k=1}^m y_k a_{ik} + \sum_{i=1}^n x'_i \sum_{k=1}^m y_k a_{ik} \\ &= b\left(\sum_{i=1}^n x_i \mathbf{b}_i, \sum_{k=1}^m y_k \mathbf{c}_k\right) + b\left(\sum_{i=1}^n x'_i \mathbf{b}_i, \sum_{k=1}^m y_k \mathbf{c}_k\right) \end{aligned}$$

und analog für skalare Vielfache der ersten Komponente sowie Summen und skalare Vielfache (in) der zweiten Komponente – also nach (#) Bilinearität von b .

Da wegen

$$\begin{aligned} b\left(\sum_{i=1}^n x_i \mathbf{b}_i, \sum_{k=1}^m y_k \mathbf{c}_k\right) &= \sum_{i=1}^n x_i b\left(\mathbf{b}_i, \sum_{k=1}^m y_k \mathbf{c}_k\right) \\ &= \sum_{i=1}^n x_i \sum_{k=1}^m y_k b(\mathbf{b}_i, \mathbf{c}_k) \end{aligned}$$

jede Bilinearform durch ihre Werte auf den Basisvektorpaaren festgelegt ist, gibt es zudem nur eine Bilinearform mit $b(\mathbf{b}_i, \mathbf{c}_k) = a_{ik}$.

b) Dem Vektor \mathbf{e}_{rs} entspricht im Sinne von (a) die Matrix (e_{ik}^{rs}) mit einer 1 in Zeile r und Spalte s und ansonsten nur Nullen. Die Matrix einer Linearkombination $b = \sum x_{rs} \mathbf{e}_{rs}$ hat die Matrix (a_{ik}) mit $a_{ik} = x_{ik}$, und b kann daher nur dann die konstante Abbildung auf 0 sein, wenn alle $x_{ik} = 0$ sind. Somit sind die \mathbf{e}_{rs} linear unabhängig. An $(a_{ik}) = \sum a_{ik} \mathbf{e}_{ik}$ sieht man, dass die \mathbf{e}_{rs} den Raum der Bilinearformen aufspannen, d.h. eine jede als Linearkombination der \mathbf{e}_{rs} darstellbar ist.

7.51 Reelle Zahlen als rationaler Vektorraum

a) (i) $1, \sqrt{2}, \sqrt{3}$ und $\sqrt{6}$ sind irrational: Der Beweis der Irrationalität von $\sqrt{2}$ überträgt sich völlig analog auf $\sqrt{3}$. Ähnlich geht es mit $\sqrt{6}$: Ist $\sqrt{6} = p/q$, o.B.d.A. nach dem Kürzen p und q teilerfremd, dann gilt $p^2 = 6q^2$, und p muss die Primfaktoren 2 und 3 haben. p^2 ist dann durch 36 teilbar und $q^2 = p^2/6$ durch 6. Dann muss auch q die Primfaktoren 2 und 3 haben, im Widerspruch zur Teilerfremdheit.

(ii) $1, \sqrt{2}, \sqrt{3}$ sind linear unabhängig über dem Körper der rationalen Zahlen:

Annahme (A) $a + b\sqrt{2} + c\sqrt{3} = 0$ und nicht $a = b = c = 0$:

Fall 1: $c = 0$

Fall 1.1: $b = 0$ – Dann folgt $a = 0$, $a = b = c = 0$, im Widerspruch zu (A).

Fall 1.2: $b \neq 0$ – Dann folgt $\sqrt{2} = -a/b$, im Widerspruch zu (i).

Fall 2: $c \neq 0$

Fall 2.1: $b = 0$ – Dann folgt $\sqrt{3} = -a/c$, im Widerspruch zu (i).

Fall 2.2: $b \neq 0$ – Dann folgt $\sqrt{3} = (-a - b\sqrt{2})/c$. Beide Seiten Quadrieren und $\sqrt{2}$ alleine auf eine Seite Bringen ergibt $\sqrt{2} = (3c^2 - 2b^2 - a^2)/2ab$, einen Widerspruch zu (i).

Da unter (A) alle Fälle unmöglich sind, muss (A) falsch sein, so dass gilt:

$$a + b\sqrt{2} + c\sqrt{3} = 0 \Rightarrow a = b = c = 0, \text{ d.h.}$$

$1, \sqrt{2}, \sqrt{3}$ sind linear unabhängig.

