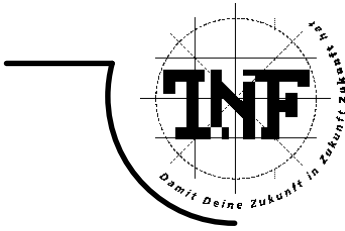




JOHANNESKEPLER  
UNIVERSITÄTLINZ  
Netzwerk für Forschung, Lehre und Praxis



# Algebra

**Bachelorstudium Informatik**

**Vorlesungsskriptum**

Sommersemester 2008

Erhard Aichinger  
Institut für Algebra  
Johannes Kepler Universität Linz

Alle Rechte vorbehalten

Linz, im März 2008

Adresse:  
Univ.-Doz. Dr. Erhard Aichinger  
Institut für Algebra  
Johannes Kepler Universität Linz  
4040 Linz  
e-mail: [erhard.aichinger@jku.at](mailto:erhard.aichinger@jku.at)  
Auflage März 2008

Druck: Kopierstelle, Abteilung Service, Universität Linz



## Vorwort

Die Vorlesung *Algebra* soll die Grundlagen der linearen Algebra liefern, die wir brauchen, um geometrische Objekte und Bewegungen dieser Objekte zu beschreiben. Dazu wird das Rechnen mit Vektoren und Matrizen vermittelt. Außerdem werden endliche Körper behandelt, da sie in vielen Algorithmen der Kryptologie und Codierungstheorie verwendet werden.

Viele Rechnungen werden mit mathematischer Software (Mathematica) durchgeführt. Einige Mathematica-Programme sind auf <http://www.algebra.uni-linz.ac.at/Students/MathInf/vlws05/MathematicaProgramme/> zu finden und werden den Studierenden ausschließlich für die Nutzung im Rahmen des Kurses *Algebra* zur Verfügung gestellt.

Für die Erstellung dieses Skriptums habe ich Unterlagen benutzt, die für Vorlesungen an der Johannes Kepler Universität Linz und der FH Oberösterreich, Standort Hagenberg, verwendet worden sind. An diesen Unterlagen haben Martin Burger, Jürgen Ecker, Julia Greslehner, Dénes Koch, Livia Koch, Peter Mayr, Bernadette Mayrhauser, Christian Neumaier und Axel Riese mitgearbeitet. Peter Mayr hat für die Vorlesung im Wintersemester 2007 einige Teile neu hinzugefügt, Erklärungen ergänzt und Fehler korrigiert. Herzlichen Dank!

Ich freue mich über Rückmeldungen zum Skriptum (auch über Kritik) und lade Sie ein, mir an [erhard.aichinger@jku.at](mailto:erhard.aichinger@jku.at) Ihre Bemerkungen zu senden. E.A.



## Inhaltsverzeichnis

Vorwort	iii
Kapitel 1. Geometrie in der Ebene und im Raum	1
1. Koordinaten	1
2. Vektoren	1
3. Die Länge eines Vektors	3
4. Trigonometrie	5
5. Der Winkel zwischen zwei Vektoren	12
6. Geraden in der Ebene	14
7. Vektoren im $\mathbb{R}^n$	18
8. Geraden und Ebenen im Raum	20
Kapitel 2. Matrizen	25
1. Die Definition von Matrizen	25
2. Die Addition von Matrizen	26
3. Die Multiplikation einer Matrix mit einer reellen Zahl	27
4. Die Multiplikation von Matrizen	27
5. Rechenregeln für die Addition und Multiplikation von Matrizen	29
6. Die Multiplikation von Vektoren und Matrizen	29
7. Das Transponieren von Matrizen	31
8. Die Einheitsmatrizen	32
9. Das Invertieren von Matrizen	33
Kapitel 3. Lineare Gleichungssysteme	37
1. Beispiele	37
2. Die Lösung von Gleichungssystemen in Staffelform	41
3. Das Gaußsche Eliminationsverfahren	43
4. Einige durchgerechnete Beispiele zum Gauß-Algorithmus	46
Kapitel 4. Unterräume des $\mathbb{R}^n$	53
1. Die Definition eines Unterraums	53
2. Die lineare Hülle von Vektoren	55
3. Die lineare Unabhängigkeit von Vektoren	56
4. Basen eines Vektorraums	57
5. Die Zeilenstaffelnormalform	62
6. Der Nullraum einer Matrix	67

7.	Die Dimension eines Unterraumes	71
8.	Der Rang einer Matrix	73
9.	Die Eindeutigkeit der Zeilenstaffelnormform	74
10.	Die Lösungsmenge inhomogener linearer Gleichungssysteme	76
11.	Koordinaten	79
12.	Summen und Durchschnitte von Unterräumen	81
Kapitel 5. Orthogonalität		85
1.	Der Winkel zwischen zwei Vektoren	85
2.	Der Normalraum auf eine Menge von Vektoren	86
3.	Orthonormalbasen	86
4.	Das Gram-Schmidtsche Orthonormalisierungsverfahren	88
5.	Orthogonalprojektionen	91
6.	Abstandsberechnungen mit Hilfe der Orthogonalprojektion	94
7.	Die bestapproximierende Lösung eines linearen Gleichungssystems	99
Kapitel 6. Rechnen in den ganzen Zahlen		101
1.	Teilbarkeit	101
2.	Das Lösen von Kongruenzen	104
Kapitel 7. Ringe, Körper und Vektorräume		109
1.	Ringe	109
2.	Der Ring $\mathbb{Z}_n$	110
3.	Das RSA-Verschlüsselungsverfahren	114
4.	Die Multiplikativität der Eulerschen $\varphi$ -Funktion	114
5.	Körper	117
6.	Vektorräume	118
Kapitel 8. Polynome und endliche Körper		121
1.	Polynome	121
2.	Teilbarkeit von Polynomen	122
3.	Polynomfunktionen und Nullstellen	124
4.	Körper aus Polynomringen	124
5.	Eigenschaften endlicher Körper	127
Kapitel 9. Lineare Abbildungen		131
1.	Beispiele	131
2.	Die Definition linearer Abbildungen	132
3.	Abbildungsmatrizen linearer Abbildungen	134
4.	Abbildungsmatrizen für Spiegelungen und Drehungen	137
5.	Basistransformationen	140
6.	Die Hintereinanderausführung und die Matrizenmultiplikation	141
7.	Abbildungsmatrizen für Spiegelungen und Drehungen bezüglich der kanonischen Basis	142

Kapitel 10. Der Zusammenhang zwischen linearen Abbildungen und Matrizen	147
1. Faktorräume	147
2. Der Homomorphiesatz	148
3. Der Rang einer Matrix und ihre Invertierbarkeit	149
4. Die Determinante einer quadratischen Matrix	150
Kapitel 11. Homogene Koordinaten	157
1. Die projektive Ebene	157
2. Lineare Abbildungen in der projektiven Ebene	158
3. Der projektive Raum	159
Anhang A. Programme, die vorrechnen	163



## KAPITEL 1

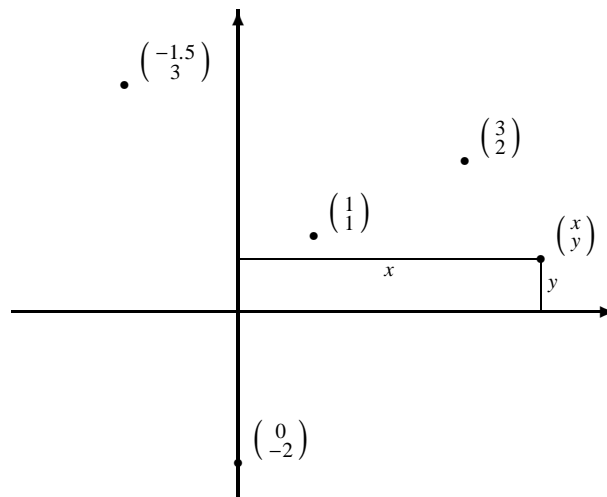
# Geometrie in der Ebene und im Raum

### 1. Koordinaten

Wir beschreiben – nach einer Idee von René Descartes (1596 – 1650) – jeden Punkt in der Ebene durch ein Paar reeller Zahlen. Die Menge der Paare reeller Zahlen kürzen wir mit  $\mathbb{R} \times \mathbb{R}$  oder  $\mathbb{R}^2$  ab.

$$\mathbb{R} \times \mathbb{R} := \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \mid x \in \mathbb{R} \text{ und } y \in \mathbb{R} \right\}.$$

Für das Paar  $\begin{pmatrix} x \\ y \end{pmatrix}$  schreiben wir auch  $(x, y)$ . Aus der folgenden Skizze ist ersichtlich, wie wir jeden Punkt durch ein Zahlenpaar (seine *kartesischen Koordinaten*) beschreiben.

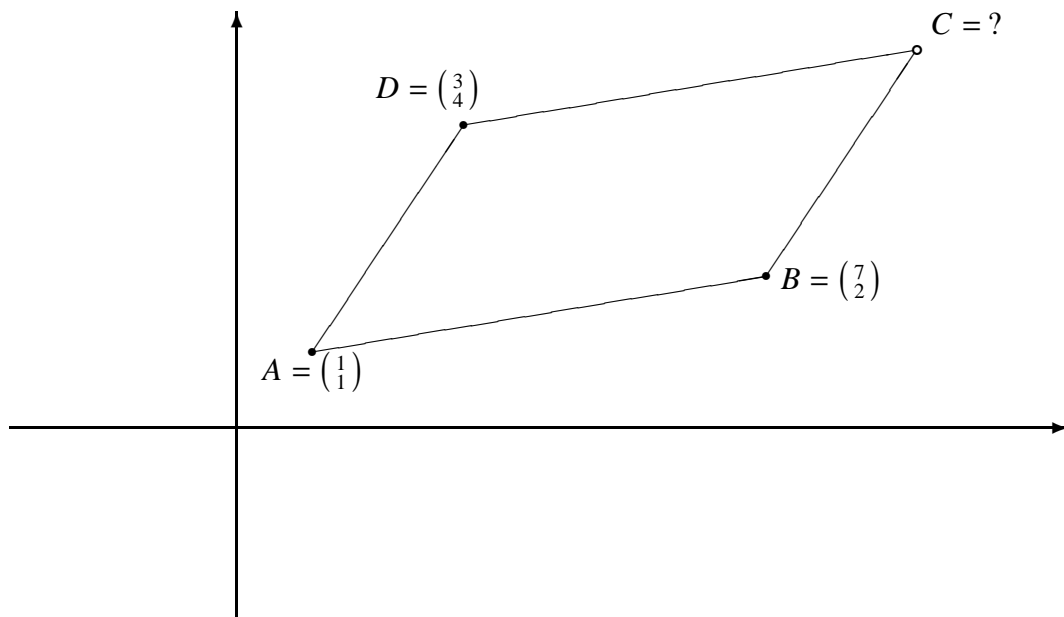


### 2. Vektoren

Wo liegt der Punkt  $C$  im Parallelogramm  $ABCD$ , dessen Punkte  $A$ ,  $B$  und  $D$  durch

$$A = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, B = \begin{pmatrix} 7 \\ 2 \end{pmatrix}, D = \begin{pmatrix} 3 \\ 4 \end{pmatrix}$$

gegeben sind?



Um von  $A$  nach  $B$  zu kommen, müssen wir 6 nach rechts und 1 nach oben gehen.

$$\vec{AB} = \begin{pmatrix} 7 \\ 2 \end{pmatrix} - \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 6 \\ 1 \end{pmatrix}.$$

Wenn wir von  $D$  starten und um 6 nach rechts und 1 nach oben gehen, landen wir bei  $C$ .

$$C = D + \vec{AB} = \begin{pmatrix} 3 \\ 4 \end{pmatrix} + \begin{pmatrix} 6 \\ 1 \end{pmatrix} = \begin{pmatrix} 9 \\ 5 \end{pmatrix}.$$

Wir bemerken, dass wir ein Paar reeller Zahlen, wie etwa  $\begin{pmatrix} 6 \\ 1 \end{pmatrix}$ , verwenden, um zwei verschiedene Dinge zu beschreiben:

- Den Punkt, der um 6 Längeneinheiten rechts und um 1 Längeneinheit über dem Punkt  $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$  liegt.
- Den Weg (*Vektor*) von  $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$  nach  $\begin{pmatrix} 7 \\ 2 \end{pmatrix}$ .

In Mathematica werden Vektoren als Listen dargestellt.

```
In[1]:= a = {1, 1};
```

```
In[2]:= b = {7, 2};
```

```
In[3]:= d = {3, 4};
```

```
In[4]:= ab = b - a
```

```
Out[4]= {6, 1}
```

```
In[5]:= c = d + ab
```

```
Out[5]= {9, 5}
```

### 3. Die Länge eines Vektors

Wir lösen folgendes Beispiel:

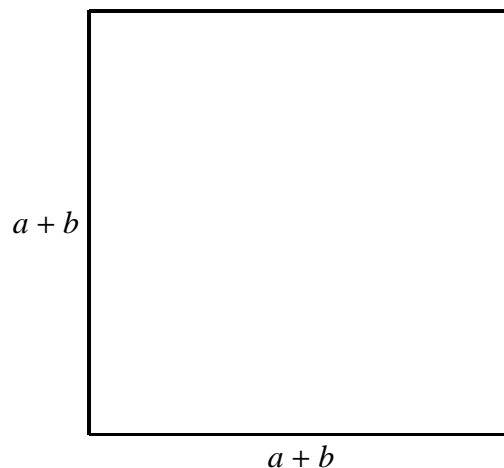
Herr A geht von  $\begin{pmatrix} 3 \\ 2 \end{pmatrix}$  aus 1 Einheit in Richtung Südosten. Wo landet er?

“Richtung Südosten” heißt “in Richtung  $\begin{pmatrix} 1 \\ -1 \end{pmatrix}$ ”. Allerdings hat  $\begin{pmatrix} 1 \\ -1 \end{pmatrix}$  die Länge  $\sqrt{2} \approx 1.41421$ . Daher hat  $v = \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 \\ -1 \end{pmatrix}$  die Länge 1 und zeigt auch in Richtung Südosten. Herr A landet also im Punkt Z, den wir uns mit

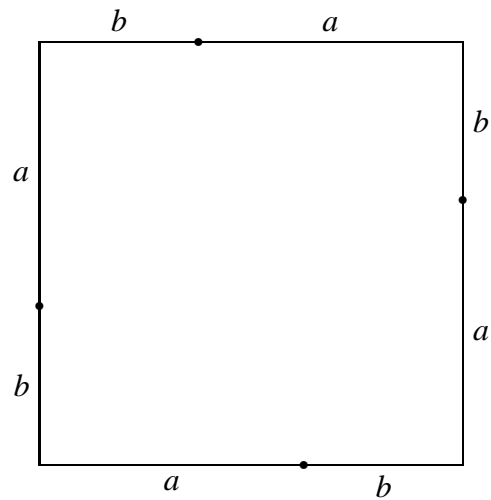
$$Z = \begin{pmatrix} 3 \\ 2 \end{pmatrix} + \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} 1 \\ -1 \end{pmatrix} \approx \begin{pmatrix} 3.7 \\ 1.3 \end{pmatrix}$$

ausrechnen.

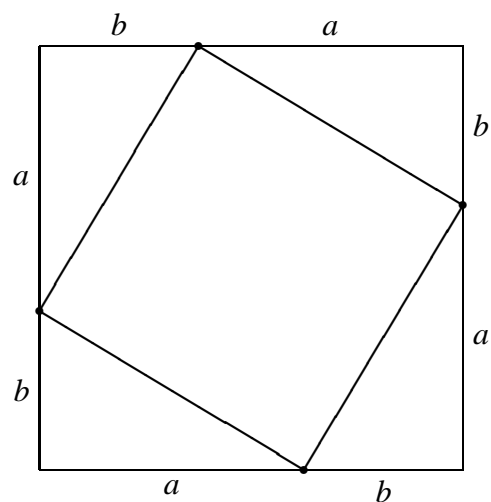
Wir überlegen uns jetzt, wie lange der Vektor  $\begin{pmatrix} a \\ b \end{pmatrix}$  ist. Das heißt, wir wollen wissen, wie lange in einem Dreieck, in dem die Seiten mit den Längen  $a$  und  $b$  einen rechten Winkel einschließen, die dem rechten Winkel gegenüberliegende Seite ist. Vergessen wir kurz unsere klassische Bildung, und zeichnen wir ein Quadrat mit Seitenlänge  $a + b$ .



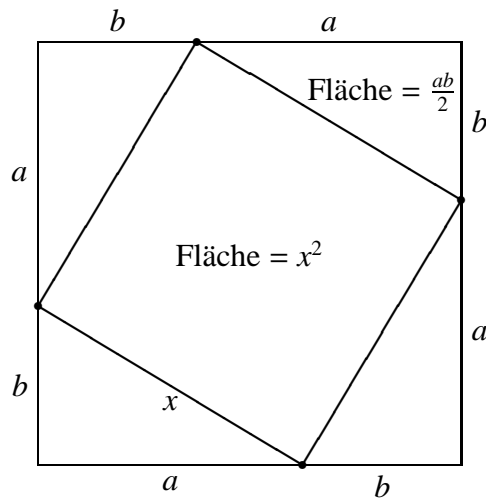
Jetzt unterteilen wir jede der vier Quadratseiten in ein Stück der Länge  $a$  und ein Stück der Länge  $b$ .



Wir verbinden die vier Teilungspunkte.



Das innere jetzt eingezeichnete Viereck ist ein Quadrat. Das kann man so begründen: wenn man die ganze Zeichnung um  $90^\circ$  gegen den Uhrzeigersinn dreht, kommt das innere Viereck auf sich selbst zu liegen: daher sind alle vier Winkel des inneren Vierecks gleich groß. In jedem Dreieck ist die Winkelsumme  $180^\circ$ , und daher ist in jedem Viereck die Winkelsumme  $360^\circ$ . Also ist jeder Winkel des inneren Vierecks gleich  $\frac{360^\circ}{4} = 90^\circ$ . Sei  $x$  die Länge des Vektors  $\begin{pmatrix} a \\ b \end{pmatrix}$ . Dann hat das innere Viereck die Fläche  $x^2$ . Jedes der vier rechtwinkligen Dreiecke hat die Fläche  $\frac{ab}{2}$ .



Das innere Viereck und die vier rechtwinkligen Dreiecke ergeben zusammen die Fläche des großen Quadrats mit der Seitenlänge  $a + b$ , also gilt

$$x^2 + 4 \frac{ab}{2} = (a + b)^2.$$

Das heißt

$$x^2 + 2ab = a^2 + 2ab + b^2,$$

also

$$x^2 = a^2 + b^2.$$

Mit diesem Zusammenhang, dem Satz des Pythagoras (Pythagoras von Samos, 6. Jh. v. Chr), können wir die Länge  $x$  des Vektors  $\begin{pmatrix} a \\ b \end{pmatrix}$  ausrechnen.

Wir kürzen die Länge des Vektors  $\begin{pmatrix} a \\ b \end{pmatrix}$  mit  $\| \begin{pmatrix} a \\ b \end{pmatrix} \|$  ab. Es gilt dann

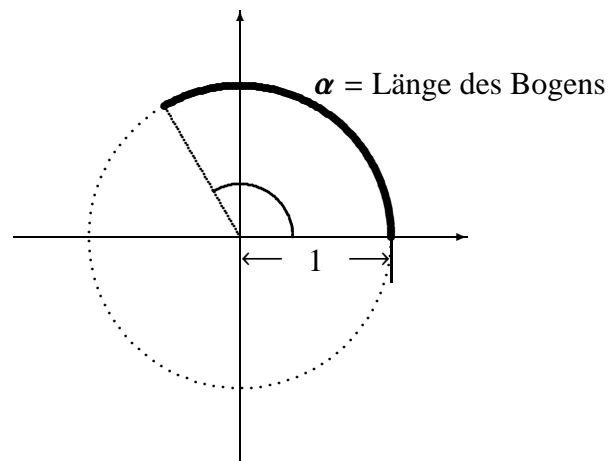
$$\| \begin{pmatrix} a \\ b \end{pmatrix} \| = \sqrt{a^2 + b^2}.$$

#### 4. Trigonometrie

In der *Trigonometrie* geht es darum, wie man – rechnerisch – aus den gegebenen Seitenlängen und Winkeln eines Dreiecks die restlichen Seitenlängen und Winkel bestimmen kann. Wenn man etwa von einem Dreieck die Längen der drei Seiten kennt, dann ist das Dreieck dadurch eindeutig bestimmt: die Winkel des Dreiecks sind also durch die Längen der drei Seiten festgelegt. (Wie konstruiert man ein Dreieck, das durch die drei Seitenlängen gegeben ist?) Ebenso ist ein Dreieck dadurch bestimmt, dass man eine Seite und die beiden daran anliegenden Winkel kennt. (Wie konstruiert man dieses Dreieck?) Uns geht es jetzt darum, die fehlenden Seitenlängen und Winkel auszurechnen. Dabei geht man so vor:

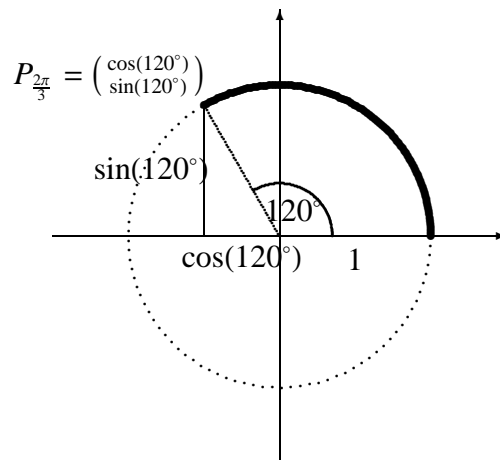
- (1) Man tabelliert den Zusammenhang zwischen den Seitenlängen und den Winkeln für rechtwinkelige Dreiecke. Dazu braucht man die *Winkelfunktionen*  $\sin$  (Sinus) und  $\cos$  (Cosinus).
- (2) Man baut sich alle anderen Dreiecke aus rechtwinkligen Dreiecken zusammen. Da dieses Zusammenbauen aber immer gleich funktioniert, macht man es einmal für alle Dreiecke. Man gewinnt so zwei Zusammenhänge zwischen Seitenlängen und Winkeln eines Dreiecks: den *Cosinussatz* und den *Sinus-satz*. Diese beiden Sätze reichen aus, um alle trigonometrischen Probleme zu lösen.

**4.1. Winkel.** Winkel misst man nicht nur in Grad ( $^\circ$ ), sondern auch in *Radian* (rad). Dabei wird der Winkel durch die Länge des zugehörigen Bogens am Einheitskreis, dem Kreis mit Radius 1, angegeben.



Dabei entsprechen  $180^\circ$  dem Winkel  $\pi$  rad. Demzufolge ist  $1^\circ = \frac{\pi}{180}$  rad, und  $1 \text{ rad} \approx 57.2958^\circ$ .

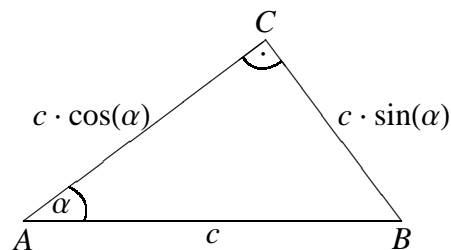
## 4.2. Winkelfunktionen.



Gegeben ist ein Winkel  $x$ . Der auf dem Kreis mit Mittelpunkt  $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$  und Radius 1 liegende Punkt  $P_x$  hat dann die Koordinaten  $\begin{pmatrix} \cos(x) \\ \sin(x) \end{pmatrix}$ . Nach dem Satz des Pythagoras gilt für jeden Winkel  $x$ :

$$(\sin(x))^2 + (\cos(x))^2 = 1.$$

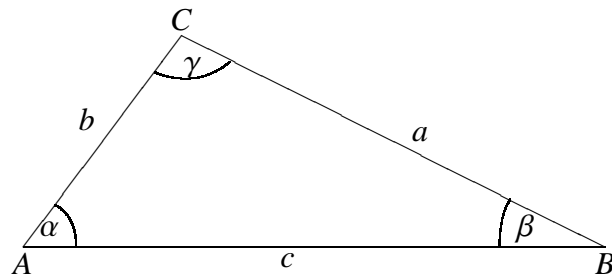
In einem rechtwinkligen Dreieck heißt die dem rechten Winkel gegenüberliegende Seite auch *Hypotenuse*, die beiden dem rechten Winkel anliegenden Seiten heißen *Katheten*.



### ÜBUNGSAUFGABEN 1.1.

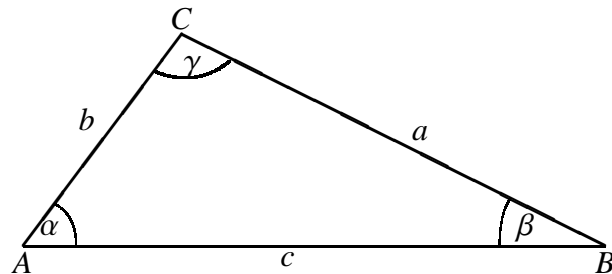
- (1) Ein Kletterer kann Wände mit einer Neigung von maximal  $65^\circ$  besteigen. Schafft er eine Pyramide mit einer quadratischen Grundfläche von  $784 \text{ m}^2$  und einer Höhe von  $40 \text{ m}$ ?

**4.3. Zusammenhang zwischen Seitenlängen und Winkeln eines Dreiecks.** Wir sagen, dass drei Punkte ein *Dreieck* bilden, wenn sie nicht alle drei auf einer Geraden liegen. In einem Dreieck bezeichnet man oft die Längen der Seiten mit  $a, b, c$ , und den der Seite mit Länge  $a$  gegenüber liegenden Winkel mit  $\alpha$ , den der Seite mit Länge  $b$  gegenüber liegenden Winkel mit  $\beta$ , und den der Seite mit Länge  $c$  gegenüber liegenden Winkel mit  $\gamma$ . Die Seiten sind üblicherweise *gegen den Uhrzeigersinn* mit  $a, b, c$  beschriftet.



Der Cosinussatz löst folgendes Problem:

- Gegeben: Seitenlängen  $a, b$  eines Dreiecks und der eingeschlossene Winkel  $\gamma$ .
- Gesucht: Die fehlende Seitenlänge  $c$ .



Wir betrachten zunächst den Fall  $\gamma \leq 90^\circ, \alpha \leq 90^\circ$ . Wir zeichnen in ein solches Dreieck die Höhe auf  $b$  und erhalten aus dem Satz des Pythagoras:

$$c^2 = (b - a \cos(\gamma))^2 + (a \sin(\gamma))^2,$$

also

$$\begin{aligned} c^2 &= b^2 - 2ab \cos(\gamma) + a^2(\cos(\gamma))^2 + a^2(\sin(\gamma))^2 \\ c^2 &= b^2 - 2ab \cos(\gamma) + a^2((\cos(\gamma))^2 + (\sin(\gamma))^2) \\ c^2 &= b^2 - 2ab \cos(\gamma) + 1a^2 \\ c^2 &= a^2 + b^2 - 2ab \cos(\gamma). \end{aligned}$$

Für den Fall  $\gamma \leq 90^\circ$  und  $\alpha > 90^\circ$  zeichnen wir die Höhe auf  $a$  und erhalten:

$$\begin{aligned} c^2 &= (a - b \cos(\gamma))^2 + (b \sin(\gamma))^2 \\ c^2 &= a^2 - 2ba \cos(\gamma) + b^2(\cos(\gamma))^2 + b^2(\sin(\gamma))^2 \\ c^2 &= a^2 - 2ba \cos(\gamma) + b^2((\cos(\gamma))^2 + (\sin(\gamma))^2) \\ c^2 &= a^2 - 2ba \cos(\gamma) + 1b^2 \\ c^2 &= a^2 + b^2 - 2ab \cos(\gamma). \end{aligned}$$



Zuletzt betrachten wir den Fall  $\gamma > 90^\circ$ . Wir zeichnen in ein solches Dreieck die Höhe auf  $b$  und erhalten:

$$\begin{aligned} c^2 &= (b + a \cos(180^\circ - \gamma))^2 + (a \sin(180^\circ - \gamma))^2 \\ c^2 &= (b - a \cos(\gamma))^2 + (a \sin(\gamma))^2 \\ c^2 &= b^2 - 2ab \cos(\gamma) + a^2(\cos(\gamma))^2 + a^2(\sin(\gamma))^2 \\ c^2 &= b^2 - 2ab \cos(\gamma) + a^2((\cos(\gamma))^2 + (\sin(\gamma))^2) \\ c^2 &= b^2 - 2ab \cos(\gamma) + 1a^2 \\ c^2 &= a^2 + b^2 - 2ab \cos(\gamma). \end{aligned}$$

Insgesamt haben wir folgenden Satz bewiesen:

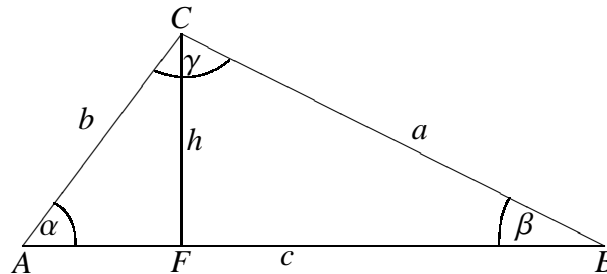
**SATZ 1.2 (Cosinussatz).** *Wir bezeichnen die Längen der Seiten eines Dreiecks mit  $a$ ,  $b$ ,  $c$ , und wir bezeichnen den der Seite mit Länge  $c$  gegenüber liegenden Winkel mit  $\gamma$ . Dann gilt*

$$c^2 = a^2 + b^2 - 2ab \cos(\gamma).$$

Man findet mit dem Cosinussatz  $\gamma$ , wenn  $a$ ,  $b$  und  $c$  gegeben sind. Zu jedem  $y \in [-1, 1]$  gibt es genau ein  $x \in [0, \pi]$ , sodass  $\cos(x) = y$ .

**4.4. Der Sinussatz.** Der Sinussatz löst folgendes Problem:

- Gegeben:  $\alpha, \beta, a$ .
- Gesucht:  $b$ .



Wir betrachten das rechtwinklige Dreieck  $AFC$  und erhalten

$$h = b \sin(\alpha).$$

Mit dem Dreieck  $FBC$  finden wir

$$h = a \sin(\beta).$$

Es gilt also  $b \sin(\alpha) = a \sin(\beta)$ . Sowohl  $\sin(\alpha)$  also auch  $\sin(\beta)$  sind ungleich 0, da in einem Dreieck kein Winkel  $0^\circ$  oder  $180^\circ$  sein kann. (Wir haben Dreiecke so definiert, dass die drei Punkte nicht auf einer Geraden liegen.) Es gilt also

$$\frac{a}{\sin(\alpha)} = \frac{b}{\sin(\beta)}.$$

Wenn man die gleiche Überlegung mit der Höhe auf  $a$  macht, erhält man  $\frac{b}{\sin(\beta)} = \frac{c}{\sin(\gamma)}$ .

**SATZ 1.3 (Sinussatz).** *Wir bezeichnen die Längen der Seiten eines Dreiecks mit  $a, b, c$ , den der Seite mit Länge  $a$  gegenüber liegenden Winkel mit  $\alpha$ , den der Seite mit Länge  $b$  gegenüber liegenden Winkel mit  $\beta$ , und den der Seite mit Länge  $c$  gegenüber liegenden Winkel mit  $\gamma$ . Sei  $d$  der Durchmesser des Umkreises des Dreiecks. Dann gilt:*

$$\frac{a}{\sin \alpha} = \frac{b}{\sin \beta} = \frac{c}{\sin \gamma} = d.$$

Wir überlegen uns jetzt, wie man Sinus- und Cosinussatz benutzen kann, um die fehlenden Winkel und Seitenlängen eines Dreiecks zu berechnen. In den Dreiecken der folgenden Beispiele bezeichnen wir die Längen der Seiten mit  $a, b, c$ , und wir bezeichnen den der Seite mit Länge  $a$  gegenüber liegenden Winkel mit  $\alpha$ , den der Seite mit Länge  $b$  gegenüber liegenden Winkel mit  $\beta$ , und den der Seite mit Länge  $c$  gegenüber liegenden Winkel mit  $\gamma$ . Die Seiten seien dabei *gegen den Uhrzeigersinn* mit  $a, b, c$  beschriftet.

- (1) *Es sind die Seitenlängen  $a, b, c$  gegeben:* Es gibt so ein Dreieck, wenn  $a < b + c$ ,  $b < a + c$ , und  $c < a + b$ . Der Winkel  $\alpha$  ist dann durch

$$a^2 = b^2 + c^2 - 2bc \cos(\alpha)$$

eindeutig bestimmt.

- (2) *Es sind eine Seitenlänge und zwei Winkel gegeben:* Da die Winkelsumme  $180^\circ$  ist, kennt man tatsächlich alle drei Winkel. Sind also  $c, \alpha$ , und  $\beta$  gegeben, so gibt es so ein Dreieck, wenn  $\alpha + \beta < \pi$ . Man berechnet  $\gamma = \pi - \alpha - \beta$ , und dann  $a$  und  $b$  mithilfe des Sinussatzes.
- (3) *Es sind zwei Seitenlängen und der eingeschlossene Winkel gegeben:* Es sind also zum Beispiel  $b, c$ , und  $\alpha$  gegeben. Wenn  $b$  und  $c$  positive reelle Zahlen sind, und  $0 < \alpha < \pi$  gilt, so gibt es sicher ein solches Dreieck. Man berechnet dann  $a$  mithilfe des Cosinussatzes; dann kennt man alle drei Seitenlängen und kann mit dem Cosinussatz die verbleibenden Winkel ausrechnen.
- (4) *Es sind zwei Seitenlängen gegeben, und ein Winkel, der nicht der von diesen Seiten eingeschlossene Winkel ist:* Es sind also zum Beispiel  $c, \alpha$  und  $a$  gegeben. In diesem Fall kann es sein, dass es gar kein, genau ein oder genau zwei Dreiecke mit dem vorgegebenen  $c, \alpha$  und  $a$  gibt. Es gibt mehrere Fälle:

(a) *Es gilt  $\alpha < 90^\circ$ :*

- (i) *Es gilt  $a \geq c$ :* Es gibt genau ein Dreieck. Wir erhalten  $b$  als die einzige positive Lösung von

$$c^2 + x^2 - 2cx \cos(\alpha) = a^2.$$

Es gilt also

$$b = c \cos(\alpha) + \sqrt{(c \cos(\alpha))^2 + a^2 - c^2}.$$

- (ii) *Es gilt  $c \sin(\alpha) < a < c$* : Es gibt genau zwei Dreiecke. Wir erhalten die beiden Möglichkeiten für  $b$  als die Lösungen der Gleichung

$$c^2 + x^2 - 2cx \cos(\alpha) = a^2,$$

also

$$b_{1,2} = c \cos(\alpha) \pm \sqrt{a^2 - (c \sin(\alpha))^2}.$$

- (iii) *Es gilt  $a = c \sin(\alpha)$* : Es gibt genau ein Dreieck. Wir erhalten  $\gamma = \frac{\pi}{2}$  und  $b = c \cos(\alpha)$ .

- (iv) *Es gilt  $a < c \sin(\alpha)$* : Es gibt kein Dreieck.

- (b) *Es gilt  $\alpha = 90^\circ$* :

- (i) *Es gilt  $a > c$* : Es gibt genau ein Dreieck, und

$$b^2 = a^2 - c^2$$

nach dem Satz des Pythagoras.

- (ii) *Es gilt  $a \leq c$* : Es gibt kein Dreieck.

- (c) *Es gilt  $\alpha > 90^\circ$* :

- (i) *Es gilt  $a > c$* : Es gibt ein Dreieck. Die Länge  $b$  ist die einzige positive Lösung von

$$c^2 + x^2 - 2cx \cos(\alpha) = a^2,$$

also

$$b = c \cos(\alpha) + \sqrt{(c \cos(\alpha))^2 + a^2 - c^2}.$$

- (ii) *Es gilt  $a \leq c$* : Es gibt kein Dreieck. Tückischerweise kann die Gleichung

$$c^2 + x^2 - 2cx \cos(\alpha) = a^2$$

trotzdem positive Lösungen haben.

#### ÜBUNGS-AUFGABEN 1.4.

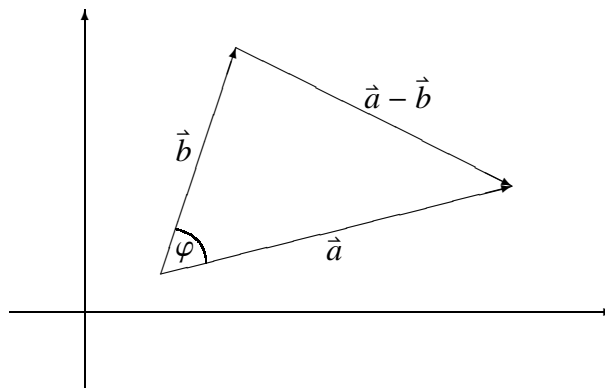
Wir bezeichnen die Längen der Seiten eines Dreiecks mit  $a, b, c$ , und wir bezeichnen den der Seite mit Länge  $a$  gegenüber liegenden Winkel mit  $\alpha$ , den der Seite mit Länge  $b$  gegenüber liegenden Winkel mit  $\beta$ , und den der Seite mit Länge  $c$  gegenüber liegenden Winkel mit  $\gamma$ . (Die Seiten seien dabei *gegen den Uhrzeigersinn* mit  $a, b, c$  beschriftet.)

- (1) Berechnen Sie  $\sin(\gamma)$  für ein Dreieck mit  $c = 10$ ,  $b = \frac{10}{\sqrt{3}}$ ,  $\beta = 30^\circ$ . Das Dreieck ist mit diesen drei Bestimmungsstücken  $c, b, \beta$  noch nicht eindeutig festgelegt. Warum nicht?
  - (2) Wie groß kann  $b$  in einem Dreieck mit  $\alpha = 45^\circ$ ,  $c = 1$ ,  $a = \frac{c}{\sqrt{6}}$  sein? (Gibt es mehr als eine Lösung?)
  - (3) Geben Sie eine Wahl von  $a$  an, sodass es genau ein Dreieck mit den Bestimmungsstücken  $\alpha = 45^\circ$ ,  $c = 1$ , und Ihrem gewählten  $a$  gibt!
  - (4) Von einem Dreieck  $ABC$  haben Sie folgende Information:  $\overline{AB} = 10$  cm, der Winkel  $\alpha$  zwischen  $AB$  und  $AC$  ist  $30^\circ$ ,  $\overline{BC} = \frac{10}{\sqrt{2}}$  cm.
    - (a) Stellen Sie diese Daten in einer Skizze dar.
    - (b) Welchen Winkel schließen  $CB$  und  $CA$  ein? Gibt es mehr als eine Lösung?
- Berechnen Sie in den folgenden Beispielen jeweils die nicht angegebenen Seitenlängen und Winkel.
- (5)
    - (a)  $c = 4$ ,  $b = 5$ ,  $a = 3$ .
    - (b)  $c = 4$ ,  $b = 5$ ,  $a = 10$ .
  - (6)
    - (a)  $c = 5$ ,  $b = 3$ ,  $\alpha = \frac{\pi}{4}$ .
    - (b) Gibt es für jede Wahl von  $c > 0$ ,  $b > 0$ ,  $\alpha$  mit  $0 < \alpha < \pi$  ein Dreieck mit den gewählten Bestimmungsstücken?

- (7) (a)  $c = 5, b = 10, \beta = \frac{\pi}{6}$ .  
 (b)  $c = 5, b = 3, \beta = \frac{\pi}{6}$ .
- (8) (a)  $c = 5, b = \frac{5}{2}, \beta = \frac{\pi}{6}$ .  
 (b)  $c = 5, b = 2, \beta = \frac{\pi}{6}$ .
- (9) (a)  $c = 5, b = 3, \beta = \frac{5\pi}{6}$ .  
 (b)  $c = 5, b = 10, \beta = \frac{5\pi}{6}$ .  
 (c)  $c = 4, b = 5, \beta = \frac{\pi}{2}$ .
- (10) Fassen Sie Ihre Beobachtungen aus den letzten Beispielen zusammen: Unter welchen Voraussetzungen an  $c, b, \beta$  gibt es
- gar kein Dreieck
  - genau ein Dreieck
  - genau zwei Dreiecke
  - mehr als zwei Dreiecke
- mit den Bestimmungsstücken  $c > 0, b > 0, \beta \in ]0, \pi[$ ?
- (11) (a)  $c = 5, \alpha = \frac{3\pi}{4}, \beta = \frac{\pi}{8}$ .  
 (b)  $c = 5, \alpha = \frac{3\pi}{4}, \beta = \frac{\pi}{4}$ .  
 (c)  $c = 5, \alpha = \frac{3\pi}{4}, \beta = \frac{\pi}{2}$ .
- (12) Fassen Sie Ihre Beobachtung aus dem letzten Beispiel zusammen: Unter welchen Voraussetzungen an  $c, \alpha, \beta$  gibt es
- gar kein Dreieck
  - genau ein Dreieck
  - genau zwei Dreiecke
  - mehr als zwei Dreiecke
- mit den Bestimmungsstücken  $c, \alpha, \beta$ ?
- (13) Bestimmen Sie  $b$  für alle Dreiecke mit  $c = 4, \alpha = 60^\circ, a = \sqrt{13}$ .
- (14) Bestimmen Sie ein  $a$ , sodass es kein Dreieck mit  $c = 4, \alpha = 60^\circ$  und Ihrem gewählten  $a$  gibt.
- (15) Bestimmen Sie ein  $a$ , sodass es *genau ein* Dreieck mit  $c = 4, \alpha = 60^\circ$  und Ihrem gewählten  $a$  gibt.
- (16) Bestimmen Sie  $c$  für alle Dreiecke mit  $a = 2, \beta = 45^\circ, b = \frac{4}{\sqrt{6}}$ .
- (17) Bestimmen Sie ein  $b$ , sodass es kein Dreieck mit  $a = 2, \beta = 45^\circ$  und Ihrem gewählten  $b$  gibt.
- (18) Bestimmen Sie ein  $b$ , sodass es *genau ein* Dreieck mit  $a = 2, \beta = 45^\circ$  und Ihrem gewählten  $b$  gibt.
- (19) Sie möchten die Entfernung eines Punktes  $B$  an einem Ufer eines Flusses zu einem Punkt  $C$  auf der anderen Seite des Flusses bestimmen. Dazu gehen Sie folgendermaßen vor: Sie messen an Ihrem Flussufer die Strecke von  $B$  zu einem weiteren Punkt  $A$  ab. Diese Strecke ist 500 m lang. Der Winkel zwischen  $BC$  und  $BA$  ist  $60^\circ$ , der Winkel zwischen  $AB$  und  $AC$  ist  $30^\circ$ .
- Stellen Sie diese Daten in einer Skizze dar.
  - Wie lang ist die Strecke  $BC$ ?
  - Um die Breite des Flusses zu bestimmen, wollen Sie wissen, wie weit  $C$  von der Strecke  $AB$  entfernt liegt. Bestimmen Sie dazu den Normalabstand von  $C$  auf die Gerade durch  $A$  und  $B$ .
- (20) Sie glauben dem italienischen Tourismusverband nicht und wollen selbst herausfinden, wie schief der Turm von Pisa ist. Dazu entfernen Sie sich in Neigerichtung des Turms 50 Meter vom Fußpunkt des Turms und blicken (vom Boden aus, damit Sie es später beim Rechnen einfacher haben) zur Turmspitze, welche nun unter einem Winkel  $\alpha$  erscheint. Sie stellen fest, dass  $\alpha$  genau  $47^\circ 12' 53''$  beträgt, und dass der Turm 45 m lang ist. Um wieviel Grad ist der Turm gegen die Vertikale geneigt?
- (21) Sie möchten die Entfernung eines Punktes  $A$  an einem Ufer eines Flusses zu einem Punkt  $B$  auf der anderen Seite bestimmen. Dazu können Sie folgendermaßen vorgehen: Messen Sie an Ihrem Flussufer die Strecke  $A$  zu einem Punkt  $C$  ab, und bestimmen Sie dann mit Hilfe eines Kompasses den Winkel  $\alpha$  zwischen der Strecke  $AB$  und  $AC$ , sowie den Winkel  $\gamma$  zwischen  $AC$  und  $CB$ . Was ergibt sich für die Entfernung  $AB$  bei  $AC = 27.5$  m und  $\alpha = 73^\circ, \gamma = 65^\circ$ ?
- (22) Sie verlassen eine gerade Straße, die die beiden Orte  $A$  und  $B$  verbindet, 20 km bevor Sie  $B$  erreichen und gehen geradeaus, bis es Ihnen nach 10 km keinen Spaß mehr macht. Dann drehen Sie sich um  $30^\circ$  nach rechts und erblicken nun den Ort  $B$  gerade vor sich. Wie weit müssen Sie jetzt noch wandern, um nach  $B$  zu gelangen, wenn Sie jetzt den geraden Weg nach  $B$  einschlagen?

## 5. Der Winkel zwischen zwei Vektoren

Wir berechnen den Winkel, den die Vektoren  $\vec{a} = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}$  und  $\vec{b} = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$  miteinander einschließen. Dazu nehmen wir an, dass keiner der beiden Vektoren der Nullvektor ist.



Für den eingeschlossenen Winkel  $\varphi$  gilt nach dem Cosinussatz:

$$\|b - a\|^2 = \|\vec{a}\|^2 + \|\vec{b}\|^2 - 2 \|\vec{a}\| \|\vec{b}\| \cos(\varphi).$$

Diese Formel können wir vereinfachen:

$$2 \cdot \|\vec{a}\| \cdot \|\vec{b}\| \cdot \cos(\varphi) = -(\|\vec{b} - \vec{a}\|^2) + \|\vec{a}\|^2 + \|\vec{b}\|^2$$

$$2 \cdot \|\vec{a}\| \cdot \|\vec{b}\| \cdot \cos(\varphi) = -((b_1 - a_1)^2 + (b_2 - a_2)^2) + (a_1^2 + a_2^2) + (b_1^2 + b_2^2)$$

$$2 \cdot \|\vec{a}\| \cdot \|\vec{b}\| \cdot \cos(\varphi) = -(b_1^2 - 2 a_1 b_1 + a_1^2) - (b_2^2 - 2 a_2 b_2 + a_2^2) + a_1^2 + a_2^2 + b_1^2 + b_2^2$$

$$2 \cdot \|\vec{a}\| \cdot \|\vec{b}\| \cdot \cos(\varphi) = 2 a_1 b_1 + 2 a_2 b_2$$

$$\|\vec{a}\| \cdot \|\vec{b}\| \cdot \cos(\varphi) = a_1 b_1 + a_2 b_2.$$

Wir erhalten

$$\cos(\varphi) = \frac{a_1 b_1 + a_2 b_2}{\|\vec{a}\| \cdot \|\vec{b}\|}.$$

Die Zahl  $a_1 b_1 + a_2 b_2$  bezeichnet man als das *Skalarprodukt* von  $\vec{a}$  und  $\vec{b}$ , und man kürzt es mit  $\langle \vec{a}, \vec{b} \rangle$  ab.

$$\langle \vec{a}, \vec{b} \rangle = \left\langle \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}, \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \right\rangle = a_1 \cdot b_1 + a_2 \cdot b_2.$$

Die Winkelformel heißt jetzt:

$$\cos(\varphi) = \frac{\langle \vec{a}, \vec{b} \rangle}{\|\vec{a}\| \cdot \|\vec{b}\|}.$$

Außerdem gilt für jeden Vektor  $\vec{a}$

$$\langle \vec{a}, \vec{a} \rangle = (\|\vec{a}\|)^2.$$

```
In[6]:= {3, 4} . {-5, 2}
```

```
Out[6]= -7
```

```
In[7]:= Laenge [v_] := Sqrt [v.v]
```

```
In[8]:= Laenge [{2, 3}]
```

```
Out[8]= Sqrt[13]
```

Unter Verwendung der Mathematica-Funktion `Norm` kann man diese Länge auch mit `Norm[ { 2, 3 } ]` ausrechnen.

**DEFINITION 1.5.** Seien  $\vec{a}, \vec{b} \in \mathbb{R}^2$ . Die Vektoren  $\vec{a}$  und  $\vec{b}$  stehen aufeinander normal, wenn  $\langle \vec{a}, \vec{b} \rangle = 0$ .

Zwei Vektoren stehen also aufeinander normal, wenn einer von ihnen der Nullvektor ist, oder wenn sie einen rechten Winkel einschließen. Damit erhält man, dass (wenn  $\begin{pmatrix} a \\ b \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ ) der Vektor  $\begin{pmatrix} a \\ b \end{pmatrix}$  mit den Vektoren  $\begin{pmatrix} b \\ -a \end{pmatrix}$  und  $\begin{pmatrix} -b \\ a \end{pmatrix}$  einen rechten Winkel einschließt.

### ÜBUNGSAUFGABEN 1.6.

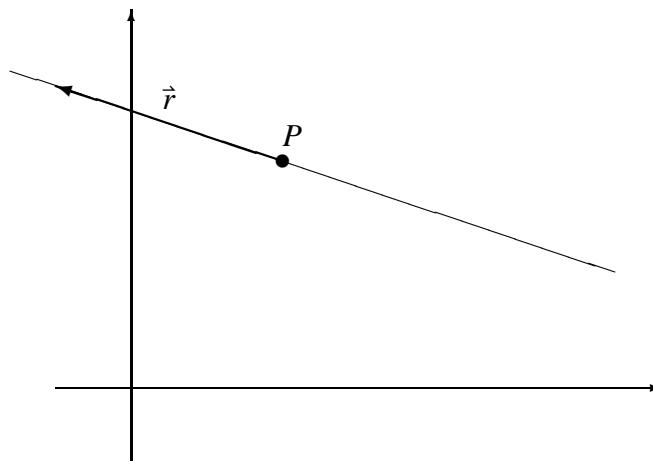
- (1) Von einem gleichschenkeligen Dreieck sind zwei Basiseckpunkte  $\begin{pmatrix} -2 \\ 3 \end{pmatrix}$  und  $\begin{pmatrix} 4 \\ 11 \end{pmatrix}$  bekannt. Ergänzen Sie diese Punkte mit einer Spitze, sodaß das entstehende Dreieck die Höhe 5 besitzt. Wie viele verschiedene Lösungen gibt es? (Sie brauchen nur eine wirklich auszurechnen.)
- (2) Berechnen Sie den Cosinus des Winkels zwischen  $x$  und  $y$  für  $x = \begin{pmatrix} 3 \\ 2 \end{pmatrix}$ ,  $y = \begin{pmatrix} -6 \\ -4 \end{pmatrix}$ .
- (3) Berechnen Sie jeweils den Winkel zwischen folgenden beiden Vektoren. Geben Sie die Ergebnisse in Grad und in Radiant an!
  - (a)  $a = \begin{pmatrix} 3 \\ 2 \end{pmatrix}$ ,  $b = \begin{pmatrix} -3 \\ 2 \end{pmatrix}$ .
  - (b)  $a = \begin{pmatrix} 3 \\ 4 \end{pmatrix}$ ,  $b = \begin{pmatrix} 4 \\ -3 \end{pmatrix}$ .
  - (c)  $a = \begin{pmatrix} 3 \\ 4 \end{pmatrix}$ ,  $b = \begin{pmatrix} 6 \\ 8 \end{pmatrix}$ .
  - (d)  $a = \begin{pmatrix} 3 \\ 4 \end{pmatrix}$ ,  $b = \begin{pmatrix} -9 \\ -12 \end{pmatrix}$ .
- (4) Zeigen Sie, dass das Skalarprodukt im  $\mathbb{R}^2$  folgende Eigenschaften erfüllt:
  - (a)  $\langle a + b, a + b \rangle = \langle a, a \rangle + 2\langle a, b \rangle + \langle b, b \rangle$ .
  - (b)  $\langle a + b, a - b \rangle = \langle a, a \rangle - \langle b, b \rangle$ .
- (5) Verwenden Sie das Skalarprodukt, um folgenden geometrischen Satz zu beweisen.  
In einem Parallelogramm mit Seitenlängen  $a, b$ , und Diagonalenlängen  $e, f$  gilt:

$$2(a^2 + b^2) = e^2 + f^2.$$

## 6. Geraden in der Ebene

Wir überlegen uns, wie man Geraden in der Ebene beschreiben kann.