(iii) $1, \sqrt{2}, \sqrt{3}$ und $\sqrt{6}$ sind lin. unabhängig über dem Körper der rationalen Zahlen:

Annahme (B) $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = 0$:

Subtrahiere in (B) Summanden 3 und 4: $a + b\sqrt{2} = -(c\sqrt{3} + d\sqrt{6})$

Quadriere: $a^2 + 2b^2 + 2ab\sqrt{2} = 3c^2 + 6d^2 + 6cd\sqrt{2}$

Sortiere um: $(a^2 + 2b^2 - 3c^2 - 6d^2) + (2ab - 6cd)\sqrt{2} = 0$

Wegen (ii): $a^2 + 2b^2 - 3c^2 - 6d^2 = 2ab - 6cd = 0$ (a)

Subtrahiere in (B) Summanden 2 und 4: $a + c\sqrt{3} = -(b\sqrt{2} + d\sqrt{6})$

Quadriere: $a^2 + 3c^2 + 2ac\sqrt{3} = 2b^2 + 6d^2 + 4bd\sqrt{3}$

Sortiere um: $(a^2 - 2b^2 + 3c^2 - 6d^2) + (2ac - 4bd)\sqrt{3} = 0$

Wegen (ii): $a^2 - 2b^2 + 3c^2 - 6d^2 = 2ac - 4bd = 0$ (b)

Aus (a) + (b): $a^2 = 6d^2$ (c)

(c) Fall 1: $a = d = 0$, aus (a) $2b^2 = 3c^2$

Quadratwurzel: $b\sqrt{2} - c\sqrt{3} = 0$ oder $b\sqrt{2} + c\sqrt{3} = 0$

wegen (ii): $b = c = 0$

(c) Fall 2: $a \neq 0 \neq d$ $6 = a^2/d^2$

Quadratwurzel: $\sqrt{6} = \pm a/d$, im Widerspruch zu (i)

Aus (B) $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = 0$ folgt, dass Fall 1, also $a = b = c = d = 0$ zutreffen muss – $1, \sqrt{2}, \sqrt{3}$ und $\sqrt{6}$ sind linear unabhängig.

b) Wegen der bekannten Rechenregeln, insbesondere des Distributivgesetzes für Multiplikation und Addition in \mathbb{R} , liegen die Bilder unter den Abbildungen (i, ii, iii) wieder in U , denn

$$\begin{aligned}\sqrt{2} \cdot (a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) &= \sqrt{2} \cdot a + \sqrt{2} \cdot b \cdot \sqrt{2} + \sqrt{2} \cdot c \cdot \sqrt{3} + d\sqrt{2} \cdot \sqrt{6} \\ &= a \cdot \sqrt{2} + b \cdot \sqrt{4} + c \cdot \sqrt{6} + d\sqrt{12} \\ &= 2b + a\sqrt{2} + 2d\sqrt{3} + c\sqrt{6} \\ (a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6})/\sqrt{3} &= (\sqrt{3}/3) \cdot (a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) \\ &= (\sqrt{3} \cdot a + \sqrt{3} \cdot b \cdot \sqrt{2} + \sqrt{3} \cdot c \cdot \sqrt{3} + d\sqrt{3} \cdot \sqrt{6})/3 \\ &= c + d\sqrt{2} + \frac{a}{3}\sqrt{3} + \frac{b}{3}\sqrt{6} \\ \sqrt{6} \cdot (a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) &= \sqrt{6} \cdot a + \sqrt{6} \cdot b \cdot \sqrt{2} + \sqrt{6} \cdot c \cdot \sqrt{3} + d\sqrt{6} \cdot \sqrt{6} \\ &= 6d + 3c\sqrt{2} + 2b\sqrt{3} + a\sqrt{6}\end{aligned}$$

Wegen der Distributiv-, Kommutativ- und Assoziativgesetze sind die Abbildungen (i, ii, iii) additiv, z.B.

$$\begin{aligned}\sqrt{2} \cdot [(a_1 + b_1\sqrt{2} + c_1\sqrt{3} + d_1\sqrt{6}) + (a_2 + b_2\sqrt{2} + c_2\sqrt{3} + d_2\sqrt{6})] \\ = \sqrt{2} \cdot (a_1 + b_1\sqrt{2} + c_1\sqrt{3} + d_1\sqrt{6}) + \sqrt{2} \cdot (a_2 + b_2\sqrt{2} + c_2\sqrt{3} + d_2\sqrt{6}),\end{aligned}$$

und multiplikativ, z.B.

$$\begin{aligned}\sqrt{2} \cdot [q \cdot (a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6})] &= (\sqrt{2} \cdot q) \cdot (a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) \\ &= (q \cdot \sqrt{2}) \cdot (a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) \\ &= q \cdot [\sqrt{2} \cdot (a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6})],\end{aligned}$$

also linear.