### 6.1. Geraden, die durch einen Punkt und eine Richtung gegeben sind.



$$P = \begin{pmatrix} 2 \\ 3 \end{pmatrix}, \vec{r} = \begin{pmatrix} -3 \\ 1 \end{pmatrix}.$$

Die Gerade  $g$  ist die Menge aller Punkte, die man erreicht, indem man von  $P$  ein Stück in Richtung  $\vec{r}$  geht.

$$g = \{P + \lambda \cdot \vec{r} \mid \lambda \in \mathbb{R}\}.$$

Lies: "g ist gleich der Menge aller Punkte  $P + \lambda$  mal  $\vec{r}$ , wobei  $\lambda$  eine reelle Zahl ist." Mit den Zahlen für  $P$  und  $\vec{r}$ :

$$g = \left\{ \begin{pmatrix} 2 \\ 3 \end{pmatrix} + \lambda \cdot \begin{pmatrix} -3 \\ 1 \end{pmatrix} \mid \lambda \in \mathbb{R} \right\},$$

oder, anders geschrieben,

$$g = \left\{ \begin{pmatrix} 2-3\lambda \\ 3+\lambda \end{pmatrix} \mid \lambda \in \mathbb{R} \right\}.$$

Man kann  $g$  auch so schreiben:

$$g = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2 \mid \text{es gibt } \lambda \in \mathbb{R}, \text{ sodass } \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2 \\ 3 \end{pmatrix} + \lambda \cdot \begin{pmatrix} -3 \\ 1 \end{pmatrix} \right\}.$$

Lies: "g ist gleich der Menge aller Punkte  $\begin{pmatrix} x \\ y \end{pmatrix}$  in  $\mathbb{R}^2$ , für die es ein  $\lambda$  in den reellen Zahlen gibt, sodass  $\begin{pmatrix} x \\ y \end{pmatrix}$  gleich  $\begin{pmatrix} 2 \\ 3 \end{pmatrix} + \lambda$  mal  $\begin{pmatrix} -3 \\ 1 \end{pmatrix}$  ist." Diese Darstellung von  $g$  durch *Punkt* und *Richtungsvektor* heißt *Parameterdarstellung der Geraden*  $g$ . Man schreibt oft kurz:

$$g : \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2 \\ 3 \end{pmatrix} + \lambda \cdot \begin{pmatrix} -3 \\ 1 \end{pmatrix}$$

oder

$$g : X = \begin{pmatrix} 2 \\ 3 \end{pmatrix} + \lambda \cdot \begin{pmatrix} -3 \\ 1 \end{pmatrix}.$$

Wir überprüfen, ob der Punkt  $\begin{pmatrix} -4 \\ 5 \end{pmatrix}$  auf der Geraden  $g$  liegt. Er liegt auf  $g$ , falls es eine reelle Zahl  $\lambda$  gibt, sodass  $\begin{pmatrix} -4 \\ 5 \end{pmatrix}$  gleich  $\begin{pmatrix} 2 \\ 3 \end{pmatrix} + \lambda \cdot \begin{pmatrix} -3 \\ 1 \end{pmatrix}$  ist. Wir suchen also ein  $\lambda \in \mathbb{R}$ , das die Gleichungen

$$\begin{aligned} -4 &= 2 - 3\lambda & \text{I} \\ 5 &= 3 + 1\lambda & \text{II} \end{aligned}$$

erfüllt. Aus der Gleichung I erhalten wir  $\lambda = 2$ ; da auch  $5 = 3 + 1 \cdot 2$  gilt, ist  $\lambda = 2$  eine Lösung des Gleichungssystems. Daher liegt der Punkt  $\begin{pmatrix} -4 \\ 5 \end{pmatrix}$  auf  $g$ ; wir schreiben dafür

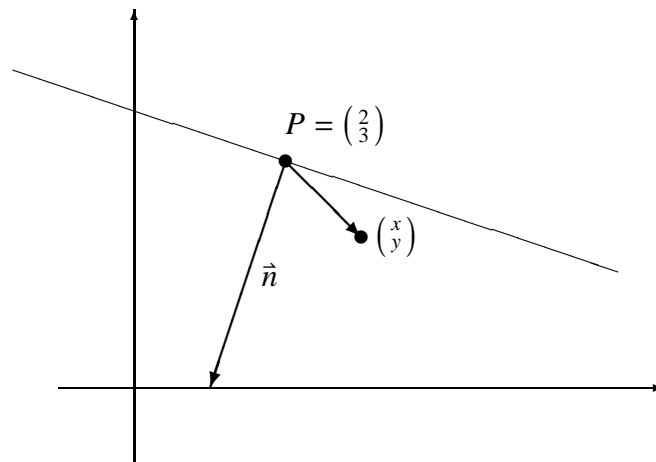
$$\begin{pmatrix} -4 \\ 5 \end{pmatrix} \in g.$$

**6.2. Geraden, die durch eine Gleichung gegeben sind.** Wir haben im letzten Beispiel überprüft, ob ein Punkt auf einer Geraden liegt. Dabei war die Gerade in Parameterform gegeben. Zur Überprüfung war es notwendig, festzustellen, ob es einen Wert für den Parameter  $\lambda$  gibt, der uns genau den getesteten Punkt liefert. Wir mussten also für jeden Punkt ein Gleichungssystem (mit zwei Gleichungen und einer Variable) lösen.

Wir testen nun wieder, ob  $\begin{pmatrix} x \\ y \end{pmatrix}$  auf der Geraden  $g$  liegt, die durch

$$g : X = \begin{pmatrix} 2 \\ 3 \end{pmatrix} + \lambda \cdot \begin{pmatrix} -3 \\ 1 \end{pmatrix}$$

gegeben ist.



Anstatt zu fragen, ob  $\begin{pmatrix} x \\ y \end{pmatrix}$  auf  $g$  liegt, fragen wir, ob  $\begin{pmatrix} x \\ y \end{pmatrix} - \begin{pmatrix} 2 \\ 3 \end{pmatrix}$  normal auf  $\vec{n}$  steht. Das ist nämlich genau für die Punkte  $\begin{pmatrix} x \\ y \end{pmatrix}$  auf  $g$  der Fall. Zunächst finden wir den Vektor  $\vec{n}$ . Auf den Vektor  $\begin{pmatrix} a \\ b \end{pmatrix}$  steht immer der Vektor  $\begin{pmatrix} -b \\ a \end{pmatrix}$  normal, denn das Skalarprodukt  $\langle \begin{pmatrix} a \\ b \end{pmatrix}, \begin{pmatrix} -b \\ a \end{pmatrix} \rangle$  ergibt  $-ab + ab = 0$ . Also finden wir  $\vec{n}$  durch

$$\vec{n} = \begin{pmatrix} -1 \\ -3 \end{pmatrix}.$$

Nun überprüfen wir, ob  $\begin{pmatrix} x \\ y \end{pmatrix} - \begin{pmatrix} 2 \\ 3 \end{pmatrix}$  normal auf  $\begin{pmatrix} -1 \\ -3 \end{pmatrix}$  steht. Das gilt genau dann, wenn

$$\langle \begin{pmatrix} x-2 \\ y-3 \end{pmatrix}, \begin{pmatrix} -1 \\ -3 \end{pmatrix} \rangle = 0.$$

Wir rechnen das Skalarprodukt aus und erhalten

$$-x - 3y + 11 = 0.$$

Ein Punkt  $\begin{pmatrix} x \\ y \end{pmatrix}$  liegt also genau dann auf der Geraden, wenn  $-x - 3y + 11 = 0$  ist. Wir können also jetzt viel einfacher überprüfen, ob ein Punkt auf der Geraden  $g$  liegt. Wir berechnen  $-x - 3y + 11$ . Ist das 0, so liegt der Punkt auf der Geraden, und sonst nicht. Außerdem können wir die Gerade jetzt kürzer angeben durch

$$g = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2 \mid -x - 3y = -11 \right\}$$

(lies: "g ist gleich der Menge aller  $\begin{pmatrix} x \\ y \end{pmatrix}$  in  $\mathbb{R}$  hoch 2, für die  $-x - 3y$  gleich  $-11$  ist.")  
Das kürzt man auch zu

$$g : -x - 3y = -11$$

ab.  $-x - 3y = -11$  heißt *Gleichung* der Geraden, diese Darstellung der Geraden *Gleichungsform* oder *implizite Darstellung* der Geraden.

### 6.3. Verwandlung zwischen Gleichungs- und Parameterform.

6.3.1. *Verwandlung von parametrisierter in implizite Darstellung.* Wir verwandeln  $g : X = \begin{pmatrix} 2 \\ 3 \end{pmatrix} + \lambda \cdot \begin{pmatrix} -3 \\ 1 \end{pmatrix}$  in  $g : -x - 3y = -11$  so, wie das in obigem Beispiel erklärt worden ist.



6.3.2. *Verwandlung von impliziter in parametrisierte Form.* Wir verwandeln  $g : 5x - 2y = 1$  in parametrisierte Form. Dazu setzen wir  $y := t$  und rechnen uns aus diesem  $y$  das  $x$  aus. Wir erhalten  $x = \frac{1}{5} + \frac{2}{5}t$ . Somit ist für jedes  $t \in \mathbb{R}$  der Punkt  $\begin{pmatrix} \frac{1}{5} + \frac{2}{5}t \\ t \end{pmatrix}$  ein Geradenpunkt. Die Gerade hat also die parametrisierte Darstellung

$$g : X = \begin{pmatrix} \frac{1}{5} \\ 0 \end{pmatrix} + t \cdot \begin{pmatrix} \frac{2}{5} \\ 1 \end{pmatrix}.$$

Eine andere Darstellung derselben Geraden ist

$$g : X = \begin{pmatrix} \frac{1}{5} \\ 0 \end{pmatrix} + t \cdot \begin{pmatrix} 2 \\ 5 \end{pmatrix},$$

oder

$$g : X = \begin{pmatrix} 1 \\ 2 \end{pmatrix} + t \cdot \begin{pmatrix} -22 \\ -55 \end{pmatrix}.$$

Spezialfall: Wir verwandeln  $g : y = -1$  in Parameterform. Dazu setzen wir  $x := t$ , und rechnen uns dann das  $y$  aus. Das ist aber immer  $-1$ . Für jedes  $t \in \mathbb{R}$  ist also  $\begin{pmatrix} t \\ -1 \end{pmatrix}$  ein Geradenpunkt. Die Gerade hat die parametrisierte Darstellung

$$g : X = \begin{pmatrix} 0 \\ -1 \end{pmatrix} + t \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

### ÜBUNGSAUFGABEN 1.7.

- (1) Geben Sie die Gerade durch die Punkte  $\begin{pmatrix} 3 \\ 2 \end{pmatrix}$  und  $\begin{pmatrix} 3 \\ -3 \end{pmatrix}$  in Parameterform und in impliziter Form an!
- (2) Bestimmen Sie jeweils eine Parameterform (= Punkt-Richtungs-Form) folgender Geraden.
  - (a)  $3x + 4y = 17$ .
  - (b)  $x = 1$ .
  - (c)  $y = -4$ .
- (3) Bestimmen Sie eine Gleichung, deren Lösungsmenge die Gerade

$$X = \begin{pmatrix} -3 \\ 6 \end{pmatrix} + \lambda \cdot \begin{pmatrix} -1 \\ 2 \end{pmatrix}$$

ist.

- (4) Bestimmen Sie die implizite Darstellung jener Geraden, die parallel zur Geraden  $g$  mit

$$g : X = \begin{pmatrix} 2 \\ -1 \end{pmatrix} + t \cdot \begin{pmatrix} 3 \\ -4 \end{pmatrix}$$

sind und von dieser Abstand 10 haben.

- (5) Ein Radfahrer startet im Punkt  $\begin{pmatrix} 2 \\ 3 \end{pmatrix}$  und fährt auf den Punkt  $\begin{pmatrix} 8 \\ 0 \end{pmatrix}$  zu. Ein Fußgänger startet im Punkt  $\begin{pmatrix} 4 \\ -3 \end{pmatrix}$  und geht auf den Punkt  $\begin{pmatrix} 4 \\ 10 \end{pmatrix}$  zu. In welchem Punkt schneiden sich die Wege der beiden?
- (6) Ein Radfahrer im Punkt  $\begin{pmatrix} 3 \\ 3 \end{pmatrix}$  und ein Fußgänger im Punkt  $\begin{pmatrix} 9 \\ -5 \end{pmatrix}$  bewegen sich aufeinander zu, der Radfahrer mit 20 km/h, der Fußgänger mit 5 km/h. Wann und wo treffen die beiden einander?
- (7) Vom Quadrat  $ABCD$  haben wir folgende Angaben:
  - $A = \begin{pmatrix} -1 \\ 2 \end{pmatrix}$ .
  - $B$  liegt auf der Geraden

$$g_B : X = \begin{pmatrix} -1 \\ 2 \end{pmatrix} + \lambda \cdot \begin{pmatrix} 4 \\ 3 \end{pmatrix}.$$

- Die Seitenlänge des Quadrats ist 10.
- Die Eckpunkte sind gegen den Uhrzeigersinn mit  $A, B, C, D$  beschriftet.

Berechnen Sie die Koordinaten des Eckpunktes  $C$ !

- (8) Vom Quadrat  $ABCD$  haben wir folgende Angaben:
  - $A = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$ .
  - $B$  liegt auf der Geraden

$$g_B : X = \begin{pmatrix} 1 \\ 2 \end{pmatrix} + \lambda \cdot \begin{pmatrix} 3 \\ -4 \end{pmatrix}.$$

- Die Seitenlänge des Quadrats ist 15.
- Die Eckpunkte sind gegen den Uhrzeigersinn mit  $A, B, C, D$  beschriftet.

Berechnen Sie die Koordinaten des Eckpunktes  $C$ !

- (9) Zeigen Sie, dass sich die Schwerlinien des Dreiecks  $ABC$  mit  $A = \begin{pmatrix} -2 \\ -1 \end{pmatrix}$ ,  $B = \begin{pmatrix} 5 \\ 1 \end{pmatrix}$  und  $C = \begin{pmatrix} 3 \\ 5 \end{pmatrix}$  in einem Punkt schneiden, und berechnen Sie diesen Schnittpunkt.

- (10) Berechnen Sie den Umkreismittelpunkt  $U = \begin{pmatrix} u_1 \\ u_2 \end{pmatrix}$  des Dreiecks  $ABC$  mit  $A = \begin{pmatrix} -2 \\ -1 \end{pmatrix}$ ,  $B = \begin{pmatrix} 5 \\ 1 \end{pmatrix}$  und  $C = \begin{pmatrix} 3 \\ 5 \end{pmatrix}$ , indem Sie die Bedingung, dass  $U$  gleich weit von  $A$ ,  $B$  und  $C$  entfernt ist, in Gleichungen in den Variablen  $u_1$  und  $u_2$  umwandeln. Verwenden Sie zur Lösung der auftretenden Gleichungen den Mathematica-Befehl `Solve`.
- (11) Bestimmen Sie die implizite Darstellung jener Geraden, die parallel zur Geraden  $g$  mit

$$g : X = \begin{pmatrix} 2 \\ 0 \end{pmatrix} + t \cdot \begin{pmatrix} 3 \\ -4 \end{pmatrix}$$

sind, und von dieser Abstand 10 haben.

- (12) Berechnen Sie den Durchschnitt der Geraden  $h$  und  $j$ , wobei

$$h : X = \begin{pmatrix} 1 \\ 2 \end{pmatrix} + t \cdot \begin{pmatrix} 2 \\ 5 \end{pmatrix}$$

und

$$j : 10x - 4y = 0.$$

- (13) Bestimmen Sie die Schnittmenge der Geraden

$$g_1 : X = \begin{pmatrix} 3 \\ 4 \end{pmatrix} + t \cdot \begin{pmatrix} -2 \\ 1 \end{pmatrix}$$

und

$$g_2 : 2x + 4y = 22.$$

- (14) Bestimmen Sie den Cosinus des Schnittwinkels der Geraden

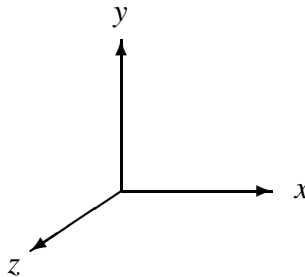
$$g_1 : X = \begin{pmatrix} 0 \\ 4 \end{pmatrix} + t \cdot \begin{pmatrix} 3 \\ 4 \end{pmatrix}$$

und

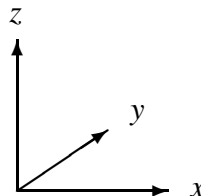
$$g_2 : 12x - 5y = 22.$$

## 7. Vektoren im $\mathbb{R}^n$

Bisher haben wir uns auf die Geometrie in der Ebene beschränkt. Analog kann man den Raum mit Tripeln reeller Zahlen, also mit Elementen aus  $\mathbb{R}^3$ , koordinatisieren. Die Konvention ist es, die Richtungen der Koordinatenachsen wie in folgenden Skizzen zu wählen:



oder



Hält man Daumen, Zeigefinger und Mittelfinger der rechten Hand so, dass sie paarweise im rechten Winkel aufeinander stehen, dann zeigen sie jeweils in die Richtung der positiven  $x$ -Achse,  $y$ -Achse und  $z$ -Achse.

Wir definieren die Operationen, die im  $\mathbb{R}^2$  hilfreich waren, allgemein für

$$\mathbb{R}^n := \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mid x_1, \dots, x_n \in \mathbb{R} \right\},$$

wobei  $n$  eine beliebige natürliche Zahl ist.

DEFINITION 1.8. Seien  $\vec{a} = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$ ,  $\vec{b} = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$  in  $\mathbb{R}^n$ . Wir definieren:

- (1)  $\vec{a} + \vec{b} := \begin{pmatrix} a_1+b_1 \\ \vdots \\ a_n+b_n \end{pmatrix}$ .
- (2)  $\lambda \vec{a} := \begin{pmatrix} \lambda a_1 \\ \vdots \\ \lambda a_n \end{pmatrix}$  für  $\lambda \in \mathbb{R}$ .
- (3)  $\langle \vec{a}, \vec{b} \rangle := a_1 \cdot b_1 + \dots + a_n \cdot b_n$  (Skalarprodukt).
- (4)  $\|\vec{a}\| := \sqrt{\langle \vec{a}, \vec{a} \rangle}$  (Länge).
- (5) Der Winkel  $\varphi$  zwischen  $\vec{a}$  und  $\vec{b}$  ist gegeben durch

$$\cos(\varphi) = \frac{\langle \vec{a}, \vec{b} \rangle}{\|\vec{a}\| \cdot \|\vec{b}\|}.$$

Im  $\mathbb{R}^3$  gibt es eine Rechenoperation, die einen Vektor liefert, der auf zwei gegebene Vektoren  $\vec{a}$  und  $\vec{b}$  normal steht: das Kreuzprodukt.

DEFINITION 1.9. Der Vektor

$$\begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} \times \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} := \begin{pmatrix} a_2 b_3 - a_3 b_2 \\ -(a_1 b_3 - a_3 b_1) \\ a_1 b_2 - a_2 b_1 \end{pmatrix}$$

ist das *Kreuzprodukt* von  $\begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix}$  und  $\begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix}$  in  $\mathbb{R}^3$ .

Für  $\vec{a} = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix}$  und  $\vec{b} = \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix}$  in  $\mathbb{R}^3$  gilt:

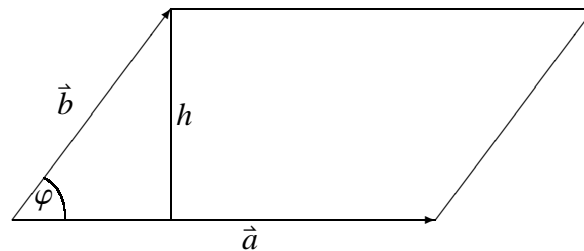
- (1)  $\vec{a} \times \vec{b}$  ist normal auf  $\vec{a}$  und auf  $\vec{b}$ .

Beweis: Es gilt

$$\langle \vec{a} \times \vec{b}, \vec{a} \rangle = (a_2 b_3 - a_3 b_2) a_1 - (a_1 b_3 - a_3 b_1) a_2 + (a_1 b_2 - a_2 b_1) a_3 = 0.$$

- (2)  $\|\vec{a} \times \vec{b}\|$  ist die Fläche des Parallelogramms, das von den Vektoren  $\vec{a}$  und  $\vec{b}$  aufgespannt wird.

Beweis:



Wir erhalten für die Höhe  $h$  auf  $\vec{a}$

$$h = \|\vec{b}\| \cdot \sin(\varphi)$$

und für den Flächeninhalt

$$F = \|\vec{a}\| \cdot h = \|\vec{a}\| \cdot \|\vec{b}\| \cdot \sin(\varphi).$$

Somit gilt

$$\begin{aligned} F^2 &= \|\vec{a}\|^2 \cdot \|\vec{b}\|^2 \cdot (\sin(\varphi))^2, \\ &= \|\vec{a}\|^2 \cdot \|\vec{b}\|^2 \cdot (1 - (\cos(\varphi))^2), \\ &= \|\vec{a}\|^2 \cdot \|\vec{b}\|^2 - \langle \vec{a}, \vec{b} \rangle^2. \end{aligned}$$

Einsetzen von  $\begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix}$  für  $\vec{a}$  und  $\begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix}$  für  $\vec{b}$  ergibt jetzt

$$F^2 = \|\vec{a} \times \vec{b}\|^2.$$

Durch diese beiden Bedingungen an Richtung und Länge ist der Vektor  $\vec{a} \times \vec{b}$  fast schon eindeutig bestimmt. Zusätzlich gilt: Zeigt der Daumen der rechten Hand in Richtung  $\vec{a}$ , der Zeigefinger in Richtung  $\vec{b}$ , und ist der Mittelfinger normal auf  $\vec{a}$  und  $\vec{b}$ , dann zeigt er in die Richtung von  $\vec{a} \times \vec{b}$ .

```
In[9]:= Kreuzprodukt[{a1_, a2_, a3_}, {b1_, b2_, b3_}] :=
      {a2 * b3 - a3 * b2, -(a1 * b3 - a3 * b1), a1 * b2 - a2 * b1}
```

```
In[10]:= Kreuzprodukt[{1, -2, 3}, {0, 2, -1}]
```

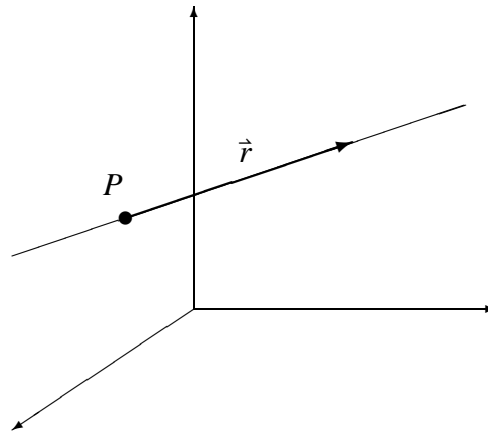
```
Out[10]= {-4, 1, 2}
```

Die Mathematica-Funktion `Cross` liefert ebenfalls das Kreuzprodukt.

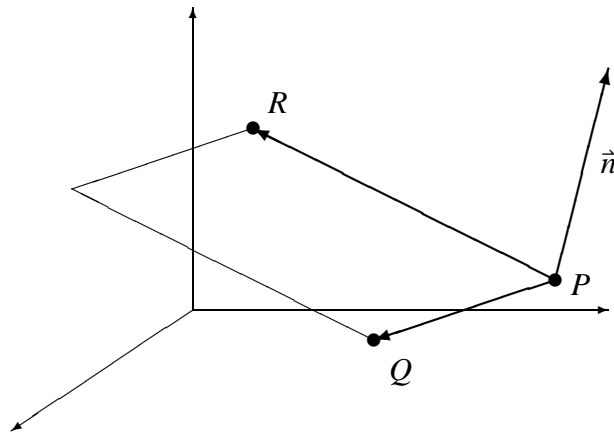
## 8. Geraden und Ebenen im Raum

**8.1. Parameterdarstellung einer Geraden.** Genau wie im  $\mathbb{R}^2$  lässt sich eine Gerade im  $\mathbb{R}^3$  durch eine Parameterdarstellung mit einem Punkt und einem Richtungsvektor angeben. Zum Beispiel,

$$g : \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 2 \\ 3 \\ -1 \end{pmatrix} + \lambda \cdot \begin{pmatrix} 1 \\ -1 \\ 3 \end{pmatrix}.$$



**8.2. Parameterdarstellung einer Ebene.** Wie kann man die Ebene  $e$  beschreiben, die die drei Punkte  $P = \begin{pmatrix} 2 \\ 3 \\ -1 \end{pmatrix}$ ,  $Q = \begin{pmatrix} 3 \\ 2 \\ 2 \end{pmatrix}$ , und  $R = \begin{pmatrix} 4 \\ 2 \\ -4 \end{pmatrix}$  enthält?