Aus den Berechnungen eingangs von (b) können wir die Matrizen ablesen, z.B. da die Bilder der kanonischen Einheitsvektoren Nr. i in der Spalte i stehen:

$$\text{i) } \begin{pmatrix} 0 & 2 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad \text{ii) } \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1/3 & 0 & 0 & 0 \\ 0 & 1/3 & 0 & 0 \end{pmatrix} \quad \text{iii) } \begin{pmatrix} 0 & 0 & 0 & 6 \\ 0 & 0 & 3 & 0 \\ 0 & 2 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

[Bezüglich der Basis $\mathbf{b}_1 = a$, $\mathbf{b}_2 = \sqrt{2}$, $\mathbf{b}_3 = \sqrt{3}$, $\mathbf{b}_4 = \sqrt{6}$ entspricht dem Vektor

$$\mathbf{v} = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \text{ der Spaltenvektor } \kappa(\mathbf{v}) = \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} \text{ und der linearen Abbildung}$$

A mit $A(\mathbf{v}) = \sqrt{2} \cdot \mathbf{v}$ die Matrix $(a_{ik}) = \mu(A)$. Die erste Spalte $a_{\bullet 1}$ von A ist

$$\kappa(A(1)) = \kappa(A(\mathbf{b}_1)) = \kappa(\sqrt{2} \cdot \mathbf{b}_1) = \kappa(\sqrt{2} \cdot 1) = \kappa(\sqrt{2}) = \kappa(1 \cdot \mathbf{b}_2) = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}; \text{ usw. }]$$

Wir entwickeln z.B. die 4×4 - und 3×3 -Determinanten nach dünn besetzten Spalten bzw. Zeilen (für (i) grafisch angedeutet):

$$\begin{vmatrix} \emptyset & 2 & 0 & 0 \\ 1 & \emptyset & \emptyset & \emptyset \\ \emptyset & 0 & 0 & 2 \\ \emptyset & 0 & 1 & 0 \end{vmatrix} = - \begin{vmatrix} 2 & \emptyset & 0 \\ 0 & \emptyset & 2 \\ \emptyset & 1 & \emptyset \end{vmatrix} = \begin{vmatrix} 2 & 0 \\ 0 & 2 \end{vmatrix} = 4,$$

$$\begin{vmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1/3 & 0 & 0 & 0 \\ 0 & 1/3 & 0 & 0 \end{vmatrix} = \begin{vmatrix} 0 & 0 & 1 \\ 1/3 & 0 & 0 \\ 0 & 1/3 & 0 \end{vmatrix} = \begin{vmatrix} 1/3 & 0 \\ 0 & 1/3 \end{vmatrix} = 1/9 ,$$

$$\begin{vmatrix} 0 & 0 & 0 & 6 \\ 0 & 0 & 3 & 0 \\ 0 & 2 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{vmatrix} = - \begin{vmatrix} 0 & 0 & 6 \\ 0 & 3 & 0 \\ 2 & 0 & 0 \end{vmatrix} = -2 \cdot \begin{vmatrix} 0 & 6 \\ 3 & 0 \end{vmatrix} = 36 .$$

7.52 Gaußscher Algorithmus für Determinanten

In Alg. 7.1 wird die Matrix in normierte Stufenform gebracht. In Alg. 7.2 wird die Matrix im Prinzip in Stufenform gebracht, aber nicht normiert. Wenn dabei in 7.2 keine obere Dreiecksmatrix entsteht, d.h. ein Diagonalelement zu 0 wird, hat die Determinante den Wert 0.

7.1(2) \rightarrow 7.2(2): Eine Nullspalte bedeutet, dass die Determinante 0 ist, während im Gleichungssystem weiter zu rechnen ist.

7.1(3) \rightarrow 7.2(3): Die Determinante ergibt sich z.B. der Reihe nach durch Entwicklung nach den Spalten von 1 bis n . Da die Matrix inzwischen eine Dreiecksmatrix ist, läuft dies auf die Multiplikation der Diagonalelemente hinaus.

7.1(4,5,6,7) \rightarrow 7.2(4,5): Beim Gleichungssystem wird die Komponente z_s zu 1 normiert, und die Komponenten unterhalb z_s werden durch Subtraktion der entsprechenden Vielfachen von Zeile z zu 0 gemacht. Bei der Determinante wird ein entsprechendes Vielfaches der Zeile subtrahiert, was den Wert der Determinante nicht verändert. Beim einfachen Zeilentausch ändert sich in der Determinante das Vorzeichen, also wird eine der beiden mit -1 multipliziert, damit die Determinante sich nicht verändert.