Die Ebene  $e$  ist die Menge aller Punkte, die man erreicht, indem man von  $P$  aus ein Stück in Richtung  $Q$ , und dann ein Stück in die Richtung von  $P$  nach  $R$  geht.

$$e = \{P + \lambda \cdot \vec{PQ} + \mu \cdot \vec{PR} \mid \lambda, \mu \in \mathbb{R}\},$$

das heißt, die Punkte der Ebene sind von der Form

$$e : \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 2 \\ 3 \\ -1 \end{pmatrix} + \lambda \cdot \begin{pmatrix} 1 \\ -1 \\ 3 \end{pmatrix} + \mu \cdot \begin{pmatrix} 2 \\ -1 \\ -3 \end{pmatrix}.$$

Eine Ebene lässt sich also durch einen Punkt und 2 Richtungsvektoren beschreiben.

**8.3. Implizite Darstellung einer Ebene.** Es sei  $e$  die Ebene durch den Punkt  $\begin{pmatrix} 2 \\ -1 \\ 4 \end{pmatrix}$ , die normal auf den Vektor  $\vec{n} = \begin{pmatrix} 1 \\ 3 \\ -2 \end{pmatrix}$  ist. Wir nennen  $\vec{n}$  den Normalvektor von  $e$ .

Die Ebene  $e$  ist die Menge aller Punkte  $\begin{pmatrix} x \\ y \\ z \end{pmatrix}$ , sodass der Vektor  $\begin{pmatrix} x \\ y \\ z \end{pmatrix} - \begin{pmatrix} 2 \\ -1 \\ 4 \end{pmatrix}$  normal auf  $\vec{n}$  ist, also

$$\left\langle \begin{pmatrix} x \\ y \\ z \end{pmatrix} - \begin{pmatrix} 2 \\ -1 \\ 4 \end{pmatrix}, \vec{n} \right\rangle = 0.$$

Einsetzen der Werte ergibt die *implizite Darstellung der Ebene*,

$$e = \left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathbb{R}^3 \mid x + 3y - 2z = -9 \right\}.$$

Ein Normalvektor von  $e$  lässt sich direkt aus den Koeffizienten der Ebenengleichung ablesen.

8.3.1. *Verwandlung von Parameterdarstellung in implizite Darstellung.* Wir verwandeln

$$e : \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 2 \\ 3 \\ -1 \end{pmatrix} + \lambda \cdot \begin{pmatrix} 1 \\ -1 \\ 3 \end{pmatrix} + \mu \cdot \begin{pmatrix} 2 \\ -1 \\ -3 \end{pmatrix}$$

in implizite Form. Dazu suchen wir zuerst einen Vektor  $\vec{n}$ , der auf beide Richtungsvektoren der Ebene normal ist. Dann ist  $\vec{n}$  auf die ganze Ebene normal. Wir beschreiben 2 Möglichkeiten einen solchen Normalvektor zu finden:

(1) Wir suchen  $\vec{n} = \begin{pmatrix} n_1 \\ n_2 \\ n_3 \end{pmatrix}$  so, dass

$$\begin{aligned} \left\langle \begin{pmatrix} 1 \\ -1 \\ 3 \end{pmatrix}, \vec{n} \right\rangle &= 0 \text{ und} \\ \left\langle \begin{pmatrix} 2 \\ -1 \\ -3 \end{pmatrix}, \vec{n} \right\rangle &= 0. \end{aligned}$$

Das heißt, wir müssen das lineare Gleichungssystem

$$\begin{aligned} n_1 - n_2 + 3n_3 &= 0 \\ 2n_1 - n_2 - 3n_3 &= 0 \end{aligned}$$

lösen. Klarerweise ist  $n_1 = n_2 = n_3 = 0$  eine Lösung, aber wir wollen einen Vektor  $\vec{n}$ , der nicht der Nullvektor ist. Wie man alle Lösungen eines linearen Gleichungssystems findet, werden wir im Kapitel 3 sehen.

(2) Alternativ finden wir  $\vec{n}$  auch als Kreuzprodukt der beiden Richtungsvektoren.

$$\vec{n} = \begin{pmatrix} 1 \\ -1 \\ 3 \end{pmatrix} \times \begin{pmatrix} 2 \\ -1 \\ -3 \end{pmatrix} = \begin{pmatrix} 6 \\ 9 \\ 1 \end{pmatrix}$$

Der Vektor  $\vec{n}$  ist normal auf die Ebene. Ein Punkt  $\begin{pmatrix} x \\ y \\ z \end{pmatrix}$  liegt also genau dann in  $e$ , wenn der Vektor  $\begin{pmatrix} x \\ y \\ z \end{pmatrix} - \begin{pmatrix} 2 \\ 3 \\ -1 \end{pmatrix}$  normal auf  $\vec{n}$  ist. Wir berechnen

$$\left\langle \begin{pmatrix} x \\ y \\ z \end{pmatrix} - \begin{pmatrix} 2 \\ 3 \\ -1 \end{pmatrix}, \vec{n} \right\rangle = 0$$

und erhalten

$$6x + 9y + z = 38.$$

Somit hat die Ebene  $e$  die implizite Darstellung

$$e = \left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathbb{R}^3 \mid 6x + 9y + z = 38 \right\}.$$

**8.3.2. Verwandlung von impliziter Darstellung in Parameterdarstellung.** Wir wandeln  $e : x + 3y - 2z = -9$  in parametrisierte Form. Wir beschreiben die Lösungsmenge der Gleichung, indem wir  $z = \mu$  und  $y = \lambda$  setzen und dann  $x$  durch  $\lambda$  und  $\mu$  ausdrücken. Wir erhalten  $x = -9 - 3\lambda + 2\mu$ . Somit liegt für alle Werte  $\lambda, \mu \in \mathbb{R}$  der Punkt  $\begin{pmatrix} -9-3\lambda+2\mu \\ \lambda \\ \mu \end{pmatrix}$  in der Ebene. Die Ebene hat also die parametrisierte Darstellung

$$e : \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} -9 \\ 0 \\ 0 \end{pmatrix} + \lambda \cdot \begin{pmatrix} -3 \\ 1 \\ 0 \end{pmatrix} + \mu \cdot \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix}.$$

**8.4. Implizite Darstellung einer Geraden.** Offenbar kann man eine Gerade im Raum nicht durch eine einzige lineare Gleichung in  $x, y, z$  beschreiben. Solche Gleichungen beschreiben nämlich Ebenen im Raum. Jede Gerade kann man aber implizit als Schnitt zweier Ebenen, das heißt als Lösungsmenge von 2 linearen Gleichungen beschreiben. Beispielsweise ist

$$g = \left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathbb{R}^3 \mid 2x - y + 3z = 1, x + 4y - 2z = 3 \right\}$$

die Gerade, die sowohl in der Ebene mit der Gleichung  $2x - y + 3z = 1$  als auch in der Ebene mit der Gleichung  $x + 4y - 2z = 3$  liegt.

Zwei Ebenen im Raum, die nicht parallel sind, schneiden sich immer in einer Geraden. Parallele Ebenen erkennt man daran, dass ihre Normalvektoren in dieselbe Richtung zeigen. Also sind etwa  $2x - y + 3z = 1$  und  $-4x + 2y - 6z = 3$  parallel.

**8.4.1. Verwandlung von Parameterdarstellung in implizite Darstellung.** Wir wandeln

$$g : \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 2 \\ 3 \\ -1 \end{pmatrix} + \lambda \cdot \begin{pmatrix} 1 \\ -1 \\ 3 \end{pmatrix}$$

in implizite Form. Dazu suchen wir 2 Ebenen, die die Gerade enthalten. Liegt  $g$  in einer Ebene mit Normalvektor  $\vec{n}$ , dann ist  $\vec{n}$  normal auf den Richtungsvektor  $\begin{pmatrix} 1 \\ -1 \\ 3 \end{pmatrix}$  der Geraden. Zusätzlich liegt der Punkt  $\begin{pmatrix} 2 \\ 3 \\ -1 \end{pmatrix}$  in der Ebene.

Auf einen Vektor  $\begin{pmatrix} a \\ b \\ c \end{pmatrix}$  sind beispielsweise  $\begin{pmatrix} b \\ -a \\ 0 \end{pmatrix}$ ,  $\begin{pmatrix} c \\ 0 \\ -a \end{pmatrix}$  und  $\begin{pmatrix} 0 \\ c \\ -b \end{pmatrix}$  normal. Wir wählen  $n_1 = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$  und  $n_2 = \begin{pmatrix} 3 \\ 0 \\ -1 \end{pmatrix}$  als Vektoren, die im rechten Winkel auf  $\begin{pmatrix} 1 \\ -1 \\ 3 \end{pmatrix}$  stehen. Damit

liegt  $g$  in den Ebenen durch den Punkt  $\begin{pmatrix} 2 \\ 3 \\ -1 \end{pmatrix}$ , die normal auf  $n_1$  bzw.  $n_2$  sind. Die Gerade ist also der Durchschnitt der beiden Ebenen

$$\begin{aligned} e_1 : & \quad x + y = 5, \text{ und} \\ e_2 : & \quad 3x - z = 7. \end{aligned}$$

Wir haben

$$g = \left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathbb{R}^3 \mid x + y = 5, 3x - z = 7 \right\}.$$

8.4.2. *Verwandlung von impliziter Darstellung in Parameterdarstellung.* Um eine Parameterdarstellung von

$$g = \left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathbb{R}^3 \mid 2x - y + 3z = 1, x + 4y - 2z = 3 \right\}$$

zu erhalten, lösen wir das lineare Gleichungssystem

$$\begin{aligned} 2x - y + 3z &= 1, \\ x + 4y - 2z &= 3. \end{aligned}$$

Eine Methode dafür werden wir im Kapitel 3 vorstellen.



## KAPITEL 2

# Matrizen

### 1. Die Definition von Matrizen

Wir haben bereits *Vektoren* kennen gelernt; solche Paare reeller Zahlen haben wir benutzt, um Punkte in der Ebene zu beschreiben. In der Geometrie brauchen wir auch *Matrizen*. Matrizen eignen sich besonders gut, um etwa Drehungen oder Spiegelungen zu beschreiben.

Eine *Matrix* ist ein rechteckiges Zahlenschema. Zunächst einige Beispiele:

BEISPIELE 2.1.

- $\begin{pmatrix} 1 & 3 & 5 \\ 7 & 2 & 1 \end{pmatrix}$  ist eine  $2 \times 3$ -Matrix.
- $\begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix}$  ist eine  $2 \times 2$ -Matrix.
- $\begin{pmatrix} 3 \\ 1 \end{pmatrix}$  ist eine  $2 \times 1$ -Matrix.
- $(1 \ 2 \ 7)$  ist eine  $1 \times 3$ -Matrix.

Eine Matrix mit  $m$  Zeilen und  $n$  Spalten bezeichnen wir als eine  $m \times n$ -Matrix. Wenn  $A$  eine  $m \times n$ -Matrix ist, und  $i \in \{1, 2, \dots, m\}$  und  $j \in \{1, 2, \dots, n\}$ , so bezeichnen wir mit  $A(i, j)$ ,  $A[i, j]$  oder  $A_{i,j}$  den Eintrag, der bei  $A$  in der  $i$ -ten Zeile und  $j$ -ten Spalte steht. Für

$$A = \begin{pmatrix} 1 & 3 & 5 \\ 7 & 2 & 1 \end{pmatrix}$$

gilt zum Beispiel  $A_{2,1} = 7$ . Die Menge aller  $m \times n$ -Matrizen kürzen wir mit  $\mathbb{R}^{m \times n}$  ab.

Wir müssen noch den Begriff “rechteckiges Zahlenschema” klären. Man kann eine  $m \times n$ -Matrix  $A$  mit Einträgen aus  $\mathbb{R}$  als Funktion von  $\{1, 2, \dots, m\} \times \{1, 2, \dots, n\}$  nach  $\mathbb{R}$  definieren. Der Eintrag, der in der 2. Zeile und 4. Spalte steht, ist dann der Funktionswert  $A(2, 4)$ . Diese Sichtweise gibt auch recht gut wieder, was eine Implementation des abstrakten Datentyps “Matrix” können muss. Es muss möglich sein, eine Funktion `LiefereEintrag` zu schreiben, sodass `LiefereEintrag(A, i, j)` den Eintrag von  $A$  an der  $i$ -ten Zeile und  $j$ -ten Spalte, also den Funktionswert  $A(i, j)$ , zurückgibt.

In Mathematica geben wir die Matrix

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$$

wie folgt ein.

```
In[11]:= A = {{1, 2, 3}, {4, 5, 6}}
```

```
Out[11]= {{1, 2, 3}, {4, 5, 6}}
```

```
In[12]:= MatrixForm[A]
```

```
Out[12]=  $\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$ 
```

```
In[13]:= A = {{5, 7, 8}, {-2, 3, 5}}
```

```
Out[13]= {{5, 7, 8}, {-2, 3, 5}}
```

```
In[14]:= MatrixForm[A]
```

```
Out[14]=  $\begin{pmatrix} 5 & 7 & 8 \\ -2 & 3 & 5 \end{pmatrix}$ 
```

```
In[15]:= A[[2]][[1]]
```

```
Out[15]= -2
```

## 2. Die Addition von Matrizen

Zwei Matrizen kann man addieren, wenn sie gleich viele Zeilen und gleich viele Spalten haben. Wie man zwei Matrizen von gleichem Format addiert, erklären wir mit folgenden Beispielen.

AUFGABEN 2.2.

$$\begin{aligned} & \bullet \begin{pmatrix} 1 & 3 & 5 \\ 7 & 2 & 1 \end{pmatrix} + \begin{pmatrix} -1 & -2 & 3 \\ 6 & 5 & -3 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 8 \\ 13 & 7 & -2 \end{pmatrix} \\ & \bullet \begin{pmatrix} 1 & -3 \\ 2 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 3 \\ 7 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 9 & 1 \end{pmatrix} \\ & \bullet \begin{pmatrix} 1 & 5 \\ 3 & 7 \end{pmatrix} + \begin{pmatrix} 2 & -3 \\ -4 & 0 \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ -1 & 7 \end{pmatrix} \\ & \bullet \begin{pmatrix} 1 & 3 \\ 1 & 0 \end{pmatrix} - \begin{pmatrix} 2 & 1 \\ 3 & 5 \end{pmatrix} = \begin{pmatrix} -1 & 2 \\ -2 & -5 \end{pmatrix}. \end{aligned}$$

Wir fassen zusammen, wie diese Addition funktioniert: Zwei Matrizen  $A \in \mathbb{R}^{m \times k}$ ,  $B \in \mathbb{R}^{n \times l}$  lassen sich genau dann addieren, wenn  $m = n$  und  $k = l$  gilt, d.h. wenn die Matrizen von gleichem Format sind. Wenn  $C$  die Matrix  $A + B$  ist, dann hat auch  $C$  das Format  $m \times k$ , und für alle  $i \in \{1, 2, \dots, m\}$  und  $j \in \{1, 2, \dots, k\}$  berechnet man den Eintrag  $C_{i,j}$  durch

$$C_{i,j} = A_{i,j} + B_{i,j}.$$

```
In[16]:= A = {{1, 4, 3}, {0, 1, 0}};
In[17]:= B = {{-7, 5, 0}, {23, -7, 16}};
In[18]:= A + B
Out[18]= {{-6, 9, 3}, {23, -6, 16}}
In[19]:= MatrixForm [%]
Out[19]= 
$$\begin{pmatrix} -6 & 9 & 3 \\ 23 & -6 & 16 \end{pmatrix}$$

```

### 3. Die Multiplikation einer Matrix mit einer reellen Zahl

Eine Matrix  $A$  wird mit einer reellen Zahl multipliziert, indem jeder Eintrag mit der Zahl multipliziert wird. Wir geben dazu wieder ein Beispiel:

AUFGABE 2.3.

$$2 \cdot \begin{pmatrix} 3 & 5 \\ 7 & 8 \end{pmatrix} = \begin{pmatrix} 6 & 10 \\ 14 & 16 \end{pmatrix}.$$

Wir formulieren wieder allgemein, wie man eine reelle Zahl mit einer Matrix  $A$  multipliziert. Wenn  $t$  eine reelle Zahl, und  $A$  eine  $m \times n$ -Matrix ist, so ist die Matrix  $C := t \cdot A$  ebenfalls eine  $m \times n$ -Matrix. Die Einträge von  $C$  sind dadurch gegeben, dass für alle  $i \in \{1, 2, \dots, m\}$ ,  $j \in \{1, 2, \dots, n\}$  gilt:

$$C_{i,j} = t A_{i,j}.$$

```
In[20]:= A = {{2, 5}, {3, 4}, {10, 2}}
Out[20]= {{2, 5}, {3, 4}, {10, 2}}
In[21]:= MatrixForm [(-10) * A]
Out[21]= 
$$\begin{pmatrix} -20 & -50 \\ -30 & -40 \\ -100 & -20 \end{pmatrix}$$

```

### 4. Die Multiplikation von Matrizen

Zwei Matrizen  $A$ ,  $B$  können genau dann miteinander multipliziert werden, wenn  $A$  genausoviele Spalten wie  $B$  Zeilen hat. Eine  $k \times l$ -Matrix ist also mit einer  $m \times n$ -Matrix multiplizierbar, wenn  $l = m$ . Das Ergebnis dieser Multiplikation ist eine  $k \times n$ -Matrix. Wir erklären die Matrixmultiplikation zunächst anhand eines Beispiels.

AUFGABE 2.4.

$$\begin{pmatrix} 3 & 1 & 2 \\ 2 & 5 & 4 \end{pmatrix} \cdot \begin{pmatrix} 3 & 9 & 3 \\ 1 & 8 & 5 \\ 7 & 1 & -4 \end{pmatrix} = \begin{pmatrix} 3 \cdot 3 + 1 \cdot 1 + 2 \cdot 7 & 3 \cdot 9 + 1 \cdot 8 + 2 \cdot 1 & 3 \cdot 3 + 1 \cdot 5 + 2 \cdot (-4) \\ 2 \cdot 3 + 5 \cdot 1 + 4 \cdot 7 & 2 \cdot 9 + 5 \cdot 8 + 4 \cdot 1 & 2 \cdot 3 + 5 \cdot 5 + 4 \cdot (-4) \end{pmatrix}.$$

Daher gilt

$$\begin{pmatrix} 3 & 1 & 2 \\ 2 & 5 & 4 \end{pmatrix} \cdot \begin{pmatrix} 3 & 9 & 3 \\ 1 & 8 & 5 \\ 7 & 1 & -4 \end{pmatrix} = \begin{pmatrix} 24 & 37 & 6 \\ 39 & 62 & 15 \end{pmatrix}.$$

Wenn man eine  $k \times m$ -Matrix  $A$  mit einer  $m \times n$ -Matrix  $B$  multipliziert, so ist das Produkt  $C$  eine  $k \times n$ -Matrix. Für  $i \in \{1, 2, \dots, k\}$  und  $j \in \{1, 2, \dots, n\}$  ist der Eintrag  $C_{i,j}$  das Skalarprodukt aus der  $i$ -ten Zeile von  $A$  und der  $j$ -ten Spalte von  $B$ . Wir rechnen noch einige Beispiele:

AUFGABEN 2.5.

$$\bullet \begin{pmatrix} 1 & 3 & 2 \\ 0 & -1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 5 & 2 \\ 1 & 7 \\ 8 & -2 \end{pmatrix} = \begin{pmatrix} 24 & 19 \\ 23 & -13 \end{pmatrix}.$$

$$\bullet \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \cdot \begin{pmatrix} 2 & 5 \\ 3 & 7 \end{pmatrix} \text{ ist nicht definiert, da die erste Matrix 3 Spalten und die zweite Matrix 2 Zeilen hat, und 2 nicht gleich 3 ist.}$$

Wenn  $A$  eine  $2 \times 3$  und  $B$  eine  $3 \times 1$ -Matrix ist, dann ist das Produkt  $A \cdot B$  eine  $2 \times 1$ -Matrix. Das Produkt  $B \cdot A$  ist nicht definiert. Selbst dann, wenn beide Produkte  $A \cdot B$  und  $B \cdot A$  definiert sind, müssen die Ergebnisse nicht gleich sein. Dazu rechnen wir folgende Beispiele:

AUFGABEN 2.6.

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

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

$$\begin{pmatrix} 1 & 2 & 5 \end{pmatrix} \cdot \begin{pmatrix} 5 \\ 1 \\ 2 \end{pmatrix} = (17)$$

$$\begin{pmatrix} 5 \\ 1 \\ 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 5 \end{pmatrix} = \begin{pmatrix} 5 & 10 & 25 \\ 1 & 2 & 5 \\ 2 & 4 & 10 \end{pmatrix}$$

Das erste Beispiel noch einmal in Mathematica.

```
In[22]:= A = {{3, 1, 2}, {2, 5, 4}};
         B = {{3, 9, 3}, {1, 8, 5}, {7, 1, -4}};
```

```
In[23]:= MatrixForm[A.B]
```

```
Out[23]=  $\begin{pmatrix} 24 & 37 & 6 \\ 39 & 62 & 15 \end{pmatrix}$ 
```

### 5. Rechenregeln für die Addition und Multiplikation von Matrizen

Wir haben bereits gesehen, dass nicht für alle Matrizen  $A \cdot B = B \cdot A$  gelten muss. Einige Rechenregeln, die wir vom Rechnen mit Zahlen kennen, gelten aber auch für Matrizen.

**SATZ 2.7** (Assoziativität der Matrizenmultiplikation). *Seien  $k, l, m, n \in \mathbb{N}$ , und seien  $A \in \mathbb{R}^{k \times l}$ ,  $B \in \mathbb{R}^{l \times m}$ ,  $C \in \mathbb{R}^{m \times n}$ . Dann gilt*

$$(A \cdot B) \cdot C = A \cdot (B \cdot C).$$

**SATZ 2.8** (Rechtsdistributivität der Matrizenmultiplikation). *Seien  $k, l, m \in \mathbb{N}$ , und seien  $A, B \in \mathbb{R}^{k \times l}$ ,  $C \in \mathbb{R}^{l \times m}$ . Dann gilt*

$$(A + B) \cdot C = (A \cdot C) + (B \cdot C).$$

**SATZ 2.9** (Links-distributivität der Matrizenmultiplikation). *Seien  $k, l, m \in \mathbb{N}$ , und seien  $A \in \mathbb{R}^{k \times l}$ ,  $B, C \in \mathbb{R}^{l \times m}$ . Dann gilt*

$$A \cdot (B + C) = (A \cdot B) + (A \cdot C).$$

Es ist nicht schwierig, die Assoziativität der Matrizenmultiplikation zu beweisen, wenn  $A, B, C$  alle  $2 \times 2$ -Matrizen sind. Man berechnet

$$\left( \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix} \right) \cdot \begin{pmatrix} i & j \\ k & l \end{pmatrix}$$

und

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \left( \begin{pmatrix} e & f \\ g & h \end{pmatrix} \cdot \begin{pmatrix} i & j \\ k & l \end{pmatrix} \right),$$

und stellt fest, dass beide Ergebnisse gleich sind. Für Matrizen von beliebigem Format braucht man folgende Definition der Matrixmultiplikation: Wenn  $A$  eine  $k \times m$ -Matrix,  $B$  eine  $m \times n$ -Matrix, und  $C = A \cdot B$  ist, so gilt für alle  $i \in \{1, 2, \dots, k\}$  und alle  $j \in \{1, 2, \dots, n\}$

$$C[i, j] := \sum_{r=1}^m A[i, r] \cdot B[r, j].$$

### 6. Die Multiplikation von Vektoren und Matrizen

Sei  $v = \begin{pmatrix} -2 \\ 4 \end{pmatrix}$  und  $A = \begin{pmatrix} -3 & 4 \\ 1 & 0 \\ -1 & 1 \end{pmatrix}$ . Dann ist der Vektor  $A \cdot v$  gegeben durch

$$A \cdot v = \begin{pmatrix} -3 & 4 \\ 1 & 0 \\ -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} -2 \\ 4 \end{pmatrix} = \begin{pmatrix} 6 + 16 \\ -2 + 0 \\ 2 + 4 \end{pmatrix}.$$

Das Ergebnis ist ein Vektor im  $\mathbb{R}^3$ .

Die Multiplikation sieht also genauso aus wie die Multiplikation der  $3 \times 2$ -Matrix  $\begin{pmatrix} -3 & 4 \\ 1 & 0 \\ -1 & 1 \end{pmatrix}$  mit der  $2 \times 1$ -Matrix  $\begin{pmatrix} -2 \\ 4 \end{pmatrix}$ . Bei der Matrizenmultiplikation ist das Ergebnis aber eine  $3 \times 1$ -Matrix.

Mit Mathematica wird der Unterschied deutlich:

```
In[24]:= A = {{-3, 4}, {1, 0}, {-1, 1}};
```

```
v = {-2, 4};
```

```
x = A.v
```

```
Out[24]= {22, -2, 6}
```

```
In[25]:= A = {{-3, 4}, {1, 0}, {-1, 1}};
```

```
v = {{-2}, {4}};
```

```
x = A.v
```

```
Out[25]= {{22}, {-2}, {6}}
```

```
In[26]:= A = {{-3, 4}, {1, 0}, {-1, 1}};
```

```
v = {{-2, 4}};
```

```
x = A.v
```

Hier liefert Mathematica eine Fehlermeldung.

```
Out[26]= {{-3, 4}, {1, 0}, {-1, 1}} . {{-2, 4}}
```

Sei  $v = (-4, 3, 2)$  und  $A = \begin{pmatrix} -3 & 5 \\ 1 & 0 \\ -1 & 1 \end{pmatrix}$ . Dann ist der Vektor  $v \cdot A$  gegeben durch

$$(-4, 3, 2) \cdot \begin{pmatrix} -3 & 5 \\ 1 & 0 \\ -1 & 1 \end{pmatrix} = (12 + 3 - 2, -20 + 2) = (13, -18).$$

Das Ergebnis ist ein Vektor im  $\mathbb{R}^2$ .