7.53 Eigenwerte von Projektionen

Zunächst gilt allgemein in Vektorräumen für Skalare k und Vektoren \mathbf{v} , dass

$$k\mathbf{v} = \mathbf{0} \Rightarrow k = 0 \vee \mathbf{v} = \mathbf{0} \quad (\#),$$

denn wenn $k\mathbf{v} = \mathbf{0}$ und $k \neq 0$, dann gilt

$$\mathbf{v} = 1\mathbf{v} = (1/k)k\mathbf{v} = (1/k)\mathbf{0} = (1/k) \cdot (0 \cdot \mathbf{0}) = (1/k \cdot 0)\mathbf{0} = 0 \cdot \mathbf{0} = \mathbf{0} .$$

Es seien λ ein Eigenwert und \mathbf{v} ein Eigenvektor von A mit $A \circ A = A$. Dann gilt

$$\lambda\mathbf{v} = A(\mathbf{v}) = A(A(\mathbf{v})) = A(\lambda\mathbf{v}) = \lambda \cdot A(\mathbf{v}) = \lambda \cdot \lambda\mathbf{v} = \lambda^2\mathbf{v} ,$$

also $\mathbf{v} \neq \mathbf{0}$ (Eigenvektor!) und $\lambda(1 - \lambda)\mathbf{v} = (\lambda^2 - \lambda)\mathbf{v} = \lambda^2\mathbf{v} - \lambda\mathbf{v} = \mathbf{0}$,

also wegen (#) $\lambda(1 - \lambda) = 0$,

und damit $\lambda = 0$ oder $\lambda = 1$.

7.54 Eigenwerte und -vektoren

Passende *Beispiele* (definiert anhand der Folgen $x = (x_1, x_2, x_3, \dots)$) sind ...

$$A(\mathbf{x})_i := x_{i+1},$$

$$B(\mathbf{x})_{2i} := x_{2i-1}, \quad B(\mathbf{x})_{2i-1} := x_{2i}$$

$$C(\mathbf{x})_i := x_1,$$

$$D(\mathbf{x})_1 := x_1, \quad D(\mathbf{x})_{i+1} := 2D(\mathbf{x})_i$$

- 1-dimensionaler Eigenraum bei: $A, C, D:$ $A\mathbf{v} = \mathbf{v} \Leftrightarrow \mathbf{v} = (k, k, k, \dots) \Leftrightarrow C\mathbf{v} = \mathbf{v}$
 $D\mathbf{v} = \mathbf{v} \Leftrightarrow \mathbf{v} = (k, 2k, 4k, \dots)$

[Es handelt sich hier also jeweils um den Eigenraum zum Eigenwert 1. Dieser spezielle Wert müsste es aber nicht unbedingt sein, wie das Beispiel $E(\mathbf{x}) := 2A(\mathbf{x})$ zeigt.]

- ∞ -dimensionaler Eigenraum bei: $B, C:$ $v^i_{2i} = v^i_{2i-1}$ und $v^i_k = 0$ für $k \neq 2i$,
 $2i-1 \Rightarrow \mathbf{v}^i$ lin. unabh., $B(\mathbf{v}^i) = \mathbf{v}^i$.
 $u^i_k = \delta_{ik}$ für $i > 0 \Rightarrow$
 $\mathbf{u}^i, i > 0$, lin. unabh., $C(\mathbf{u}^i) = \mathbf{0}$.

[Es handelt sich hier um den Eigenraum zum Eigenwert 1 bzw. 0, der hier jeweils unendlich viele, wie man leicht zeigt, linear unabhängige Vektoren \mathbf{v}^i bzw. \mathbf{u}^i enthält.]

- konstante Folge als Eigenv. bei: $A, B, C:$ s.o. & $B: B(1,1,1,\dots) = (1,1,1,\dots)$
- keine konst. Folge als Eigenv. bei: $D:$ $D(\mathbf{x})$ konstante Folge $\Leftrightarrow \mathbf{x} = \mathbf{0}$
- Eigenwert 1 bei: $A, B, C, D:$ s.o. bei 1-dim. E.-R.
- Eigenwert 2 bei: $A:$ $A(1,2,4,8,\dots) = (2,4,8,\dots)$

7.55 Bilder von Normalteilern

Nehmen wir an, die Voraussetzungen des ersten Satzes seien gegeben. Ist nun $y \in f(N)$ und $b \in H$, dann existieren $x \in N$ mit $y = f(x)$ und $a \in G$ mit $b = f(a)$, und es gilt nun (wobei wir auf die Symbole \circ und \bullet verzichten)

$$byb^{-1} = f(a)f(x)f(a)^{-1} = f(axa^{-1}) \in f(N), \text{ denn } aNa^{-1} \subseteq N, axa^{-1} \in N, \text{ also}$$

$$bf(N)b^{-1} \subseteq f(N),$$

d.h. $f(N)$ ist Normalteiler von H .