Die Multiplikation sieht also genauso aus wie die Multiplikation der  $1 \times 3$ -Matrix  $(-4 \ 3 \ 2)$  mit der  $3 \times 2$ -Matrix  $\begin{pmatrix} -3 & 5 \\ 1 & 0 \\ -1 & 1 \end{pmatrix}$ . Bei der Matrizenmultiplikation ist das Ergebnis aber eine  $1 \times 2$ -Matrix.

Wenn man diese Multiplikation ‘Matrix mal Vektor’ verwendet, lassen sich lineare Gleichungssysteme kürzer anschreiben.

$$\begin{aligned} 3x + 4y - 2z &= 1 \\ 2x + 5y - 8z &= 2 \end{aligned}$$

läßt sich dann als

$$\begin{pmatrix} 3 & 4 & -2 \\ 2 & 5 & -8 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$$

schreiben. Im allgemeinen erhält man bei  $m$  Gleichungen und  $n$  Unbekannten die Form

$$A \cdot x = b,$$

wobei  $A$  eine  $m \times n$ -Matrix ist,  $x$  ein Vektor im  $\mathbb{R}^n$  und  $b$  ein Vektor im  $\mathbb{R}^m$ .

Die Funktion `LinearSolve[A, b]` liefert eine Lösung des linearen Gleichungssystems  $A \cdot x = b$ .

Wir lösen zum Beispiel  $2x - 3y = 5$ .

```
In[27]:= LinearSolve[{{2, -3}}, {5}]
```

```
Out[27]= {5/2, 0}
```

Später werden wir sehen, wie man alle Lösungen erhält.

## 7. Das Transponieren von Matrizen

Beim *Transponieren* einer Matrix wird die Matrix an der Hauptdiagonale gespiegelt.

$$\begin{pmatrix} 1 & 4 & -3 \\ 2 & -5 & 3 \end{pmatrix}^T = \begin{pmatrix} 1 & 2 \\ 4 & -5 \\ -3 & 3 \end{pmatrix}$$

Wenn  $A$  eine  $m \times n$ -Matrix ist, so ist  $A^T$  eine  $n \times m$ -Matrix, und für alle  $i \in \{1, 2, \dots, n\}$  und  $j \in \{1, 2, \dots, m\}$  gilt

$$A^T(i, j) = A(j, i).$$

```
In[28]:= A = {{1, 4, -3}, {2, -5, 3}};
```

```
In[29]:= MatrixForm[A]
```

```
Out[29]=  $\begin{pmatrix} 1 & 4 & -3 \\ 2 & -5 & 3 \end{pmatrix}$ 
```

```
In[30]:= B = Transpose[A]
```

```
Out[30]= {{1, 2}, {4, -5}, {-3, 3}}
```

```
In[31]:= MatrixForm[B]
```

```
Out[31]=  $\begin{pmatrix} 1 & 2 \\ 4 & -5 \\ -3 & 3 \end{pmatrix}$ 
```

**SATZ 2.10.** *Haben die Matrizen passendes Format, sodass Addition bzw. Multiplikation ausführbar sind, so gilt:*

- (1)  $(A \cdot B)^T = B^T \cdot A^T$   
 (2)  $(A + B)^T = A^T + B^T$

### ÜBUNGSAUFGABEN 2.11.

- (1) Berechnen Sie für die Matrix

$$A := \begin{pmatrix} 0 & -2 & 3 \\ 8 & 7 & 6 \end{pmatrix}$$

die Matrix  $B := A^T \cdot A$ .

- (2) Berechnen Sie  $(A - B) \cdot C^T$  für die Matrizen

$$A = \begin{pmatrix} 1 & 3 \\ 4 & -2 \end{pmatrix}, B = \begin{pmatrix} -2 & -3 \\ 2 & 2 \end{pmatrix}, C = \begin{pmatrix} 0 & 1 \\ 1 & -1 \\ 2 & 0 \end{pmatrix}.$$

- (3) Finden Sie eine Matrix  $X$ , sodaß  $A \cdot X = B$ , wobei  $A = \begin{pmatrix} -4 & 0 \\ 1 & 2 \end{pmatrix}$ ,  $B = \begin{pmatrix} -4 & -8 \\ 7 & 10 \end{pmatrix}$ . (Hinweis: Bestimmen Sie jede Spalte von  $X$  durch Lösen eines linearen Gleichungssystems.)

## 8. Die Einheitsmatrizen

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

$$\begin{pmatrix} 3 & 5 \\ 4 & 2 \\ 8 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 5 \\ 4 & 2 \\ 8 & 1 \end{pmatrix}$$

Die Matrix

$$E_n = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

heißt Einheitsmatrix vom Format  $n \times n$ . Man sieht leicht, daß für jede  $m \times n$ -Matrix  $A$  und jede  $n \times k$ -Matrix  $B$  gilt:

$$\begin{aligned} A \cdot E_n &= A, \\ E_n \cdot B &= B. \end{aligned}$$

Besonders einfach zu lösen sind Gleichungssysteme mit der Einheitsmatrix: Das Gleichungssystem

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 4 \\ 2 \end{pmatrix}$$

hat die Lösung  $x = 4$ ,  $y = 2$ , und daher die Lösungsmenge  $L = \{(4, 2)\}$ .



```
In[32]:= A = -24 * IdentityMatrix[5];
```

```
MatrixForm[A]
Out[32]= 
$$\begin{pmatrix} -24 & 0 & 0 & 0 & 0 \\ 0 & -24 & 0 & 0 & 0 \\ 0 & 0 & -24 & 0 & 0 \\ 0 & 0 & 0 & -24 & 0 \\ 0 & 0 & 0 & 0 & -24 \end{pmatrix}$$

```

## 9. Das Invertieren von Matrizen

Betrachtet man die Gleichung  $5x = 7$ , so erhält man die Lösung  $x = \frac{7}{5}$  durch Multiplikation beider Seiten mit  $\frac{1}{5}$  (des Inversen von 5). Wir betrachten das Gleichungssystem

$$\begin{pmatrix} 2 & 3 \\ 5 & -5 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 12 \\ -20 \end{pmatrix}$$

Seien wir nun optimistisch, und stellen wir uns vor, wir haben eine Matrix  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ , sodass

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 2 & 3 \\ 5 & -5 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Für die Lösungen des Gleichungssystems muss dann auch gelten:

$$\begin{aligned} A \cdot \begin{pmatrix} 2 & 3 \\ 5 & -5 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} &= A \cdot \begin{pmatrix} 12 \\ -20 \end{pmatrix} \\ \begin{pmatrix} x \\ y \end{pmatrix} &= A \cdot \begin{pmatrix} 12 \\ -20 \end{pmatrix} \end{aligned}$$

Wie bestimmen wir so eine Matrix  $A$ ? Wir suchen eine Matrix  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  die folgende Eigenschaft besitzt:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 2 & 3 \\ 5 & -5 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Durch Ausmultiplizieren erhalten wir folgendes Gleichungssystem:

$$\begin{aligned} 2a + 5b &= 1 \\ 3a - 5b &= 0 \\ 2c + 5d &= 0 \\ 3c - 5d &= 1 \end{aligned}$$

Lösen wir dieses, so erhalten wir

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0,2 & 0,12 \\ 0,2 & -0,08 \end{pmatrix} = \frac{1}{25} \begin{pmatrix} 5 & 3 \\ 5 & -2 \end{pmatrix}.$$

Nun können wir auch die Lösung des ursprünglichen Systems berechnen:

$$\begin{pmatrix} x \\ y \end{pmatrix} = \frac{1}{25} \begin{pmatrix} 5 & 3 \\ 5 & -2 \end{pmatrix} \begin{pmatrix} 12 \\ -20 \end{pmatrix} = \begin{pmatrix} 0 \\ 4 \end{pmatrix}$$

Somit ist  $(0, 4)$  der einzige Kandidat für eine Lösung des Systems. Da  $(0, 4)$  auch wirklich Lösung ist, ergibt sich als Lösungsmenge  $L = \{(0, 4)\}$ .

**DEFINITION 2.12.** Sei  $A$  eine  $n \times n$ -Matrix über  $\mathbb{R}$ .  $A$  heißt *invertierbar*, falls es eine  $n \times n$ -Matrix  $B$  mit  $A \cdot B = B \cdot A = E_n$  gibt.

**SATZ 2.13.** Seien  $A_1, A_2$  invertierbare Matrizen in  $\mathbb{R}^{n \times n}$ . Dann ist auch  $A_1 \cdot A_2$  invertierbar.

*Beweis.* Seien  $A_1, A_2 \in \mathbb{R}^{n \times n}$  invertierbar. Es gibt daher Matrizen  $B_1, B_2$ , sodass  $A_1 \cdot B_1 = B_1 \cdot A_1 = E_n$  und  $A_2 \cdot B_2 = B_2 \cdot A_2 = E_n$ . Dann gilt  $(A_1 \cdot A_2) \cdot (B_2 \cdot B_1) = A_1 \cdot (A_2 \cdot B_2) \cdot B_1 = A_1 \cdot E_n \cdot B_1 = A_1 \cdot B_1 = E_n$ . Somit ist  $A_1 \cdot A_2$  invertierbar. ■

**SATZ 2.14.** Sei  $A$  eine invertierbare Matrix in  $\mathbb{R}^{n \times n}$ , und sei  $B$  so, dass  $A \cdot B = B \cdot A = E_n$ . Sei  $C$  eine Matrix mit  $A \cdot C = E_n$ . Dann gilt  $B = C$ .

*Beweis.* Es gilt  $C = E_n \cdot C = (B \cdot A) \cdot C = B \cdot (A \cdot C) = B \cdot E_n = B$ . ■

Zu jeder invertierbaren Matrix  $A$  gibt es also genau eine Matrix  $B$  mit  $A \cdot B = E_n$ . Diese Matrix  $B$  kürzen wir mit  $A^{-1}$  ab.

**DEFINITION 2.15.** Sei  $A$  eine  $n \times n$ -Matrix.  $A$  ist *regulär* genau dann, wenn  $A$  invertierbar ist.  $A$  ist *singulär* genau dann, wenn  $A$  nicht invertierbar ist.

## ÜBUNGSAUFGABEN 2.16.

- (1) Zeigen Sie, dass für  $a, b, c, d \in \mathbb{R}$  mit  $ad \neq bc$  die Matrix  $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$  invertierbar ist, und dass

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

gilt.

- (2) Sei  $A$  eine  $m \times m$ -Matrix, für die es ein  $n \in \mathbb{N}$  mit  $A^n = 0$  gibt, und sei  $E$  die  $m \times m$ -Einheitsmatrix. Zeigen Sie, dass  $E - A$  invertierbar ist. *Hinweis:* Denken Sie beim Auffinden der inversen Matrix an  $\frac{1}{1-x} = \sum_{i=0}^{\infty} x^i$ .

**SATZ 2.17.** Seien  $A, B \in \mathbb{R}^{n \times n}$  invertierbare Matrizen.

- (1)  $A^{-1}$  ist invertierbar, und es gilt  $(A^{-1})^{-1} = A$ .
- (2)  $A^T$  ist invertierbar, und es gilt  $(A^T)^{-1} = (A^{-1})^T$ .
- (3)  $A \cdot B$  ist invertierbar, und es gilt  $(A \cdot B)^{-1} = B^{-1} \cdot A^{-1}$ .

*Beweis.*

- (1) Es gilt  $A^{-1} \cdot A = A \cdot A^{-1} = E_n$ . Also ist  $A^{-1}$  invertierbar, und  $B := A^{-1}$  ihre inverse Matrix.
- (2) Es gilt  $A \cdot A^{-1} = A^{-1} \cdot A = E_n$ . Durch Transponieren erhält man  $(A^{-1})^T \cdot A^T = A^T \cdot (A^{-1})^T = E_n$ . Folglich ist  $A^T$  invertierbar, und die inverse Matrix zu  $A^T$  ist  $(A^{-1})^T$ .
- (3) Es gilt  $(A \cdot B) \cdot (B^{-1} \cdot A^{-1}) = E_n$  und  $(B^{-1} \cdot A^{-1}) \cdot (A \cdot B) = E_n$ . Folglich ist  $A \cdot B$  invertierbar, und die inverse Matrix von  $A \cdot B$  ist  $B^{-1} \cdot A^{-1}$ .

■

Den folgenden Satz werden wir erst später (als Satz 10.12) beweisen:

**SATZ 2.18.** *Sei  $A \in \mathbb{R}^{n \times n}$ , und sei  $B \in \mathbb{R}^{n \times n}$  so, dass  $A \cdot B = E_n$ . Dann ist  $A$  invertierbar. Außerdem ist dann  $B$  die zu  $A$  inverse Matrix.*

Wir berechnen jetzt die inverse Matrix von  $\begin{pmatrix} 1 & 3 \\ 2 & -4 \end{pmatrix}$  durch den Ansatz

$$\begin{pmatrix} 1 & 3 \\ 2 & -4 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

`In[33] := A = {{1, 3}, {2, -4}};`

`LinearSolve[A, {1, 0}]`

`Out[33] = {2/5, 1/5}`

Also  $a = 0.4, c = 0.2$ .

`In[34] := A = {{1, 3}, {2, -4}};`

`LinearSolve[A, {0, 1}]`

`Out[34] = {3/10, -1/10}`

Also  $b = 0.3, d = -0.1$ .

Die Funktion `Inverse` berechnet die inverse Matrix; die Funktion `^(-1)` macht leider etwas ganz anderes.

`In[35] := A = {{1, 3}, {2, -4}};`

`B = Inverse[A];`

`MatrixForm[B]`

`Out[35] =  $\begin{pmatrix} \frac{2}{5} & \frac{3}{10} \\ \frac{1}{5} & -\frac{1}{10} \end{pmatrix}$`

`In[36] := A.B`

*Out[36]*=  $\{\{1, 0\}, \{0, 1\}\}$

*In[37]*:= **B.A**

*Out[37]*=  $\{\{1, 0\}, \{0, 1\}\}$

*In[38]*:= **A<sup>-1</sup>**

*Out[38]*=  $\{\{1, \frac{1}{3}\}, \{\frac{1}{2}, -\frac{1}{4}\}\}$

*In[39]*:= **A.A<sup>-1</sup>**

*Out[39]*=  $\{\{\frac{5}{2}, -\frac{5}{12}\}, \{0, \frac{5}{3}\}\}$

## KAPITEL 3

# Lineare Gleichungssysteme

### 1. Beispiele

Wir betrachten zunächst vier Gleichungssysteme und bestimmen ihre Lösungsmenge. Dabei geht es uns noch nicht darum, ein Lösungsverfahren für lineare Gleichungssysteme zu entwickeln (das kommt später), sondern nur darum, ein paar typische Phänomene zu beobachten.

- (1) Man bestimme alle Paare  $(x, y)$  in  $\mathbb{R}^2$ , die sowohl die Gleichung  $x + y = -1$  als auch die Gleichung  $3x + 2y = -5$  erfüllen. Wir suchen also alle Lösungen des Gleichungssystems

$$(3.1) \quad \begin{aligned} x + y &= -1 & (1) \\ 3x + 2y &= -5 & (2). \end{aligned}$$

*Lösung:* Wenn  $\begin{pmatrix} x \\ y \end{pmatrix}$  eine Lösung des Gleichungssystems ist, dann gilt  $x + y = -1$ . Daher gilt auch  $-3x - 3y = 3$ . Somit ist jede Lösung des Systems (3.1) auch eine Lösung von

$$(3.2) \quad \begin{aligned} -3x - 3y &= 3 & (1') \\ 3x + 2y &= -5 & (2). \end{aligned}$$

Wenn  $-3x - 3y = 3$  und  $3x + 2y = -5$ , dann gilt auch  $(-3x - 3y) + (3x + 2y) = 3 + (-5)$ , also  $-y = -2$ . Daher muss  $y = 2$  sein. Da aber  $x + y = -1$  ist, muss  $x = -1 - y$  sein, und daher ist  $x = -3$ . Daher ist nur  $\begin{pmatrix} -3 \\ 2 \end{pmatrix}$  als Lösung des Gleichungssystems möglich.

Wir probieren nun aus, ob  $\begin{pmatrix} -3 \\ 2 \end{pmatrix}$  auch wirklich eine Lösung ist. Tatsächlich gilt  $-3 + 2 = -1$  und  $3 \cdot (-3) + 2 \cdot 2 = -5$ . Daher ist die Menge

$$L = \left\{ \begin{pmatrix} -3 \\ 2 \end{pmatrix} \right\}$$

die Lösungsmenge des Gleichungssystems.

Wir interpretieren dieses Beispiel jetzt geometrisch. Jene Punkte  $\begin{pmatrix} x \\ y \end{pmatrix}$  im  $\mathbb{R}^2$ , die die Gleichung  $x + y = -1$  erfüllen, liegen auf einer Geraden (eben auf der Geraden mit Gleichung  $x + y = -1$ ). Jene Punkte  $\begin{pmatrix} x \\ y \end{pmatrix}$ , die die Gleichung  $3x + 2y = -5$  erfüllen, liegen auf der Geraden mit Gleichung  $3x + 2y = -5$ . Die Lösungsmenge des Gleichungssystems enthält alle Punkte, die auf beiden Geraden liegen. Wenn die beiden Geraden nicht parallel sind, so gibt es genau einen Punkt, der auf beiden Geraden liegt, nämlich den Schnittpunkt

der beiden Geraden. Dieser Schnittpunkt ist in diesem Beispiel der Punkt  $\begin{pmatrix} -3 \\ 2 \end{pmatrix}$ .

(2) Wir suchen alle Lösungen des Gleichungssystems

$$(3.3) \quad \begin{aligned} x + 3y &= -1 & (1) \\ -3x - 9y &= 2 & (2). \end{aligned}$$

*Lösung:* Wenn  $\begin{pmatrix} x \\ y \end{pmatrix}$  eine Lösung des Gleichungssystems ist, dann gilt  $x + 3y = -1$ . Daher gilt auch  $3x + 9y = -3$ . Somit ist jede Lösung des Systems (3.3) auch eine Lösung von

$$(3.4) \quad \begin{aligned} 3x + 9y &= -3 & (1') \\ -3x - 9y &= 2 & (2). \end{aligned}$$

Wenn  $3x + 9y = -3$  und  $-3x - 9y = 2$ , dann gilt auch

$$(3.5) \quad (3x + 9y) + (-3x - 9y) = -3 + 2.$$

Die linke Seite von (3.5) ist aber immer 0. Jede Lösung  $\begin{pmatrix} x \\ y \end{pmatrix}$  des Gleichungssystems (3.3) muss also  $0 = -3 + 2$ , also  $0 = -1$  erfüllen. Egal welche  $x, y$  man in die Gleichung (3.5) einsetzt: die Gleichung (3.5) kann nie erfüllt sein.

Somit hat das Gleichungssystem (3.3) keine Lösung. Die Lösungsmenge ist also die leere Menge, also

$$L = \{\} = \emptyset.$$

Wir interpretieren dieses Beispiel jetzt geometrisch. Die Gerade  $x + 3y = -1$  hat den Normalvektor  $\begin{pmatrix} 1 \\ 3 \end{pmatrix}$ . Die Gerade  $-3x - 9y = 2$  hat den Normalvektor  $\begin{pmatrix} -3 \\ -9 \end{pmatrix}$ . Der Vektor  $\begin{pmatrix} -3 \\ -9 \end{pmatrix}$  ist ein Vielfaches des Vektors  $\begin{pmatrix} 1 \\ 3 \end{pmatrix}$ . Die beiden Geraden sind also parallel. Zwei parallele Geraden sind entweder identisch, oder sie haben keinen gemeinsamen Punkt. Da das Gleichungssystem (3.3) unlösbar ist, haben die beiden Geraden keinen gemeinsamen Punkt; sie sind also zwei verschiedene parallele Geraden.

(3) Wir suchen alle Lösungen des Gleichungssystems

$$(3.6) \quad \begin{aligned} x + 5y &= -4 & (1) \\ -2x - 10y &= 8 & (2). \end{aligned}$$

*Lösung:* Wenn  $\begin{pmatrix} x \\ y \end{pmatrix}$  eine Lösung des Gleichungssystems ist, dann gilt  $x + 5y = -4$ . Daher gilt auch  $2x + 10y = -8$ . Somit ist jede Lösung des Systems (3.6) auch eine Lösung von

$$(3.7) \quad \begin{aligned} 2x + 10y &= -8 & (1') \\ -2x - 10y &= 8 & (2). \end{aligned}$$

Wenn  $2x + 10y = -8$  und  $-2x - 10y = 8$ , dann gilt auch

$$(3.8) \quad (2x + 10y) + (-2x - 10y) = -8 + 8.$$

Sowohl die linke als auch die rechte Seite der Gleichung (3.8) ist also 0. Somit ist die Gleichung (3.8) für alle  $\begin{pmatrix} x \\ y \end{pmatrix}$  in  $\mathbb{R}^2$  erfüllt. Sie liefert also keine Einschränkung für die Lösungen.

Nicht jeder Punkt  $\begin{pmatrix} x \\ y \end{pmatrix}$  in  $\mathbb{R}^2$  ist eine Lösung des Systems (3.6). (Der Punkt  $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$  erfüllt nicht einmal die erste Gleichung.) Wir sehen aber, dass jede Lösung der ersten Gleichung von (3.6) auch eine Lösung der zweiten Gleichung von (3.6) ist: das liegt daran, dass die zweite Gleichung entsteht, wenn man beide Seiten der ersten Gleichung mit  $-2$  multipliziert. Man kann also die zweite Gleichung einfach weglassen (sie liefert keine weitere Einschränkung für  $x$  und  $y$ ), und nur mehr die Lösungen von

$$x + 5y = -4$$

bestimmen. Wir sehen, dass wir für jeden Wert, den wir für  $y$  vorgeben, einen Wert für  $x$  erhalten. Wenn wir für  $y := t$  setzen, erhalten wir für  $x$  den Wert  $x = -4 - 5t$ . Somit können wir die Lösungsmenge  $L$  so angeben:

$$L = \left\{ \begin{pmatrix} -4-5t \\ t \end{pmatrix} \mid t \in \mathbb{R} \right\}.$$

Die Lösungsmenge  $L$  ist also eine Gerade durch  $\begin{pmatrix} -4 \\ 0 \end{pmatrix}$  mit Richtungsvektor  $\begin{pmatrix} -5 \\ 1 \end{pmatrix}$ .

Wir interpretieren dieses Beispiel jetzt geometrisch. Die Gleichungen  $x + 5y = -4$  und  $-2x - 10y = 8$  werden von denselben  $\begin{pmatrix} x \\ y \end{pmatrix}$  erfüllt. Sie beschreiben also die gleiche Gerade. Der Schnitt dieser beiden Geraden miteinander ist also genau diese eine Gerade. Und wirklich:  $X = \begin{pmatrix} -4 \\ 0 \end{pmatrix} + t \cdot \begin{pmatrix} -5 \\ 1 \end{pmatrix}$  ist genau die Parameterdarstellung der Geraden  $x + 5y = -4$ .

- (4) Wir suchen alle Lösungen des Gleichungssystems

$$(3.9) \quad \begin{aligned} 3x + 4y &= -1 & (1) \\ 5x + 10y &= -5 & (2) \\ 2x + 8y &= -6 & (3). \end{aligned}$$

*Lösung:* Wir multiplizieren die Gleichung (1) mit 5, und die Gleichung (2) mit  $-3$  und erhalten

$$(3.10) \quad \begin{aligned} 15x + 20y &= -5 & (1') \\ -15x - 30y &= 15 & (2') \\ 2x + 8y &= -6 & (3). \end{aligned}$$

Jede Lösung von (1') und (2') erfüllt auch

$$(15x + 20y) + (-15x - 30y) = -5 + 15,$$

also  $-10y = 10$ , und somit  $y = -1$ . Wenn  $y = -1$ , dann muss wegen der Gleichung (1) gelten:

$$3x = -1 - 4y,$$

also  $3x = -1 + 4$ , und somit  $x = 1$ .

Die Frage ist, ob  $\begin{pmatrix} 1 \\ -1 \end{pmatrix}$  auch wirklich eine Lösung des Gleichungssystems ist. Wir haben bis jetzt ja nur so begründet, dass für jede Lösung  $\begin{pmatrix} x \\ y \end{pmatrix}$  des Gleichungssystems  $x = 1$  und  $y = -1$  gelten muss. Wir wissen aber noch nicht, ob  $\begin{pmatrix} 1 \\ -1 \end{pmatrix}$  die Gleichungen (1), (2) und (3) erfüllt. So haben wir etwa die Gleichung (3) beim Ausrechnen von  $x$  und  $y$  noch gar nicht verwendet! Wir müssen also ausprobieren, ob  $\begin{pmatrix} 1 \\ -1 \end{pmatrix}$  wirklich alle drei Gleichungen erfüllt. Es gilt  $3 \cdot 1 + 4 \cdot (-1) = -1$ ,  $5 \cdot 1 + 10 \cdot (-1) = -5$  und  $2 \cdot 1 + 8 \cdot (-1) = -6$ . Das Paar  $\begin{pmatrix} 1 \\ -1 \end{pmatrix}$  erfüllt also wirklich alle drei Gleichungen, und es gilt somit

$$L = \left\{ \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\}.$$

Wir interpretieren dieses Beispiel jetzt geometrisch. Von den drei Geraden, die durch die Gleichungen (1), (2) und (3) beschrieben werden, sind keine zwei parallel, da kein Normalvektor ein Vielfaches eines anderen Normalvektors ist. Alle drei Geraden gehen durch den Punkt  $\begin{pmatrix} 1 \\ -1 \end{pmatrix}$ . Die drei Geraden gehen also "sternförmig" durch den Punkt  $\begin{pmatrix} 1 \\ -1 \end{pmatrix}$ .

Das Gleichungssystem (3.6) zeigt, dass die Lösungsmenge  $L$  eines linearen Gleichungssystems nicht leer oder einelementig sein muss, sondern auch eine unendliche Menge sein kann. Für die Darstellung der Lösungsmenge  $L$  des Systems (3.6) gibt es zwei Möglichkeiten:

- (1) *Implizite Darstellung* der Lösung: Jedes Paar  $(x, y)$ , das  $x + 5y = -4$  erfüllt, ist auch eine Lösung für das gesamte Gleichungssystem. Die Lösung kann also in der Form

$$L = \{(x, y) \in \mathbb{R}^2 \mid x + 5y = -4\}$$

geschrieben werden.

- (2) *Parametrisierte Darstellung* der Lösung: Wir können die Lösungsmenge als

$$L = \{(-4, 0) + t \cdot (-5, 1) \mid t \in \mathbb{R}\}$$

schreiben.

Wollen wir nun überprüfen, ob das Paar  $(3, 4)$  in der Lösungsmenge liegt, so müssen wir bei impliziter Darstellung nur  $x = 3$  und  $y = 4$  in  $x + 5y$  einsetzen. Da wir dabei 23 und nicht  $-4$  erhalten, folgt  $(3, 4) \notin L$ . Bei parametrisierter Darstellung müssen wir dazu das Gleichungssystem

$$\begin{aligned} -4 - 5t &= 3 \\ t &= 4 \end{aligned}$$

lösen. Aus der Tatsache, dass dieses System keine Lösung besitzt, können wir  $(3, 4) \notin L$  schließen.

Die implizite Darstellung lässt jedoch keine direkte geometrische Interpretation zu, während man aus der parametrisierten Darstellung sofort erkennt, dass es sich bei der Lösungsmenge um eine Gerade im  $\mathbb{R}^2$  mit der Steigung  $-\frac{1}{5}$  handelt.



Auch andere Kurven im  $\mathbb{R}^2$  lassen sich sowohl implizit als auch parametrisiert darstellen. So ist zum Beispiel der Kreis mit Radius 1 um den Ursprung gegeben durch

$$\begin{aligned} K &= \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\} \\ &= \{(\cos t, \sin t) \mid t \in \mathbb{R}, 0 \leq t < 2\pi\}. \end{aligned}$$

Wir werden uns überlegen, wie wir die Lösungsmenge von einer Darstellungsform in die andere umrechnen können. Die jeweiligen Übergänge nennt man *Parametrisieren* (*Lösen*) bzw. *Implizitisieren*.

## 2. Die Lösung von Gleichungssystemen in Staffelform

Wir betrachten das Gleichungssystem

$$(3.11) \quad \begin{pmatrix} 1 & -5 & 8 & 2 & -2 \\ 0 & 1 & -2 & -4 & 2 \\ 0 & 0 & 0 & -16 & 8 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \cdot x = \begin{pmatrix} -9 \\ 5 \\ 16 \\ 0 \end{pmatrix}.$$

Dieses Gleichungssystem können wir so lösen:  $x_5$  können wir beliebig festlegen. Wir setzen also

$$x_5 = t.$$

Wir erhalten

$$-16x_4 + 8t = 16,$$

also

$$x_4 = -1 + \frac{1}{2}t.$$

Da  $x_3$  frei wählbar ist, setzen wir  $x_3$  auf  $s$ .

Dann erhalten wir

$$x_2 = 5 + 2x_3 + 4x_4 - 2x_5,$$

also

$$\begin{aligned} x_2 &= 5 + 2s - 4 + 2t - 2t \\ x_2 &= 1 + 2s. \end{aligned}$$

Schließlich

$$x_1 = -2 + 2s + t.$$

Also ergibt sich als Lösungsmenge

$$L = \left\{ \begin{pmatrix} -2 \\ 1 \\ 0 \\ -1 \\ 0 \end{pmatrix} + s \cdot \begin{pmatrix} 2 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + t \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ \frac{1}{2} \\ 1 \end{pmatrix} \mid s, t \in \mathbb{R} \right\}.$$

Die Matrix

$$\begin{pmatrix} 1 & -5 & 8 & 2 & -2 \\ 0 & 1 & -2 & -4 & 2 \\ 0 & 0 & 0 & -16 & 8 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

ist eine besonders angenehme Koeffizientenmatrix. Sie ist nämlich in *Zeilenstufenform*. Wir definieren:

**DEFINITION 3.1.** Sei  $A$  eine  $m \times n$ -Matrix.  $A$  ist in *Zeilenstufenform*, wenn es  $r \in \mathbb{N}_0$  und  $j_1, j_2, \dots, j_r \in \{1, \dots, n\}$  gibt, sodass

- (1)  $j_r > j_{r-1} > \dots > j_1$ .
- (2) Für alle  $i \in \{1, 2, \dots, r\}$  gilt:  $A(i, j_i) \neq 0$ .
- (3) Für alle  $i \in \{1, 2, \dots, r\}$  und für alle  $k \in \{1, 2, \dots, n\}$  mit  $k < j_i$  gilt:  $A(i, k) = 0$ .
- (4) Für alle  $i \in \{1, 2, \dots, m\}$  mit  $i > r$  und für alle  $k \in \{1, 2, \dots, n\}$  gilt:  $A(i, k) = 0$ .

Wenn  $A$  eine  $m \times n$ -Matrix in Zeilenstufenform ist, und  $r$  wie in obiger Definition, dann treten in der Lösung von  $A \cdot x = 0$  genau  $n - r$  frei wählbare Parameter auf.

### ÜBUNGSAUFGABEN 3.2.

- (1) Bestimmen Sie die Lösungsmenge des linearen Gleichungssystems

$$\begin{pmatrix} 2 & 0 & 1 & -1 \\ 0 & 1 & 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

Geben Sie die Lösungsmenge in parametrisierter Form an.

- (2) Bestimmen Sie die Lösungsmenge des linearen Gleichungssystems

$$\begin{pmatrix} 1 & 1 & 1 & -1 \\ 0 & 1 & 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

Geben Sie die Lösungsmenge in parametrisierter Form an.

- (3) Bestimmen Sie alle Lösungen des folgenden Gleichungssystems:

$$\begin{aligned} 2x_1 - 1x_2 + 1x_3 - 1x_4 + 1x_5 &= 12 \\ 1x_2 + 1x_3 - 1x_4 + 1x_5 &= 4 \\ 1x_3 + 0x_4 - 1x_5 &= 14. \end{aligned}$$

- (4) Lösen Sie das Gleichungssystem

$$\begin{pmatrix} 2 & 5 & 7 & 3 & 2 \\ 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & -1 & 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} = \begin{pmatrix} 1 \\ -2 \\ 0 \end{pmatrix},$$

und geben Sie die Lösungsmenge parametrisiert an.

### 3. Das Gaußsche Eliminationsverfahren

Wenn die Koeffizientenmatrix eines Gleichungssystems Zeilenstaffelform hat, dann wissen wir bereits, wie wir alle Lösungen des Gleichungssystems bestimmen. Wir erklären mit einem Beispiel, wie wir sonst vorgehen. Wir betrachten das Gleichungssystem

$$(3.12) \quad \begin{pmatrix} 1 & -5 & 8 & 2 & -2 \\ 1 & -4 & 6 & -2 & 0 \\ -1 & 0 & 2 & 2 & 0 \\ 5 & -8 & 6 & 0 & -5 \end{pmatrix} \cdot x = \begin{pmatrix} -9 \\ -4 \\ 0 \\ -18 \end{pmatrix}$$

Wir schreiben uns zunächst das System anders auf.

$$\begin{array}{rccccccc} I & 1 & -5 & 8 & 2 & -2 & -9 \\ II & 1 & -4 & 6 & -2 & 0 & -4 \\ III & -1 & 0 & 2 & 2 & 0 & 0 \\ IV & 5 & -8 & 6 & 0 & -5 & -18 \end{array}$$

Wir addieren nun passende Vielfache der Gleichung I zu jeder der anderen Gleichungen, sodass in den neuen Gleichungen die Variable  $x_1$  nicht mehr vorkommt. Das führt auf

$$(3.13) \quad \begin{array}{rccccccc} II' & 0 & 1 & -2 & -4 & 2 & 5 & -I + II \\ III' & 0 & -5 & 10 & 4 & -2 & -9 & I + III \\ IV' & 0 & 17 & -34 & -10 & 5 & 27 & (-5) \cdot I + IV \end{array}$$

Nun hat das Gleichungssystem, das aus den Gleichungen I,II,III,IV besteht, die gleiche Lösungsmenge wie das Gleichungssystem, das aus den Gleichungen I,II',III',IV' besteht.

Das kann man so begründen: wenn ein Tupel  $(x_1, x_2, x_3, x_4, x_5)$  die Gleichungen I und IV erfüllt, dann erfüllt es auch die Gleichung IV', die ja eine Linearkombination (= Summer von Vielfachen) der Gleichungen I und IV ist. Sei nun  $(x_1, x_2, x_3, x_4, x_5)$  ein Tupel, das die Gleichungen I und IV' erfüllt. Da  $IV' = -5 \cdot I + IV$ , gilt  $IV = IV' + 5 \cdot I$ . Daher ist die Gleichung IV eine Linearkombination der Gleichungen IV' und I. Also muss das Tupel  $(x_1, x_2, x_3, x_4, x_5)$  auch die Gleichung IV erfüllen.

Wir können also anstelle des Gleichungssystems I,II,III,IV das Gleichungssystem I,II',III',IV' lösen. In den Gleichungen II', III', IV' kommt die Variable  $x_1$  nicht vor. Also können wir so vorgehen: wir bestimmen die Lösungen  $(x_2, x_3, x_4, x_5)$  der Gleichungen II', III', IV'. Für jede dieser Lösungen rechnen wir uns dann aus der Gleichung I den Wert von  $x_1$  aus.

Um die Lösungen von II', III', IV' zu bestimmen, addieren wir wieder passende Vielfache der Gleichung II' zu III' und IV'. Wir erhalten

$$(3.14) \quad \begin{array}{rccccccc} III'' & 0 & 0 & 0 & -16 & 8 & 16 & 5 \cdot II' + III' \\ IV'' & 0 & 0 & 0 & 58 & -29 & -58 & (-17) \cdot II' + IV' \end{array}$$

Nun können wir alle Lösungen  $(x_3, x_4, x_5)$  der Gleichungen III'' und IV'' bestimmen. Dann können wir für jede Lösung aus II' den Wert von  $x_2$  bestimmen (und dann aus I den Wert von  $x_1$ ).

In den Gleichungen III'' und IV'' kommt  $x_3$  nicht vor. Wenn wir also eine Lösung  $(x_4, x_5)$  für die Gleichungen III'' und IV'' finden, dann können wir für  $x_3$  jede beliebige Zahl einsetzen. Für jede solche Setzung erhalten wir eine Lösung  $(x_3, x_4, x_5)$  von III'' und IV''. Wir merken uns:

$x_3$  ist frei wählbar,

sofern es Lösungen  $(x_4, x_5)$  für III'' und IV'' gibt. Jetzt versuchen wir, alle Lösungen  $(x_4, x_5)$  von III'' und IV'' zu finden. Dazu addieren wir ein passendes Vielfaches der Gleichung III'' zur Gleichung IV''. Wir erhalten

$$(3.15) \quad \underline{IV''' \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 0 \quad 58 \cdot III'' + 16 \cdot IV''}$$

Alle Lösungen  $(x_5)$  dieser letzten Gleichung zu finden, ist einfach: wir können jeden Wert für  $x_5$  einsetzen. Also:

$x_5$  ist frei wählbar.

Setzen wir also  $x_5$  auf  $t$ , und schauen wir, welche Werte sich für die anderen Variablen ergeben.

Aus der Gleichung III'' erhalten wir

$$-16x_4 + 8t = 16,$$

also

$$x_4 = -1 + \frac{1}{2}t.$$

Da  $x_3$  frei wählbar ist, setzen wir  $x_3$  auf  $s$ .

Aus der Gleichung II' erhalten wir

$$x_2 = 5 + 2x_3 + 4x_4 - 2x_5,$$

also

$$\begin{aligned} x_2 &= 5 + 2s - 4 + 2t - 2t \\ x_2 &= 1 + 2s. \end{aligned}$$

Aus der Gleichung I erhalten wir schließlich

$$x_1 = -2 + 2s + t.$$

Also ergibt sich als Lösungsmenge

$$L = \left\{ \begin{pmatrix} -2 \\ 1 \\ 0 \\ -1 \\ 0 \end{pmatrix} + s \cdot \begin{pmatrix} 2 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} + t \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ \frac{1}{2} \\ 1 \end{pmatrix} \mid s, t \in \mathbb{R} \right\}.$$

## ÜBUNGSAUFGABEN 3.3.

- (1) Bestimmen Sie alle Lösungen des Gleichungssystems

$$\begin{aligned}x + 2y + 3z &= -10 \\ -x + 7y + 2z &= -10 \\ 5x - 8y + 5z &= -10.\end{aligned}$$

- (2) Bestimmen Sie alle Lösungen des Gleichungssystems

$$\begin{aligned}-4x + 2y + 3z &= 12 \\ -6x + 3y + 0z &= -18 \\ 6x - 3y + 2z &= 34\end{aligned}$$

- (3) Bestimmen Sie alle Lösungen des Gleichungssystems

$$\begin{aligned}1x + 0y + 2z &= 16 \\ 2x + 3y - z &= -8 \\ 0x + 2y - 3z &= -36\end{aligned}$$

- (4) Geben Sie die Lösungsmenge des folgenden linearen Gleichungssystems in parametrisierter Form an!

$$\begin{pmatrix} -2 & -1 & 0 & 8 \\ 2 & -3 & 8 & 0 \\ 10 & -7 & 24 & -16 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} -32 \\ 16 \\ 112 \end{pmatrix}.$$

- (5) Geben Sie die Lösungsmenge des folgenden linearen Gleichungssystems in parametrisierter Form an!

$$\begin{pmatrix} -2 & -1 & 8 & 0 \\ 2 & -3 & 0 & 8 \\ 10 & -7 & -16 & -24 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} -16 \\ 8 \\ 56 \end{pmatrix}$$

- (6) Ergänzen Sie die Gleichung

$$3x - 2y + 5z = 0$$

so zu einem Gleichungssystem mit drei Gleichungen, dass das System

- (a) keine Lösung
- (b) genau eine Lösung
- (c) genau zwei Lösungen
- (d) eine Gerade als Lösungsmenge
- (e) eine Ebene als Lösungsmenge

hat.

- (7) Für zwei Goldbarren und acht Silbertaler erhalten Sie 69.000.– Schilling, für 7 Barren und 3 Taler 84.000.– Schilling. Wieviel ist ein Goldbarren wert? Wieviel ist ein Silbertaler wert?

- (8) Bestimmen Sie alle Lösungen des Gleichungssystems

$$\begin{pmatrix} 1 & 5 & 3 \\ 2 & 10 & 8 \\ 4 & 20 & 15 \\ 1 & 6 & 5 \end{pmatrix} \cdot x = \begin{pmatrix} 16 \\ 34 \\ 67 \\ 21 \end{pmatrix}.$$

- (9) Bestimmen Sie alle Lösungen des Gleichungssystems

$$\begin{pmatrix} 1 & 3 & 5 & 2 \\ 2 & 8 & 14 & 4 \\ -1 & -2 & -3 & -2 \end{pmatrix} \cdot x = \begin{pmatrix} 3 \\ 6 \\ -2 \end{pmatrix}.$$

- (10) Lösen Sie folgendes Gleichungssystem, und geben Sie die Lösungsmenge paramtrisiert an!

$$\begin{pmatrix} -2 & 1 & 0 & 1 \\ -3 & 2 & 2 & 0 \\ -6 & 5 & 8 & -3 \end{pmatrix} \cdot x = \begin{pmatrix} -8 \\ -13 \\ -28 \end{pmatrix}.$$

#### 4. Einige durchgerechnete Beispiele zum Gauß-Algorithmus

---

AUFGABE 3.4.

$$\begin{pmatrix} 1 & -5 & 8 & 2 & -2 \\ 1 & -4 & 6 & -2 & 0 \\ -1 & 0 & 2 & 2 & 0 \\ 5 & -8 & 6 & 0 & -5 \end{pmatrix} \cdot x = \begin{pmatrix} -9 \\ -4 \\ 0 \\ -18 \end{pmatrix}$$

`In[40] := << GaussDemo6.m`

`In[41] := Gauss [A1, b1]`

$$\begin{array}{cccccc|c} x1 & x2 & x3 & x4 & x5 & & \\ \hline 1 & -5 & 8 & 2 & -2 & & -9 \\ 1 & -4 & 6 & -2 & 0 & & -4 \\ -1 & 0 & 2 & 2 & 0 & & 0 \\ 5 & -8 & 6 & 0 & -5 & & -18 \end{array}$$

We use equation (1) of the last system to eliminate x1

$$\begin{array}{cccc|c} x2 & x3 & x4 & x5 & \\ \hline 1 & -2 & -4 & 2 & 5 \\ -5 & 10 & 4 & -2 & -9 \\ 17 & -34 & -10 & 5 & 27 \end{array}$$

We use equation (1) of the last system to eliminate x2

$$\begin{array}{ccc|c} x3 & x4 & x5 & \\ \hline 0 & -16 & 8 & 16 \\ 0 & 58 & -29 & -58 \end{array}$$

x3 does not appear in any equation.

$$\begin{array}{cc|c} x4 & x5 & \\ \hline -16 & 8 & 16 \\ 58 & -29 & -58 \end{array}$$

We use equation (1) of the last system to eliminate x4

$$\begin{array}{c|c} x5 & \\ \hline 0 & 0 \end{array}$$

x5 does not appear in any equation.

`x5 := t1`

We use

$$\begin{array}{cc|c} x4 & x5 & \\ \hline -16 & 8 & 16 \end{array}$$

to compute x4

$$x4 = -1 + \frac{t1}{2}$$

`x3 := t2`

We use

$$\left( \begin{array}{cccc|c} x_2 & x_3 & x_4 & x_5 & \\ 1 & -2 & -4 & 2 & 5 \end{array} \right)$$

to compute  $x_2$

$$x_2 = 1 + 2t_2$$

We use

$$\left( \begin{array}{ccccc|c} x_1 & x_2 & x_3 & x_4 & x_5 & \\ 1 & -5 & 8 & 2 & -2 & -9 \end{array} \right)$$

to compute  $x_1$

$$x_1 = -2 + t_1 + 2t_2$$

$$\text{Out}[41]= \{ \{-2, 1, 0, -1, 0\}, \{ \{1, 0, 0, \frac{1}{2}, 1\}, \{2, 2, 1, 0, 0\} \} \}$$

### AUFGABE 3.5.

$$\begin{pmatrix} 1 & 5 & 7 & 9 \\ 2 & 10 & 14 & 18 \\ 3 & 2 & 1 & 0 \end{pmatrix} \cdot x = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$$

`In[42]:= << GaussDemo6.m`

`In[43]:= Gauss [A2, b2]`

$$\left( \begin{array}{cccc|c} x_1 & x_2 & x_3 & x_4 & \\ 1 & 5 & 7 & 9 & 0 \\ 2 & 10 & 14 & 18 & 1 \\ 3 & 2 & 1 & 0 & 1 \end{array} \right)$$

We use equation (1) of the last system to eliminate  $x_1$

$$\left( \begin{array}{ccc|c} x_2 & x_3 & x_4 & \\ 0 & 0 & 0 & 1 \\ -13 & -20 & -27 & 1 \end{array} \right)$$

We use equation (2) of the last system to eliminate  $x_2$

$$\left( \begin{array}{cc|c} x_3 & x_4 & \\ 0 & 0 & 1 \end{array} \right)$$

$x_3$  does not appear in any equation.

$$\left( \begin{array}{c|c} x_4 & \\ 0 & 1 \end{array} \right)$$

$x_4$  does not appear in any equation.

The system has no solution

`Out[43]= NOSOLUTION`

## AUFGABE 3.6.

$$\begin{pmatrix} 1 & 5 & 3 \\ 2 & 10 & 8 \\ 4 & 20 & 15 \\ 1 & 6 & 5 \end{pmatrix} \cdot x = \begin{pmatrix} 16 \\ 34 \\ 67 \\ 21 \end{pmatrix}$$

`In[44] := << GaussDemo6.m`

`In[45] := Gauss [A3, b3]`

$$\begin{pmatrix} x1 & x2 & x3 & | & \\ 1 & 5 & 3 & | & 16 \\ 2 & 10 & 8 & | & 34 \\ 4 & 20 & 15 & | & 67 \\ 1 & 6 & 5 & | & 21 \end{pmatrix}$$

We use equation (1) of the last system to eliminate x1

$$\begin{pmatrix} x2 & x3 & | & \\ 0 & 2 & | & 2 \\ 0 & 3 & | & 3 \\ 1 & 2 & | & 5 \end{pmatrix}$$

We use equation (3) of the last system to eliminate x2

$$\begin{pmatrix} x3 & | & \\ 2 & | & 2 \\ 3 & | & 3 \end{pmatrix}$$

We use equation (1) of the last system to eliminate x3

We use

$$\begin{pmatrix} x3 & | & \\ 2 & | & 2 \end{pmatrix}$$

to compute x3

$$x3 = 1$$

We use

$$\begin{pmatrix} x2 & x3 & | & \\ 1 & 2 & | & 5 \end{pmatrix}$$

to compute x2

$$x2 = 3$$

We use

$$\begin{pmatrix} x1 & x2 & x3 & | & \\ 1 & 5 & 3 & | & 16 \end{pmatrix}$$

to compute x1

$$x1 = -2$$

`Out[45] = {{-2, 3, 1}, {}}`



## AUFGABE 3.7.

$$\begin{pmatrix} 1 & 5 & 3 \\ 2 & 10 & 8 \\ 4 & 20 & 15 \\ 1 & 6 & 5 \end{pmatrix} \cdot x = \begin{pmatrix} 16 \\ 34 \\ 68 \\ 22 \end{pmatrix}$$

```
In[46]:= << GaussDemo6.m
```

```
In[47]:= Gauss [A4, b4]
```

$$\begin{array}{ccc|c} x1 & x2 & x3 & \\ \hline 1 & 5 & 3 & 16 \\ 2 & 10 & 8 & 34 \\ 4 & 20 & 15 & 68 \\ 1 & 6 & 5 & 22 \end{array}$$

We use equation (1) of the last system to eliminate x1

$$\begin{array}{ccc|c} x2 & x3 & & \\ \hline 0 & 2 & & 2 \\ 0 & 3 & & 4 \\ 1 & 2 & & 6 \end{array}$$

We use equation (3) of the last system to eliminate x2

$$\begin{array}{c|c} x3 & \\ \hline 2 & 2 \\ 3 & 4 \end{array}$$

We use equation (1) of the last system to eliminate x3

The system has no solution

```
Out[47]= NOSOLUTION
```

## AUFGABE 3.8.

$$\begin{pmatrix} 1 & 2 & -3 & 0 & 6 & 7 & 0 \\ -2 & -4 & 1 & 0 & 2 & 3 & 0 \\ 4 & 8 & 1 & 0 & 1 & -1 & 0 \\ 3 & 6 & -1 & 0 & 9 & 9 & 0 \end{pmatrix} \cdot x = \begin{pmatrix} 5 \\ 7 \\ 3 \\ 15 \end{pmatrix}$$

```
In[48]:= << GaussDemo6.m
```

```
In[49]:= Gauss [A5, b5]
```

$$\begin{array}{ccccccc|c} x1 & x2 & x3 & x4 & x5 & x6 & x7 & \\ \hline 1 & 2 & -3 & 0 & 6 & 7 & 0 & 5 \\ -2 & -4 & 1 & 0 & 2 & 3 & 0 & 7 \\ 4 & 8 & 1 & 0 & 1 & -1 & 0 & 3 \\ 3 & 6 & -1 & 0 & 9 & 9 & 0 & 15 \end{array}$$

We use equation (1) of the last system to eliminate  $x_1$

$$\left( \begin{array}{cccccc|c} x_2 & x_3 & x_4 & x_5 & x_6 & x_7 & \\ 0 & -5 & 0 & 14 & 17 & 0 & 17 \\ 0 & 13 & 0 & -23 & -29 & 0 & -17 \\ 0 & 8 & 0 & -9 & -12 & 0 & 0 \end{array} \right)$$

$x_2$  does not appear in any equation.

$$\left( \begin{array}{cccc|c} x_3 & x_4 & x_5 & x_6 & x_7 & \\ -5 & 0 & 14 & 17 & 0 & 17 \\ 13 & 0 & -23 & -29 & 0 & -17 \\ 8 & 0 & -9 & -12 & 0 & 0 \end{array} \right)$$

We use equation (1) of the last system to eliminate  $x_3$

$$\left( \begin{array}{cccc|c} x_4 & x_5 & x_6 & x_7 & \\ 0 & 67 & 76 & 0 & 136 \\ 0 & 67 & 76 & 0 & 136 \end{array} \right)$$

$x_4$  does not appear in any equation.

$$\left( \begin{array}{ccc|c} x_5 & x_6 & x_7 & \\ 67 & 76 & 0 & 136 \\ 67 & 76 & 0 & 136 \end{array} \right)$$

We use equation (1) of the last system to eliminate  $x_5$

$$\left( \begin{array}{cc|c} x_6 & x_7 & \\ 0 & 0 & 0 \end{array} \right)$$

$x_6$  does not appear in any equation.

$$\left( \begin{array}{c|c} x_7 & \\ 0 & 0 \end{array} \right)$$

$x_7$  does not appear in any equation.