7.56 Ein Kriterium für Normalteiler

Wir arbeiten mit dem neutralen Element e in G und lassen das Verknüpfungszeichen und wegen der Assoziativität auch die zugehörigen Klammern oft weg, vgl. eingangs von 7.5.1. Wir verwenden die Inversion jetzt auch als Kurzform auf ganzen Mengen und meinen damit die Mengen aller Inversen aller Elemente. Vorab stellen wir fest: Gilt die Gleichung am Ende, so gilt auch $(Ug)(Uh) = U(gh)$, denn dann ist

$$(Ug)(Uh) = ((Ug)(Uh))^{-1} = ((Uh)^{-1}(Ug)^{-1})^{-1} = (h^{-1}U^{-1}g^{-1}U^{-1})^{-1} = (h^{-1}Ug^{-1}U)^{-1}$$

$$\dots = (h^{-1}g^{-1}U)^{-1} = (h^{-1}g^{-1}U^{-1})^{-1} = ((gh)^{-1}U^{-1})^{-1} = U(gh).$$

Gilt die Gleichung am Ende, ist U Normalteiler von G , denn dann gilt für jedes $g \in G$:

$$gU = geU = gg^{-1}gU = gg^{-1}UgU = eUgU = UgU = UgUe = UgUg^{-1}g$$

$$\dots = Ugg^{-1}g = Ueg = Ug.$$

Ist umgekehrt U Normalteiler, so folgt

$$(gU)(hU) = g(Uh)U = g(hU)U = gh(UU) = (gh)U.$$

7.57 Kleinste Ideale (Achtung: Aufgabe wurde in den Korrekturen neu formuliert!)

a.i) Jedes $m \in M$ ist mittels $m_1 := m$ identisch mit $\sum_{i=1}^1 m_i - \sum_{k=1}^0 l_k$, also Element von $[M]_+$. Nun verwenden wir noch das Untergruppen-Kriterium von Satz 7.7:

Für $\sum_{i=1}^m m_i - \sum_{k=1}^n l_k$ und $\sum_{i=1}^o m'_i - \sum_{k=1}^p l'_k \in [M]_+$ gilt mit $m_{m+k} := l'_k$ und $l_{n+i} := m'_i$: $(\sum_{i=1}^m m_i - \sum_{k=1}^n l_k) - (\sum_{i=1}^o m'_i - \sum_{k=1}^p l'_k) = \sum_{i=1}^{m+p} m_i - \sum_{k=1}^{n+o} l_k \in [M]_+$.

a.ii) Wegen $\sum_{i=1}^0 m_i = 0_R$ und $\sum_{i=1}^m m_i := (\sum_{i=1}^{m-1} m_i) + m_m$ für $m > 0$ muss jede M enthaltende Untergruppe von $(R, +)$ alle endlichen Summen $\sum_{i=1}^m m_i$ und $\sum_{k=1}^n l_k$ sowie deren Differenzen enthalten, also alle Elemente von $[M]_+$.

[Etwas strenger ist ein – nun einfacher – induktiver Beweis entlang der obigen Betrachtung. Teil (a) ist von der Ringstruktur unabhängig und liefert uns allgemein die kleinste („von M erzeugte“) Untergruppe einer abelschen Gruppe, die eine vorgegebene Teilmenge M enthält.]

b.i) I_a ist Untergruppe und enthält a und M_a , vgl. (a).

$$RR \subseteq R \quad RM_a = Ra + RRa + RaR + RRaR \subseteq Ra + RaR \subseteq M_a \text{ und analog}$$

$$M_a R \subseteq M_a. \text{ Ferner ist wegen } R \sum_{i=1}^m m_i = \sum_{i=1}^m R m_i \text{ und } (\sum_{i=1}^m m_i) R = \sum_{i=1}^m m_i R$$

$$RI_a \subseteq I_a \supseteq I_a R.$$

b.ii) Jedes a enthaltende Ideal I in R , muss alle seine – auch wiederholten – Produkte mit R umfassen, also insbesondere auch RI , IR und RIR . Diese Mengen umfassen wegen $a \in I$ auch Ra , aR und RaR . Als +-Untergruppe enthält I nun auch alle endlichen Summen und Differenzen aus a und Elementen von Ra , aR und RaR – umfasst also ganz I_a .