$x_7 := t_1$

$x_6 := t_2$

We use

$$\left( \begin{array}{ccc|c} x_5 & x_6 & x_7 & \\ 67 & 76 & 0 & 136 \end{array} \right)$$

to compute  $x_5$

$$x_5 = \frac{136}{67} + -\frac{76 t_2}{67}$$

$x_4 := t_3$

We use

$$\left( \begin{array}{ccccc|c} x_3 & x_4 & x_5 & x_6 & x_7 & \\ -5 & 0 & 14 & 17 & 0 & 17 \end{array} \right)$$

to compute  $x_3$

$$x_3 = \frac{153}{67} + \frac{15 t_2}{67}$$

`x2 := t4`

We use

$$\left( \begin{array}{ccccccc|c} x1 & x2 & x3 & x4 & x5 & x6 & x7 & | & \\ 1 & 2 & -3 & 0 & 6 & 7 & 0 & | & 5 \end{array} \right)$$

to compute `x1`

$$x1 = -\frac{22}{67} + \frac{32t2}{67} - 2t4$$

$$\text{Out}[49]= \left\{ \left\{ -\frac{22}{67}, 0, \frac{153}{67}, 0, \frac{136}{67}, 0, 0 \right\}, \right. \\ \left. \left\{ \{0, 0, 0, 0, 0, 0, 1\}, \left\{ \frac{32}{67}, 0, \frac{15}{67}, 0, -\frac{76}{67}, 1, 0 \right\}, \right. \right. \\ \left. \left. \{0, 0, 0, 1, 0, 0, 0\}, \{-2, 1, 0, 0, 0, 0, 0\} \right\} \right\}$$



## KAPITEL 4

### Unterräume des $\mathbb{R}^n$

#### 1. Die Definition eines Unterraums

Mengen, mit denen man so rechnen kann wie mit Vektoren, werden wir als *Vektorräume* bezeichnen. Wir behandeln zunächst den für die Geometrie wichtigsten Vektorraum, nämlich  $\mathbb{R}^3$ , und, in Verallgemeinerung davon, für jedes  $n \in \mathbb{N}$ , den Vektorraum

$$\mathbb{R}^n = \left\{ \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \mid x_1, x_2, \dots, x_n \in \mathbb{R} \right\}.$$

Für einen Vektor  $x \in \mathbb{R}^n$  und  $i \in \{1, 2, \dots, n\}$  schreiben wir  $x(i)$ ,  $x[i]$ , und  $x_i$  für den  $i$ -ten Eintrag von  $x$ .

Manche Teilmengen des  $\mathbb{R}^n$  sind abgeschlossen bezüglich der Addition von Vektoren und der Multiplikation mit reellen Zahlen. Solche Teilmengen bezeichnen wir als *Unterräume* des  $\mathbb{R}^n$ .

DEFINITION 4.1.  $T \subseteq \mathbb{R}^n$  ist *Unterraum* des  $\mathbb{R}^n$  : $\Leftrightarrow$

- (1) Die Menge  $T$  enthält zumindest ein Element.
- (2) Für alle  $\lambda \in \mathbb{R}$  und für alle  $t \in T$  gilt  $\lambda \cdot t \in T$ .
- (3) Für alle  $s, t \in T$  gilt  $s + t \in T$ .

Wir geben einige Beispiele von Unterräumen des  $\mathbb{R}^n$  :

BEISPIELE 4.2.

- (1)  $T_1 = \{(x, y) \in \mathbb{R}^2 \mid 2x - 3y = 0\}$  ist Unterraum des  $\mathbb{R}^2$ . Begründung: Wegen  $(0, 0) \in T_1$  ist die Menge  $T_1$  nicht leer. Sei  $(u, v) \in T_1$  und  $\lambda \in \mathbb{R}$ . Dann gilt  $2u - 3v = 0$  und damit  $2(\lambda u) - 3(\lambda v) = 0$ , also gilt  $\lambda \cdot (u, v) \in T_1$ . Für  $(u_1, v_1), (u_2, v_2) \in T_1$  gilt  $2 \cdot (u_1 + u_2) - 3 \cdot (v_1 + v_2) = 2u_1 - 3v_1 + 2u_2 - 3v_2 = 0$ , also ist  $(u_1, v_1) + (u_2, v_2) \in T_1$ .  
Damit haben wir gezeigt, dass  $T_1$  ein Unterraum des  $\mathbb{R}^2$  ist.
- (2)  $T_2 = \{(x, y) \in \mathbb{R}^2 \mid 3x + 2y = 1\}$  ist kein Unterraum des  $\mathbb{R}^2$ , denn  $(1, -1) \in T_2$ , aber  $2 \cdot (1, -1) \notin T_2$ .
- (3)  $T_3 = \{(x, y, z) \in \mathbb{R}^3 \mid \text{es gibt } s, t \in \mathbb{R}, \text{ sodass } (x, y, z) = s \cdot (1, -2, 4) + t \cdot (0, 1, 8)\}$  ist ein Unterraum des  $\mathbb{R}^3$ .

- (4)  $T_4 = \{(0, 0)\}$  ist Unterraum des  $\mathbb{R}^2$ .  
 (5)  $T_5 = \{(0, 1)\}$  ist kein Unterraum des  $\mathbb{R}^2$ , da  $2 \cdot (0, 1) \notin T_5$ .

### ÜBUNGSAUFGABEN 4.3.

- (1) Vervollständigen Sie die folgenden Begründungen dafür, dass die Menge

$$T = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \mid \text{es gibt } \alpha \in \mathbb{R}, \text{ sodass } \begin{pmatrix} x \\ y \end{pmatrix} = \alpha \cdot \begin{pmatrix} -2 \\ 1 \end{pmatrix} \right\}$$

die Unterraumeigenschaften (V1) und (V2) erfüllt.

(a)  $T$  ist nicht die leere Menge, weil \_\_\_\_\_.

(b) Für alle  $\lambda \in \mathbb{R}$  und  $t \in T$  liegt  $\lambda \cdot t$  in  $T$ : Wir fixieren  $t$  aus  $T$  und  $\lambda \in \mathbb{R}$ . Wir wollen zeigen, dass \_\_\_\_\_ in \_\_\_\_\_ liegt. Da  $t$  in  $T$  liegt, gibt es ein  $\alpha \in \mathbb{R}$ , sodass  $t = \alpha \cdot \begin{pmatrix} -2 \\ 1 \end{pmatrix}$ . Um zu zeigen, dass  $\lambda \cdot t$  in  $T$  liegt, müssen wir ein  $\alpha' \in \mathbb{R}$  finden, sodass

$$\lambda \cdot t = \alpha' \cdot \underline{\hspace{2cm}}$$

Nun wissen wir, dass  $t = \alpha \cdot \begin{pmatrix} -2 \\ 1 \end{pmatrix}$  ist. Daher gilt  $\lambda \cdot t = \underline{\hspace{2cm}}$ . Das heißt, dass für  $\alpha' = \underline{\hspace{2cm}}$  gilt:

$$\lambda \cdot t = \alpha' \cdot \begin{pmatrix} -2 \\ 1 \end{pmatrix}.$$

Daher liegt auch \_\_\_\_\_ in  $T$ .

- (2) Welche der folgenden Mengen sind Unterräume des Vektorraumes  $\mathbb{R}^2$ ? Geben Sie jeweils an, welche Unterraumeigenschaften erfüllt sind.  
 (a)  $\left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2 \mid 3x + 2y = 0 \right\}$ .  
 (b)  $\left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2 \mid 3x + 2y = 1 \right\}$ .
- (3) Welche der folgenden Mengen sind Unterräume des Vektorraumes  $\mathbb{R}^2$ ? Geben Sie jeweils an, welche Unterraumeigenschaften erfüllt sind.  
 (a)  $\left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2 \mid \exists \lambda \in \mathbb{R} : \begin{pmatrix} x \\ y \end{pmatrix} = \lambda \cdot \begin{pmatrix} 1 \\ 3 \end{pmatrix} \right\}$ .  
 (b)  $\left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2 \mid \exists \lambda \in \mathbb{R} : \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -4 \\ -12 \end{pmatrix} + \lambda \cdot \begin{pmatrix} 1 \\ 3 \end{pmatrix} \right\}$ .
- (4) Welche der folgenden Mengen sind Unterräume des Vektorraumes  $\mathbb{R}^2$ ? Geben Sie jeweils an, welche Unterraumeigenschaften erfüllt sind.  
 (a)  $\left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2 \mid x + 3y \leq 0 \right\}$ .  
 (b)  $\left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2 \mid x^4 + y^2 = 0 \right\}$ .
- (5) Zeigen Sie: Wenn ein Unterraum des  $\mathbb{R}^n$  ( $\mathbb{R}^n$  als Vektorraum über  $\mathbb{R}$ ) zwei Punkte enthält, so enthält er bereits die gesamte Verbindungsgerade.

Die Lösungsmenge eines linearen Gleichungssystems mit rechter Seite = 0 ist immer ein Unterraum.

**SATZ 4.4.** Seien  $m, n \in \mathbb{N}$ , und sei  $A$  eine  $m \times n$ -Matrix. Dann ist die Lösungsmenge des Gleichungssystems  $A \cdot x = 0$  ein Unterraum des  $\mathbb{R}^n$ .

*Beweis.* Sei  $U = \{x \mid A \cdot x = 0\}$ .

- (1) Wegen  $0 \in U$  ist  $U$  nicht die leere Menge.  
 (2) Sei  $x \in U$ ,  $\lambda \in \mathbb{R}$ . Dann gilt  $\lambda \cdot (A \cdot x) = A \cdot (\lambda \cdot x) = 0$ , d.h.  $\lambda \cdot x \in U$ .  
 (3) Seien  $u, v \in U$ . Dann gilt  $A \cdot (u + v) = A \cdot u + A \cdot v = 0$ , d.h.  $u + v \in U$ .

Somit ist  $U$  ein Unterraum des  $\mathbb{R}^n$ . ■

**AUFGABE 4.5.** Wir bestimmen diesen Unterraum für die Matrix  $A = \begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 3 \end{pmatrix}$ . Als

Lösungsmenge von  $A \cdot x = 0$  erhalten wir

$$L = \{(-2t, -3t, t) \mid t \in \mathbb{R}\}.$$

## 2. Die lineare Hülle von Vektoren

DEFINITION 4.6. Sei  $m \in \mathbb{N}_0$ , und seien  $v_1, \dots, v_m \in \mathbb{R}^n$ . Die Menge

$$L(v_1, \dots, v_m) := \left\{ \sum_{i=1}^m \lambda_i \cdot v_i \mid \lambda_1, \dots, \lambda_m \in \mathbb{R} \right\}$$

heißt die *lineare Hülle* der Vektoren  $v_1, \dots, v_m$ .

$L\left(\begin{pmatrix} 3 \\ 2 \end{pmatrix}\right)$  ist also die Gerade im  $\mathbb{R}^2$ , die durch  $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$  und  $\begin{pmatrix} 6 \\ 4 \end{pmatrix}$  geht.  $L(\cdot)$  definiert man als  $\{\vec{0}\}$ .

Die lineare Hülle von  $v_1, \dots, v_m$  ist der kleinste Unterraum, der  $v_1, \dots, v_m$  enthält:

SATZ 4.7. Sei  $m \in \mathbb{N}_0$ ,  $n \in \mathbb{N}$ , und seien  $v_1, \dots, v_m$  Vektoren im  $\mathbb{R}^n$ . Dann gilt

- (1)  $L(v_1, \dots, v_m)$  ist ein Unterraum des  $\mathbb{R}^n$ .
- (2) Sei  $M$  ein Unterraum der  $v_1, \dots, v_m$  enthält. Dann gilt  $L(v_1, \dots, v_m) \subseteq M$ .

Wollen wir etwa überprüfen, ob z.B.  $(3, 0, 1)$  in der linearen Hülle von  $(2, 1, -3)$  und  $(7, 2, -5)$  liegt, müssen wir ein Gleichungssystem lösen:

$$\lambda_1 \cdot \begin{pmatrix} 2 \\ 1 \\ -3 \end{pmatrix} + \lambda_2 \cdot \begin{pmatrix} 7 \\ 2 \\ -5 \end{pmatrix} = \begin{pmatrix} 3 \\ 0 \\ 1 \end{pmatrix},$$

das heißt

$$\begin{pmatrix} 2 & 7 \\ 1 & 2 \\ -3 & -5 \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \lambda_2 \end{pmatrix} = \begin{pmatrix} 3 \\ 0 \\ 1 \end{pmatrix}.$$

Lösen wir dieses System, so erhalten wir  $\lambda_1 = -2$  und  $\lambda_2 = 1$ . Also ist  $(3, 0, 1)$  eine Linearkombination von  $(2, 1, -3)$  und  $(7, 2, -5)$ , und liegt somit in der linearen Hülle dieser beiden Vektoren.

SATZ 4.8. Seien  $m, n \in \mathbb{N}$ , seien  $b_1, b_2, \dots, b_m$  Vektoren im  $\mathbb{R}^n$ , und sei  $\bar{B} = (b_1, b_2, \dots, b_m)$  die Matrix mit den Vektoren  $b_1, b_2, \dots, b_m$  als Spaltenvektoren. Dann liegt  $v$  genau dann in  $L(b_1, \dots, b_m)$ , wenn das Gleichungssystem  $\bar{B} \cdot x = v$  eine Lösung  $x \in \mathbb{R}^m$  hat.

### ÜBUNGSAUFGABEN 4.9.

- (1) Liegt  $\begin{pmatrix} 2 \\ -1 \end{pmatrix}$  in der linearen Hülle von  $\begin{pmatrix} 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} -2 \\ -4 \end{pmatrix}$ ?
- (2) Liegt  $\begin{pmatrix} 1 \\ -5 \end{pmatrix}$  in der linearen Hülle von  $\begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ 3 \end{pmatrix}, \begin{pmatrix} 1 \\ 4 \end{pmatrix}$ ?
- (3) Testen Sie, ob  $\begin{pmatrix} 7 \\ -2 \end{pmatrix}$  in der linearen Hülle von  $\begin{pmatrix} 1 \\ 0 \\ -2 \end{pmatrix}, \begin{pmatrix} -2 \\ 0 \\ 4 \end{pmatrix}, \begin{pmatrix} 3 \\ 1 \\ 0 \end{pmatrix}$  liegt.

Sei nun  $n \in \mathbb{N}$  eine natürliche Zahl, und sei  $M$  eine (möglicherweise unendliche) Teilmenge von  $\mathbb{R}^n$ . Wir definieren die lineare Hülle von  $M$  als

$$L(M) = \left\{ \sum_{i=1}^k \lambda_i \cdot m_i \mid k \in \mathbb{N}_0, \lambda_1, \dots, \lambda_k \in \mathbb{R}, m_1, \dots, m_k \in M \right\}.$$

Die lineare Hülle von  $M$  ist also die Menge aller Linearkombinationen endlich vieler Vektoren aus  $M$ .

DEFINITION 4.10. Für eine  $m \times n$ -Matrix  $A$  mit Einträgen aus  $\mathbb{R}$  definieren wir ihren *Zeilenraum*  $Z(A)$  als die lineare Hülle der Zeilen von  $A$ . Der Zeilenraum ist ein Unterraum von  $\mathbb{R}^n$ .

Den *Spaltenraum*  $S(A)$  definieren wir als die lineare Hülle der Spalten von  $A$ . Der Spaltenraum ist ein Unterraum von  $\mathbb{R}^m$ .

Den *Nullraum*  $N(A)$  definieren wir als die Lösungsmenge des Gleichungssystems  $A \cdot x = 0$ . Er ist ein Unterraum des  $\mathbb{R}^n$ .

### 3. Die lineare Unabhängigkeit von Vektoren

DEFINITION 4.11. Seien  $m, n \in \mathbb{N}$ , und seien  $v_1, \dots, v_m$  in  $\mathbb{R}^n$ . Die Folge  $(v_1, \dots, v_m)$  heißt *linear unabhängig*, wenn für alle  $\lambda_1, \dots, \lambda_m \in \mathbb{R}$  mit

$$\sum_{i=1}^m \lambda_i \cdot v_i = \lambda_1 \cdot v_1 + \dots + \lambda_m \cdot v_m = 0$$

gilt, dass alle  $\lambda_i = 0$  sind.

Man sagt dann oft auch einfach, dass die Vektoren  $v_1, \dots, v_m$  linear unabhängig sind. Als Spezialfall definiert man noch für  $m = 0$ , dass die Folge  $()$  aus 0 Vektoren immer linear unabhängig ist.

Vektoren  $v_1, \dots, v_m$ , die nicht linear unabhängig sind, nennt man *linear abhängig*. Die Folge  $(v_1, \dots, v_m)$  ist also genau dann linear abhängig, wenn es  $(\lambda_1, \dots, \lambda_m) \neq (0, \dots, 0)$  gibt, sodass  $\sum_{i=1}^m \lambda_i \cdot v_i = 0$ .

AUFGABE 4.12. Sind  $(3, 2)$  und  $(1, 3)$  linear unabhängig ?

*Lösung.* Wir betrachten

$$\lambda_1 \cdot \begin{pmatrix} 3 \\ 2 \end{pmatrix} + \lambda_2 \cdot \begin{pmatrix} 1 \\ 3 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \lambda_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Dieses System besitzt nur die Lösung  $(0, 0)$ . Daher sind die beiden Vektoren linear unabhängig.

AUFGABE 4.13. Sind  $(3, 2)$ ,  $(1, 4)$  und  $(5, 3)$  linear unabhängig ?

*Lösung.* Hier erhalten wir

$$\lambda_1 \cdot \begin{pmatrix} 3 \\ 2 \end{pmatrix} + \lambda_2 \cdot \begin{pmatrix} 1 \\ 4 \end{pmatrix} + \lambda_3 \cdot \begin{pmatrix} 5 \\ 3 \end{pmatrix} = \begin{pmatrix} 3 & 1 & 5 \\ 2 & 4 & 3 \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$



Eine Lösung des Gleichungssystems ist  $\lambda_1 = -1.7$ ,  $\lambda_2 = 0.1$  und  $\lambda_3 = 1$ . Die drei Vektoren sind also linear abhängig.

**SATZ 4.14.** Seien  $m, n \in \mathbb{N}$ , seien  $b_1, b_2, \dots, b_m$  Vektoren im  $\mathbb{R}^n$ , und sei  $\bar{B} = (b_1, b_2, \dots, b_m)$  die Matrix mit den Vektoren  $b_1, b_2, \dots, b_m$  als Spaltenvektoren. Dann sind  $(b_1, b_2, \dots, b_m)$  genau dann linear abhängig, wenn das System  $\bar{B} \cdot x = 0$  eine Lösung  $x \neq 0$  hat.

**SATZ 4.15.** Sei  $m \geq 1$  und seien  $b_1, \dots, b_m \in \mathbb{R}^n$ . Die folgenden zwei Aussagen sind äquivalent:

- (1)  $(b_1, \dots, b_m)$  ist linear abhängig.
- (2) Es gibt ein  $k \in \{1, \dots, m\}$ , sodass  $b_k$  in  $L(b_1, \dots, b_{k-1})$  liegt.

**SATZ 4.16.** Sei  $m \in \mathbb{N}_0$ , sei  $n \in \mathbb{N}$ , und seien  $v_1, \dots, v_m, v \in \mathbb{R}^n$ . Wir nehmen an, dass  $v_1, \dots, v_m$  linear unabhängig sind. Dann sind äquivalent:

- (1)  $v \in L(v_1, \dots, v_m)$ .
- (2)  $(v_1, \dots, v_m, v)$  ist linear abhängig.

#### ÜBUNGSAUFGABEN 4.17.

- (1) Zeigen Sie, dass die Vektoren  $\begin{pmatrix} 1 \\ 4 \\ -2 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ 10 \\ -10 \end{pmatrix}$  linear abhängig sind, indem Sie eine Linearkombination finden, bei der nicht jeder Vektor 0 mal genommen wird, und die trotzdem den Nullvektor ergibt.
- (2) Testen Sie jeweils, ob folgende Mengen von Vektoren linear abhängig sind. Finden Sie, falls die Vektoren linear abhängig sind, eine Linearkombination, die den Nullvektor ergibt, und bei der nicht jeder Vektor 0 mal genommen wird.
  - (a)  $\begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ 3 \end{pmatrix}, \begin{pmatrix} 1 \\ 4 \end{pmatrix}$ .
  - (b)  $\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \\ -2 \end{pmatrix}, \begin{pmatrix} -1 \\ 2 \\ 2 \end{pmatrix}$ .
- (3) Sind  $\begin{pmatrix} 3 \\ 4 \\ -5 \end{pmatrix}, \begin{pmatrix} -2 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 16 \\ 8 \\ -25 \end{pmatrix}$  linear abhängig?
- (4) Sind die Vektoren  $\begin{pmatrix} 1 \\ 4 \\ -2 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ 10 \\ -8 \end{pmatrix}$  linear abhängig?
- (5) Geben Sie einen Vektor  $v \in \mathbb{R}^2$  an, sodass  $\begin{pmatrix} -1 \\ 3 \end{pmatrix}$  und  $v$  linear abhängig sind.
- (6) Finden Sie drei Vektoren  $a, b, c \in \mathbb{R}^3$ , sodass  $(b, c)$  linear unabhängig und  $(a, b, c)$  linear abhängig sind.
- (7) Vervollständigen Sie die Begründung für folgende Aussage.  
Seien  $v_1, v_2, w \in \mathbb{R}^n$  so, dass  $w$  in der linearen Hülle von  $v_1$  und  $v_2$  liegt. Dann sind  $(v_1, v_2, w)$  linear abhängig.

*Begründung:* Da  $w$  in der linearen Hülle von  $v_1$  und  $v_2$  liegt, gibt es  $\lambda_1, \lambda_2 \in \mathbb{R}$ , sodass

$$w = \underline{\hspace{10em}}$$

Daher gilt

$$\lambda_1 \cdot v_1 + \lambda_2 \cdot v_2 + \underline{\hspace{2em}} = 0.$$

Das ist eine Linearkombination, die 0 ergibt, obwohl nicht jeder Vektor  $\underline{\hspace{10em}}$  mal genommen wurde. Daher sind  $(v_1, v_2, w)$   $\underline{\hspace{10em}}$ .

## 4. Basen eines Vektorraums

### 4.1. Definition.

**DEFINITION 4.18.** Sei  $T$  Unterraum von  $\mathbb{R}^n$ . Die Folge  $B = (b_1, \dots, b_m)$  heißt Basis von  $T$  : $\Leftrightarrow$

- (1)  $b_1, \dots, b_m$  sind linear unabhängig,  
 (2)  $L(b_1, \dots, b_m) = T$ .

Wir geben einige Beispiele:

BEISPIEL 4.19.

- (1)  $\{(1, 0), (0, 1)\}$  ist Basis des  $\mathbb{R}^2$ : Jeder Vektor  $\begin{pmatrix} x \\ y \end{pmatrix}$  lässt sich als

$$x \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} + y \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

schreiben, und liegt somit in der linearen Hülle von  $(1, 0)$  und  $(0, 1)$ . Somit ist die lineare Hülle der Vektoren  $\{(1, 0), (0, 1)\}$  der ganze  $\mathbb{R}^2$ . Die beiden Vektoren sind außerdem linear unabhängig.

- (2)  $\{(2, 3)\}$  ist keine Basis des  $\mathbb{R}^2$ , da es kein  $\lambda$  gibt, sodass  $\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \lambda \cdot \begin{pmatrix} 2 \\ 3 \end{pmatrix}$ .  
 (3)  $\{(2, 3)\}$  ist Basis von  $L((2, 3))$ .

Sei  $U$  ein Unterraum des  $\mathbb{R}^n$ . Dann ist eine Basis eine Möglichkeit, die Menge  $U$  anzugeben. Mathematica nutzt das, um die Lösungen des Gleichungssystems  $A \cdot x = 0$  durch die Funktion `NullSpace` auszugeben. Dabei wird der unendliche Raum  $U = \{x \in \mathbb{R}^n \mid A \cdot x = 0\}$  durch eine Basis dieses Raums angegeben.

```
In[50]:= A = {{1, 2, 3}}
```

```
Out[50]= {{1, 2, 3}}
```

```
In[51]:= NullSpace[A]
```

```
Out[51]= {{-3, 0, 1}, {-2, 1, 0}}
```

ÜBUNGSAUFGABEN 4.20.

- (1) Finden Sie eine Basis  $B$  der Ebene  $L\left(\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \\ 2 \end{pmatrix}\right)$ , die weder  $\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$  noch  $\begin{pmatrix} 1 \\ -1 \\ 2 \end{pmatrix}$  enthält.

**4.2. Bestimmen der Basis eines Unterraums.** Wir können Unterräume des  $\mathbb{R}^n$  auf zwei Arten angeben.

- explizit, das heißt, als lineare Hülle von Vektoren.
- implizit, das heißt, durch ein Gleichungssystem, dessen Lösungsmenge der anzugebende Unterraum ist.