7.58 Idealmultiplikation

Im Ring $(\mathbb{Z}, +, \cdot)$ ist $4\mathbb{Z}$ ein Ideal, denn Summen, Differenzen und ganzzahlige Vielfache von Vielfachen von 4 sind Vielfache von 4. Nun betrachten wir in \mathbb{Z}_4 das Element $2_4 = 2 + 4\mathbb{Z}$. Per Mengenummultiplikation in \mathbb{Z} ist

$$(2 + 4\mathbb{Z}) \cdot (2 + 4\mathbb{Z}) = (4 + 8\mathbb{Z} + 8\mathbb{Z} + 16\mathbb{Z}) = 4 + 8\mathbb{Z}.$$

In $(\mathbb{Z}_4, +, \cdot)$ ist $2_4 + 2_4 = 4_4 = 0_4 = 4\mathbb{Z}$.

Nun ist $0 = 4 \cdot 0 \in 4\mathbb{Z}$, aber $0 \notin 4 + 8\mathbb{Z}$, d.h. die beiden Mengen unterscheiden sich.

7.59 Ein interessanter Quotient eines Polynomrings

$\mathbb{R}[x]$ bildet mit der üblichen Polynomaddition und -multiplikation, z.B. mit

$$(3x^2 - x + 2)(x - 1) = 3x^3 - x^2 + 2x - 3x^2 + x - 2 = 3x^3 - 4x^2 + 3x - 2$$

einen kommutativen Ring mit Nullelement 0 und mit Eins 1. Wegen der Kommutativität und der Eins in $\mathbb{R}[x]$ ist jede additive Untergruppe I mit $\mathbb{R}I \subseteq I$ ein Ideal, und in dem Fall ist $\mathbb{R}I = I$. Nun ist $\mathbb{R}[x](x^2 + 1)$ eine additive Untergruppe, denn

$$\left(\sum_{i=0}^m r_i x^i\right)(x^2 + 1) - \left(\sum_{i=0}^n q_i x^i\right)(x^2 + 1) = \left(\sum_{i=0}^{\max(m,n)} (r_i - q_i) x^i\right)(x^2 + 1) \in \mathbb{R}[x](x^2 + 1),$$

wobei zunächst fehlende r_i bzw. q_i als 0 definiert sind.

Und natürlich ist ein Vielfaches eines Vielfachen von $x^2 + 1$ wegen der Assoziativität der Multiplikation selbst ein Vielfaches von $x^2 + 1$, also $\mathbb{R}[x](x^2 + 1)$ sogar ein Ideal.

Nun ist wegen der Polynomdivisionsregeln die Abbildung von $\sum_{i=1}^m r_i x^i$ auf (r_0, r_1, q) mit $q \in \mathbb{R}[x]$ und $\sum_{i=1}^m r_i x^i = r_0 + r_1 x + q(x^2 + 1)$ bijektiv von $\mathbb{R}[x]$ auf $\mathbb{R} \times \mathbb{R} \times \mathbb{R}[x]$. Also ist auch die Abbildung

$$f : \begin{cases} \mathbb{R}[x]/I & \rightarrow \mathbb{R} \times \mathbb{R} \\ r_0 + r_1 x + I & \mapsto (r_0, r_1) \end{cases}$$

bijektiv und ein +-Homomorphismus. Sie ist allerdings kein Ringhomomorphismus, da $f(p_1 \cdot p_2) = f(p_1) \cdot f(p_2)$ nicht immer gilt, sonst gälte auch

$$\begin{aligned} (0,0) &= f(0 + I) = f(x^2 + 1) = f((x+1)(x-1) + 2) \\ &= f(x+1) \cdot f(x-1) + f(2) = (1,1) + (1,-1) + (0,2) \\ &= (2,2). \end{aligned}$$

Ein Isomorphismus liegt jedoch mit

$$f : \begin{cases} \mathbb{R}[x]/I & \rightarrow \mathbb{C} \\ r_0 + r_1 x + I & \mapsto r_0 + r_1 i, \end{cases}$$

vor, denn g ist additiv und, wie man hier sieht, auch multiplikativ:

$$\begin{aligned} g((r_0 + r_1 x + I)(s_0 + s_1 x + I)) &= g((r_0 + r_1 x)(s_0 + s_1 x) + I) \\ &= g(r_0 s_0 + r_1 s_1 x^2 + (r_0 s_1 + r_1 s_0)x + I) \\ &= g(r_0 s_0 + r_1 s_1 x^2 + (r_0 s_1 + r_1 s_0)x + I - r_1 s_1(x^2 + 1)) \\ &= g((r_0 s_0 - r_1 s_1) + (r_0 s_1 + r_1 s_0)x + I) \\ &= (r_0 s_0 - r_1 s_1) + (r_0 s_1 + r_1 s_0)i \\ &= (r_0 + r_1 i)(s_0 + s_1 i) \\ &= g(r_0 + r_1 x + I) \cdot g(s_0 + s_1 x + I). \end{aligned}$$

7.60 Gleichungsspezifizierte Warteschlange

a) Die FIFO-Warteschlange

def FifoWarteschlange
sorten symbol, fifoschl
operatoren

a, b, c: → symbol;
leer: → fifoschl;
vorn: fifoschl → symbol;
rein: fifoschl, symbol → fifoschl;
raus: fifoschl → fifoschl;

axiome

fuer alle x, y in symbol; q in fifoschl:

raus(rein(leer,x)) = leer
raus(rein(rein(q,x),y)) = rein(raus(rein(q,x)),y)
vorn(rein(leer,x)) = x
vorn(rein(rein(q,x),y)) = vorn(rein(q,x))

[Das *erste* und *dritte* Axiom sind selbsterklärend. Das *zweite* Axiom schiebt das „raus“ näher an das „leer“ in q, damit irgendwann das erste Axiom greift. Das *vierte* Axiom kürzt den Term, damit irgendwann das dritte Axiom greift. Mit diesen Axiomen können wir beispielsweise die Antwort auf folgende Frage berechnen:

Mit leer führen wir aus: rein a, rein b, raus. Was liefert nun vorn?

$$\begin{aligned} \text{vorn}(\text{raus}(\text{rein}(\text{rein}(\text{leer},a),b))) &= \text{vorn}(\text{rein}(\text{raus}(\text{rein}(\text{leer},a),b))) \\ &= \text{vorn}(\text{rein}(\text{leer},b)) \\ &= b \end{aligned}$$

Hierbei ist jeweils der nächste gemäß Axiom umzuformende Unterterm unterstrichen.]

b) Für die Leer-Abfrage wird ergänzt ...

unter sorten: , wahr/falsch
unter operatoren

W, F: → boole;
istleer: fifoschl → boole;

unter axiome:

istleer(leer) = W
istleer(rein(q,x)) = F

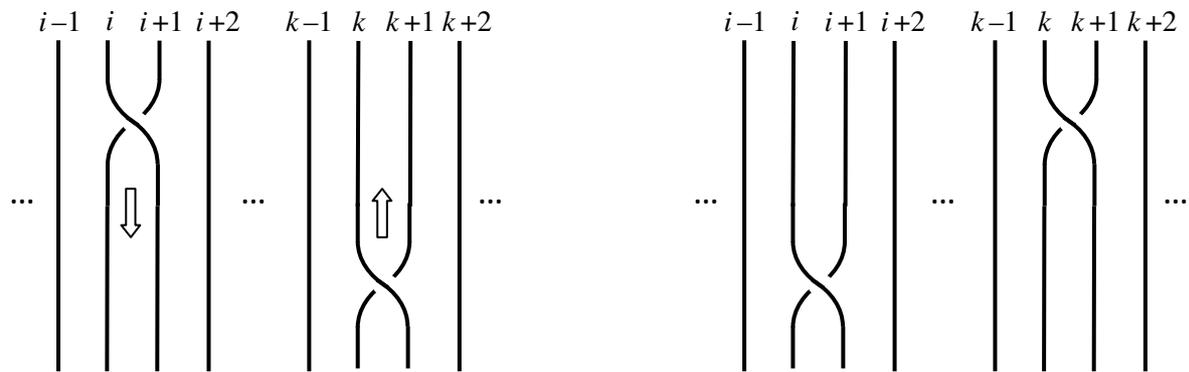
[Noch ein Beispiel: Mit leer führen wir aus: rein a, raus, rein b, rein a, raus.
Was liefert nun istleer?

$$\begin{aligned} \text{istleer}(\text{raus}(\text{rein}(\text{rein}(\text{raus}(\text{rein}(\text{leer},a)),b),a))) &= \text{istleer}(\text{rein}(\text{raus}(\text{rein}(\text{leer},b)),a)) \\ &= \text{istleer}(\text{rein}(\text{leer},a)) \\ &= F \end{aligned}$$

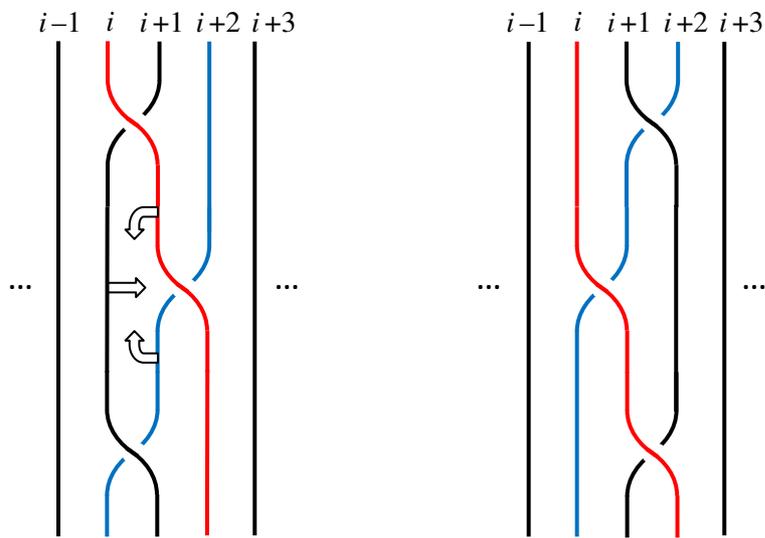
Technisch offen gelassen ist hierbei noch die Frage der „unerwünschten Terme“, wie „raus(leer)“. Die Axiome verraten darüber nichts, da sie sich nur auf erwünschte Terme beziehen.]

7.61 Zopfgruppe als initiale Algebra

$$a_i a_k = a_k a_i :$$



$$a_i a_{i+1} a_i = a_{i+1} a_i a_{i+1} :$$



7.62 Matrizenrechnung in der Graphentheorie

- a) Wir bearbeiten den Fall der gerichteten Graphen. Ungerichtete Graphen sind dann mit eingeschlossen, da wir sie wie beschrieben als gerichtete Graphen mit den Kanten (a,a) für $\{a\}$ sowie (a,b) und (b,a) für $\{a,b\}$ auffassen können. [Die Nachbarschaftsmatrix eines ungerichteten Graphen ist deshalb symmetrisch.]
 Einen Pfad der Länge 0 (also ohne Kanten) – und zwar genau einen – gibt es genau von jedem Knoten zu sich selbst. Und in $A^0 = E_n$ mit den Komponenten δ_{ij} gilt $\delta_{ii} = 1$, ansonsten $\delta_{ij} = 0$ für $i \neq j$. Die in (a) zu zeigende Aussage gilt also für $k = 0$.
 Angenommen, sie gilt für ein $k \in \mathbb{N}_0$, und ${}^k a_{ij}$ sind die Komponenten von A^k . Dann besteht jeder Pfad von v_i nach v_j der Länge $k+1$ aus einem Pfad der Länge k und einer letzten Kante. Davon gibt es für jeden vorletzten vorkommenden Knoten – und diese sind alle Vorgänger v_l von v_j – so viele, wie es Pfade von v_i nach v_l gibt. Ansonsten kann man für jeden dabei *nicht* an vorletzter Stelle vorkommenden Knoten v_l die Anzahl der Wege von v_i nach v_l , multipliziert mit der Anzahl der Kanten (0 oder 1) von v_l nach v_j dazu addieren, denn einer der Faktoren ist 0. Damit ist die Anzahl der Pfade von v_i nach v_j der Länge $k+1$ gleich der Summe (über alle l) der Produkte aus der Anzahl der Pfade von v_i nach v_l und der Anzahl der Kanten von v_l nach v_j , d.h.

$$\sum_{l=1}^n ({}^k a_{il} \cdot a_{lj}) = {}^{k+1} a_{ij}, \text{ die Komponente } ij \text{ von } A^{k+1}$$

womit die Aussage induktiv bewiesen ist.

- b) ... ist nach (a) trivial, da sich die Menge der Pfade einer Länge von höchstens k in G von v_i nach v_j zusammensetzt aus den (sogar disjunkten) Teilmengen der entsprechenden Pfade der Länge 0, 1, ... bis k .
- c) Aus (b) folgt, dass es genau dann von jedem Knoten v_i zu jedem Knoten v_j einen Pfad gibt (also starker Zusammenhang vorliegt), wenn die Komponente ij der endlichen Teilsummen von

$$E_n + A + A^2 + A^3 + \dots$$

irgendwann 0 überschreitet. Wenn aber ein Pfad von v_i nach v_j einer Länge $\geq n$ existiert, so enthält er nach Satz 6.2 eine Schleife $v \dots v$ von einem Knoten zu sich selbst, so dass man, wenn man von der Schleife alles außer dem ersten v streicht, immer noch einen (nun echt kürzeren) Pfad von v_i nach v_j erhält. Das geht so lange, bis man einen Pfad einer Länge $< n$ gefunden hat, d.h. die Komponente ij von

$$E_n + A + A^2 + A^3 + \dots + A^{n-1}$$

ist größer als 0. Die Umkehrung ergibt sich unmittelbar aus (b).