Wir überlegen uns als erstes, wie wir eine Basis eines explizit gegebenen Unterraums berechnen können. Dazu berechnen wir die Basis des Raums

$$V = L\left(\begin{pmatrix} -5 \\ 3 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} -33 \\ 17 \\ 1 \\ -1 \end{pmatrix}, \begin{pmatrix} 85 \\ -44 \\ -3 \\ 2 \end{pmatrix}, \begin{pmatrix} -19 \\ 10 \\ 1 \\ 0 \end{pmatrix}\right).$$

Wir wollen also eine Basis des Zeilenraums der Matrix

$$\begin{pmatrix} -5 & 3 & 1 & 1 \\ -33 & 17 & 1 & -1 \\ 85 & -44 & -3 & 2 \\ -19 & 10 & 1 & 0 \end{pmatrix}$$

bestimmen. Der Zeilenraum ändert sich nicht, wenn wir eine Zeile mit einer von 0 verschiedenen Zahl multiplizieren, oder wenn wir zu einer Zeile ein Vielfaches einer anderen Zeile addieren. Wir können uns also jetzt systematisch Matrizen erzeugen, die alle den gleichen Zeilenraum haben wie die ursprüngliche Matrix. Das machen wir mit Mathematica.

```
In[52]:= << RowRed9.m
```

```
In[53]:= RowEchelonForm[{{-5, 3, 1, 1}, {-33, 17, 1, -1}, {85, -44, -3, 2}, {-19, 10, 1, 0}}]
```

$$\begin{pmatrix} -5 & 3 & 1 & 1 \\ -33 & 17 & 1 & -1 \\ 85 & -44 & -3 & 2 \\ -19 & 10 & 1 & 0 \end{pmatrix}$$

$$\begin{pmatrix} -5 & 3 & 1 & 1 \\ 0 & -14 & -28 & -38 \\ 0 & 7 & 14 & 19 \\ 0 & -7 & -14 & -19 \end{pmatrix}$$

$$\begin{pmatrix} -5 & 3 & 1 & 1 \\ 0 & -14 & -28 & -38 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

```
Out[53]= {{{1, 0, 0, 0}, {-33, 5, 0, 0}, {1, 5, 2, 0}, {-5, -5, 0, 10}},
           {{-5, 3, 1, 1}, {0, -14, -28, -38}},
           {{0, 0, 0, 0}, {0, 0, 0, 0}}}
```

Wir haben also eine Matrix in Zeilenstufenform erzeugt, deren Zeilenraum der gleiche wie der Zeilenraum der gegebenen Matrix ist.

ALGORITHMUS 4.21 (Zeilenstaffelform).

Eingabe: Eine  $m \times n$ -Matrix  $A$ .

Ausgabe: Eine  $m \times n$ -Matrix  $B$ , sodass  $B$  in Zeilenstaffelform ist, und  $Z(A) = Z(B)$ .

```

1   $B \leftarrow A$ 
2   $zeile \leftarrow 1$ 
3   $spalte \leftarrow 1$ 
4  while  $zeile \leq m$ 
5      do while  $spalte \leq n$  und  $B(i, spalte) = 0$  für alle  $i$  mit  $zeile \leq i \leq m$ 
6          do  $spalte \leftarrow spalte + 1$ 
7          if  $spalte \leq n$ 
8              then  $gewaehlteZeile \leftarrow$  ein  $i$ , sodass  $zeile \leq i \leq m$  und  $B(i, spalte) \neq$ 
9                  0
10                 if  $gewaehlteZeile \neq zeile$ 
11                     then Vertausche die  $gewaehlteZeile$ -te mit der  $zeile$ -ten
12                     Zeile von  $B$ 
13                  $i \leftarrow zeile + 1$ 
14                 while  $i \leq m$ 
15                     do Addiere passendes Vielfaches der  $zeile$ -ten Zeile zur
16                      $i$ -ten Zeile von  $B$ , sodass  $B(i, spalte) = 0$ 
17                      $i \leftarrow i + 1$ 
18              $zeile \leftarrow zeile + 1$ 
19              $spalte \leftarrow spalte + 1$ 
20 return  $B$ 

```

Dieser Algorithmus liefert also folgenden Satz.

SATZ 4.22. Seien  $m, n \in \mathbb{N}$ , und sei  $A$  eine  $m \times n$ -Matrix. Dann gibt es eine Matrix  $B$  in Zeilenstaffelform, sodass  $Z(A) = Z(B)$ .

Die Zeilen einer Matrix in Zeilenstaffelform, die nicht 0 sind, sind linear unabhängig. Daher haben wir auch eine Basis von

$$V = L((-5, 3, 1, 1), (-33, 17, 1, -1), (85, -44, -3, 2), (-19, 10, 1, 0))$$

gefunden, nämlich

$$B = \left( \begin{pmatrix} -5 \\ 3 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ -14 \\ -28 \\ -38 \end{pmatrix} \right).$$

Wir fassen zusammen:

ALGORITHMUS 4.23 (Basis eines explizit gegebenen Unterraums).

Eingabe: Vektoren  $v_1, \dots, v_m \in \mathbb{R}^n$ .

Ausgabe: Eine Basis  $b_1, \dots, b_k$  von  $L(v_1, \dots, v_m)$ .

- 1 Bilde die  $m \times n$ -Matrix  $V$ , in deren Zeilen die Vektoren  $v_1, \dots, v_m$  stehen
- 2 Berechne eine Matrix  $B$  in Zeilenstaffelform, sodass  $Z(V) = Z(B)$

3 **return**  $(b_1, \dots, b_k)$  als jene Zeilen von  $B$ , die nicht 0 sind

Was wir noch nicht begründet haben ist, dass die Zeilen einer Matrix in Zeilenstaffelform, die nicht 0 sind, linear unabhängig sind. Betrachten wir dazu die Matrix

$$A = \begin{pmatrix} 1 & 2 & -3 & 0 & 6 & 7 & 0 \\ 0 & 0 & -5 & 0 & 14 & 17 & 0 \\ 0 & 0 & 0 & 0 & 67 & 76 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Um zu zeigen, dass die von 0 verschiedenen Zeilen von  $A$  linear unabhängig sind, müssen wir zeigen, dass das Gleichungssystem

$$\begin{pmatrix} 1 & 0 & 0 \\ 2 & 0 & 0 \\ -3 & -5 & 0 \\ 0 & 0 & 0 \\ 6 & 14 & 67 \\ 7 & 17 & 76 \\ 0 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

nur die Lösung  $(0, 0, 0)$  hat. Wir sehen, dass uns die erste Gleichung  $\lambda_1 = 0$ , dann die dritte Gleichung  $\lambda_2 = 0$ , und dann die fünfte Gleichung  $\lambda_3 = 0$  liefert.

Das machen wir jetzt allgemein:

**SATZ 4.24.** *Sei  $A$  eine  $m \times n$ -Matrix in Zeilenstaffelform. Dann sind die Zeilen von  $A$ , die nicht 0 sind, linear unabhängige Vektoren im  $\mathbb{R}^n$ .*

*Beweis.* Seien  $r \in \mathbb{N}$  und  $j_1 < j_2 < \dots < j_r$  wie in Definition 3.1. Wir betrachten eine Linearkombination der ersten  $r$  Zeilen von  $A$ , die 0 ist. Seien also  $(\lambda_1, \dots, \lambda_r) \in \mathbb{R}^r$  so, dass für alle  $k \in \{1, \dots, n\}$  gilt:

$$(4.1) \quad \sum_{l=1}^r \lambda_l \cdot A[l, k] = 0.$$

Wir zeigen jetzt, dass für alle  $i \in \{1, \dots, r\}$  gilt:  $\lambda_i = 0$ . Wir zeigen das mit Induktion nach  $i$ . Betrachten wir die Gleichung 4.1 für  $k := j_1$ . Dann gilt

$$\sum_{l=1}^r \lambda_l \cdot A[l, j_1] = 0.$$

Für  $l \geq 2$  gilt  $A[l, j_1] = 0$ , da Bedingung (3) von Definition 3.1 für  $i := l$  und  $k := j_1$  ergibt, dass  $A(l, j_1) = 0$ . Also gilt  $\lambda_1 \cdot A[1, j_1] = 0$ . Da  $A[1, j_1] \neq 0$ , gilt  $\lambda_1 = 0$ .

Sei nun  $i \in \{1, \dots, r\}$ . Wir nehmen an, dass  $\lambda_1 = \lambda_2 = \dots = \lambda_{i-1} = 0$ . Wir betrachten die Gleichung 4.1 für  $k := j_i$ . Es gilt dann

$$\sum_{l=1}^r \lambda_l \cdot A[l, j_i] = 0,$$

also

$$\lambda_i \cdot A[i, j_i] + \sum_{l=i+1}^r \lambda_l \cdot A[l, j_i] = 0.$$

Für  $l > i$  ergibt Bedingung (3) von Definition 3.1 (mit  $i' := l$  und  $k' := j_i$ ), dass  $A[l, j_i] = 0$  gilt. Also gilt  $\lambda_i \cdot A[i, j_i] = 0$ . Da  $A[i, j_i] \neq 0$ , gilt auch  $\lambda_i = 0$ .

Es ist also  $\lambda_1 = \lambda_2 = \dots = \lambda_r = 0$ . Also sind die ersten  $r$  Zeilen von  $A$  linear unabhängig. ■

#### ÜBUNGSAUFGABEN 4.25.

- (1) Bestimmen Sie eine Basis von  $L\left(\begin{pmatrix} 1 \\ 0 \\ -2 \end{pmatrix}, \begin{pmatrix} -2 \\ 0 \\ 4 \end{pmatrix}, \begin{pmatrix} 3 \\ -1 \\ 0 \end{pmatrix}\right)$ .
- (2) Finden Sie jeweils eine Basis folgender Unterräume!
  - (a)  $\left\{\begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathbb{R}^3 \mid x + 3y + z = 0\right\}$ .
  - (b)  $L\left(\begin{pmatrix} 1 \\ 4 \\ -5 \end{pmatrix}\right)$ .
  - (c)  $L\left(\begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 2 \\ 4 \end{pmatrix}, \begin{pmatrix} -2 \\ 4 \end{pmatrix}\right)$ .

### 5. Die Zeilenstaffelnormalform

Wir studieren folgendes Problem: Gegeben sind zwei Unterräume  $U, V$  von  $\mathbb{R}^n$ . Beide Unterräume sind explizit gegeben, das heißt, durch  $u_1, \dots, u_l$  und  $v_1, \dots, v_m$  so, dass  $U = L(u_1, \dots, u_l)$  und  $V = L(v_1, \dots, v_m)$ . Wir fragen uns nun, ob  $U = V$ .

**DEFINITION 4.26 (Zeilenstaffelnormalform).** Sei  $A$  eine  $m \times n$ -Matrix.  $A$  ist in *Zeilenstaffelnormalform*, wenn es  $r \in \mathbb{N}_0$  und  $j_1, j_2, \dots, j_r \in \{1, \dots, n\}$  gibt, sodass

- (1)  $j_r > j_{r-1} > \dots > j_1$ .
- (2) Für alle  $i \in \{1, 2, \dots, r\}$  gilt:  $A(i, j_i) = 1$ .
- (3) Für alle  $i \in \{1, 2, \dots, r\}$  und für alle  $k \in \{1, 2, \dots, r\}$  gilt: Wenn  $k \neq i$ , dann gilt  $A(k, j_i) = 0$ .
- (4) Für alle  $i \in \{1, 2, \dots, r\}$  und für alle  $k \in \{1, 2, \dots, n\}$  mit  $k < j_i$  gilt:  $A(i, k) = 0$ .
- (5) Für alle  $i \in \{1, 2, \dots, m\}$  mit  $i > r$  und für alle  $k \in \{1, 2, \dots, n\}$  gilt:  $A(i, k) = 0$ .

ALGORITHMUS 4.27 (Zeilenstaffelnormalform).

Eingabe: Eine  $m \times n$ -Matrix  $A$ .

Ausgabe: Eine  $m \times n$ -Matrix  $B$ , sodass  $B$  in Zeilenstaffelnormalform ist, und  $Z(A) = Z(B)$ .

```

1   $B \leftarrow A$ 
2   $zeile \leftarrow 1$ 
3   $spalte \leftarrow 1$ 
4  while  $zeile \leq m$ 
5      do (* Die ersten  $spalte - 1$  Spalten sind in Zeilenstaffelnormalform *)
6          while  $spalte \leq n$  und  $B(i, spalte) = 0$  für alle  $i$  mit  $zeile \leq i \leq m$ 
7              do  $spalte \leftarrow spalte + 1$ 
8          if  $spalte \leq n$ 
9              then  $gewaehlteZeile \leftarrow$  ein  $i$ , sodass  $zeile \leq i \leq m$  und  $B(i, spalte) \neq$ 
0
10                 if  $gewaehlteZeile \neq zeile$ 
11                     then Vertausche die  $gewaehlteZeile$ -te mit der  $zeile$ -ten
12                 Zeile von  $B$ 
13                 Multipliziere die  $zeile$ -te Zeile von  $B$  mit  $\frac{1}{B(zeile,spalte)}$ 
14                  $i \leftarrow 1$ 
15                 while  $i \leq m$ 
16                     do if  $i \neq zeile$ 
17                         then Addiere passendes Vielfaches der  $zeile$ -ten
18                         Zeile zur  $i$ -ten Zeile von  $B$ , sodass  $B(i, spalte) = 0$ 
19                          $i \leftarrow i + 1$ 
20                  $zeile \leftarrow zeile + 1$ 
21                  $spalte \leftarrow spalte + 1$ 
22 return  $B$ 

```

Wir geben einige Beispiele für das Berechnen einer Matrix in Zeilenstaffelnormalform, die den gleichen Zeilenraum wie die Ausgangsmatrix besitzt.

AUFGABE 4.28.

```
In[54] := << RowRed9.m
```

```
In[55] := MatrixForm[A1]
```

```
Out[55]= 
$$\begin{pmatrix} 1 & -5 & 8 & 2 & -2 \\ 1 & -4 & 6 & -2 & 0 \\ -1 & 0 & 2 & 2 & 0 \\ 5 & -8 & 6 & 0 & -5 \end{pmatrix}$$

```

```
In[56] := RowEchelonNormalForm[A1]
```

$$\begin{pmatrix} 1 & -5 & 8 & 2 & -2 \\ 1 & -4 & 6 & -2 & 0 \\ -1 & 0 & 2 & 2 & 0 \\ 5 & -8 & 6 & 0 & -5 \end{pmatrix}$$

$$\begin{pmatrix} 1 & -5 & 8 & 2 & -2 \\ 0 & 1 & -2 & -4 & 2 \\ 0 & -5 & 10 & 4 & -2 \\ 0 & 17 & -34 & -10 & 5 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & -2 & -18 & 8 \\ 0 & 1 & -2 & -4 & 2 \\ 0 & 0 & 0 & -16 & 8 \\ 0 & 0 & 0 & 58 & -29 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & -2 & -18 & 8 \\ 0 & 1 & -2 & -4 & 2 \\ 0 & 0 & 0 & 1 & -\frac{1}{2} \\ 0 & 0 & 0 & 58 & -29 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & -2 & 0 & -1 \\ 0 & 1 & -2 & 0 & 0 \\ 0 & 0 & 0 & 1 & -\frac{1}{2} \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\begin{aligned} \text{Out}[56] = & \{ \{ \frac{1}{2}, -\frac{5}{8}, -\frac{9}{8}, 0 \}, \{ 0, -\frac{1}{4}, -\frac{1}{4}, 0 \}, \\ & \{ \frac{1}{4}, -\frac{5}{16}, -\frac{1}{16}, 0 \}, \{ -\frac{5}{2}, \frac{9}{8}, \frac{29}{8}, 1 \} \}, \{ \{ 1, 0, -2, 0, -1 \}, \\ & \{ 0, 1, -2, 0, 0 \}, \{ 0, 0, 0, 1, -\frac{1}{2} \}, \{ 0, 0, 0, 0, 0 \} \} \end{aligned}$$

#### AUFGABE 4.29.

`In[57]:= << RowRed9.m`

`In[58]:= MatrixForm[A2]`

$$\text{Out}[58] = \begin{pmatrix} 1 & 5 & 7 & 9 \\ 2 & 10 & 14 & 18 \\ 3 & 2 & 1 & 0 \end{pmatrix}$$

`In[59]:= RowEchelonNormalForm[A2]`

$$\begin{pmatrix} 1 & 5 & 7 & 9 \\ 2 & 10 & 14 & 18 \\ 3 & 2 & 1 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 5 & 7 & 9 \\ 0 & 0 & 0 & 0 \\ 0 & -13 & -20 & -27 \end{pmatrix}$$



$$\begin{pmatrix} 1 & 5 & 7 & 9 \\ 0 & -13 & -20 & -27 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 5 & 7 & 9 \\ 0 & 1 & \frac{20}{13} & \frac{27}{13} \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & -\frac{9}{13} & -\frac{18}{13} \\ 0 & 1 & \frac{20}{13} & \frac{27}{13} \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\text{Out}[59] = \left\{ \left\{ \left\{ -\frac{2}{13}, 0, \frac{5}{13} \right\}, \left\{ \frac{3}{13}, 0, -\frac{1}{13} \right\}, \{-2, 1, 0\} \right\}, \right. \\ \left. \left\{ \left\{ 1, 0, -\frac{9}{13}, -\frac{18}{13} \right\}, \left\{ 0, 1, \frac{20}{13}, \frac{27}{13} \right\}, \{0, 0, 0, 0\} \right\} \right\}$$

AUFGABE 4.30.

`In[60]:= << RowRed9.m`

`In[61]:= MatrixForm [A3]`

$$\text{Out}[61] = \begin{pmatrix} 1 & 5 & 3 \\ 2 & 10 & 8 \\ 4 & 20 & 15 \\ 1 & 6 & 5 \end{pmatrix}$$

`In[62]:= RowEchelonNormalForm [A3]`

$$\begin{pmatrix} 1 & 5 & 3 \\ 2 & 10 & 8 \\ 4 & 20 & 15 \\ 1 & 6 & 5 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 5 & 3 \\ 0 & 0 & 2 \\ 0 & 0 & 3 \\ 0 & 1 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 5 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 3 \\ 0 & 0 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & -7 \\ 0 & 1 & 2 \\ 0 & 0 & 3 \\ 0 & 0 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & -7 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \\ 0 & 0 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

$$\begin{aligned} \text{Out}[62] = & \{ \{ \{-\frac{10}{3}, 0, \frac{7}{3}, -5\}, \{\frac{5}{3}, 0, -\frac{2}{3}, 1\}, \\ & \{-\frac{4}{3}, 0, \frac{1}{3}, 0\}, \{\frac{2}{3}, 1, -\frac{2}{3}, 0\} \}, \\ & \{ \{1, 0, 0\}, \{0, 1, 0\}, \{0, 0, 1\}, \{0, 0, 0\} \} \} \end{aligned}$$

AUFGABE 4.31.

`In[63]:= << RowRed9.m`

`In[64]:= MatrixForm[A5]`

$$\text{Out}[64] = \begin{pmatrix} 1 & 2 & -3 & 0 & 6 & 7 & 0 \\ -2 & -4 & 1 & 0 & 2 & 3 & 0 \\ 4 & 8 & 1 & 0 & 1 & -1 & 0 \\ 3 & 6 & -1 & 0 & 9 & 9 & 0 \end{pmatrix}$$

`In[65]:= RowEchelonNormalForm[A5]`

$$\begin{pmatrix} 1 & 2 & -3 & 0 & 6 & 7 & 0 \\ -2 & -4 & 1 & 0 & 2 & 3 & 0 \\ 4 & 8 & 1 & 0 & 1 & -1 & 0 \\ 3 & 6 & -1 & 0 & 9 & 9 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & -3 & 0 & 6 & 7 & 0 \\ 0 & 0 & -5 & 0 & 14 & 17 & 0 \\ 0 & 0 & 13 & 0 & -23 & -29 & 0 \\ 0 & 0 & 8 & 0 & -9 & -12 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & -3 & 0 & 6 & 7 & 0 \\ 0 & 0 & 1 & 0 & -\frac{14}{5} & -\frac{17}{5} & 0 \\ 0 & 0 & 13 & 0 & -23 & -29 & 0 \\ 0 & 0 & 8 & 0 & -9 & -12 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 0 & 0 & -\frac{12}{5} & -\frac{16}{5} & 0 \\ 0 & 0 & 1 & 0 & -\frac{14}{5} & -\frac{17}{5} & 0 \\ 0 & 0 & 0 & 0 & \frac{67}{5} & \frac{76}{5} & 0 \\ 0 & 0 & 0 & 0 & \frac{67}{5} & \frac{76}{5} & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 0 & 0 & -\frac{12}{5} & -\frac{16}{5} & 0 \\ 0 & 0 & 1 & 0 & -\frac{14}{5} & -\frac{17}{5} & 0 \\ 0 & 0 & 0 & 0 & 1 & \frac{76}{67} & 0 \\ 0 & 0 & 0 & 0 & \frac{67}{5} & \frac{76}{5} & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 0 & 0 & 0 & -\frac{32}{67} & 0 \\ 0 & 0 & 1 & 0 & 0 & -\frac{15}{67} & 0 \\ 0 & 0 & 0 & 0 & 1 & \frac{76}{67} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\text{Out}[65]= \left\{ \left\{ \left\{ \frac{1}{67}, -\frac{9}{67}, \frac{12}{67}, 0 \right\}, \left\{ -\frac{10}{67}, \frac{23}{67}, \frac{14}{67}, 0 \right\}, \right. \right. \\
 \left. \left. \left\{ \frac{6}{67}, \frac{13}{67}, \frac{5}{67}, 0 \right\}, \{-1, -1, -1, 1\} \right\}, \right. \\
 \left. \left\{ \left\{ 1, 2, 0, 0, 0, -\frac{32}{67}, 0 \right\}, \left\{ 0, 0, 1, 0, 0, -\frac{15}{67}, 0 \right\}, \right. \right. \\
 \left. \left. \left\{ 0, 0, 0, 0, 1, \frac{76}{67}, 0 \right\}, \{0, 0, 0, 0, 0, 0, 0\} \right\} \right\}$$

Der Algorithmus liefert den folgenden Satz.

**SATZ 4.32.** Seien  $m, n \in \mathbb{N}$ , und sei  $A$  eine  $m \times n$ -Matrix. Dann gibt es eine Matrix  $B$  in Zeilenstaffelnormform, sodass  $Z(A) = Z(B)$ .

Mathematica hat einen eigenen Befehl zur Berechnung der Zeilenstaffelnormform, nämlich `RowReduce`.

$$\text{In}[66]:= \text{MatrixForm}[\mathbf{A1}]$$

$$\text{Out}[66]= \begin{pmatrix} 1 & -5 & 8 & 2 & -2 \\ 1 & -4 & 6 & -2 & 0 \\ -1 & 0 & 2 & 2 & 0 \\ 5 & -8 & 6 & 0 & -5 \end{pmatrix}$$

$$\text{In}[67]:= \text{MatrixForm}[\text{RowReduce}[\mathbf{A1}]]$$

$$\text{Out}[67]= \begin{pmatrix} 1 & 0 & -2 & 0 & -1 \\ 0 & 1 & -2 & 0 & 0 \\ 0 & 0 & 0 & 1 & -\frac{1}{2} \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

## 6. Der Nullraum einer Matrix

Wir überlegen uns jetzt, wie wir eine Basis eines implizit gegebenen Unterraums des  $\mathbb{R}^n$  berechnen.

**DEFINITION 4.33 (Skalarprodukt).** Seien  $v = (v_1, \dots, v_n)$  und  $w = (w_1, \dots, w_n) \in \mathbb{R}^n$ . Wir definieren das Skalarprodukt  $\langle v, w \rangle$  durch

$$\langle v, w \rangle = \sum_{i=1}^n v_i w_i.$$

**DEFINITION 4.34.** Sei  $M$  eine Teilmenge des  $\mathbb{R}^n$ . Dann definieren wir

$$M^\wedge := \{v \in \mathbb{R}^n \mid \langle m, v \rangle = 0 \text{ für alle } m \in M\}.$$

SATZ 4.35. Sei  $A$  eine  $m \times n$ -Matrix. Dann gilt  $N(A) = (Z(A))^\wedge$ .

KOROLLAR 4.36. Sei  $A$  eine  $l \times n$ , und sei  $B$  eine  $m \times n$ -Matrix. Wenn  $Z(A) = Z(B)$ , dann gilt auch  $N(A) = N(B)$ .

Wenn eine Matrix  $B$  in Zeilenstaffelnormalform ist, dann kann man ihren Nullraum  $N(B)$  besonders schnell berechnen.

SATZ 4.37. Sei  $B$  eine  $m \times n$ -Matrix in Zeilenstaffelnormalform, seien  $j_1 < j_2 < \dots < j_r \in \{1, 2, \dots, n\}$  wie in Definition 4.26. Seien  $i_1 < i_2 < \dots < i_{n-r} \in \{1, 2, \dots, n\}$  so, dass  $\{i_1, \dots, i_{n-r}\} \cup \{j_1, \dots, j_r\} = \{1, 2, \dots, n\}$ . Sei  $C$  eine  $(n-r) \times n$ -Matrix, die so definiert ist: Für alle  $k \in \{1, 2, \dots, n-r\}$  gilt:

- $C(k, i_k) = 1$ ,
- für alle  $s \in \{1, \dots, r\}$ :  $C(k, j_s) = -B(s, i_k)$ , und
- für alle  $l \in \{i_1, i_2, \dots, i_{n-r}\} \setminus \{i_k\}$ :  $C(k, l) = 0$ .

Dann steht in den Zeilen von  $C$  eine Basis des Nullraumes von  $B$ .

*Beweis.* Wir zeigen als erstes, dass jede Zeile von  $C$  im Nullraum von  $B$  liegt. Sei dazu  $c$  die  $k$ -te Zeile von  $C$ . Wir berechnen jetzt  $B \cdot c$  (dazu stellen wir uns  $c$  als Spaltenvektor vor). Für  $t \in \{1, \dots, r\}$  berechnen wir den  $t$ -ten Eintrag von  $B \cdot c$ . Wir erhalten:

$$\begin{aligned}
 (B \cdot c)[t] &= \sum_{l=1}^n B[t, l] \cdot c[l] \\
 &= \sum_{l=1}^n B[t, l] \cdot C[k, l] \\
 &= B[t, i_k] \cdot C[k, i_k] + \sum_{s=1}^r B[t, j_s] \cdot C[k, j_s] + \sum_{l \in \{i_1, i_2, \dots, i_{n-r}\} \setminus \{i_k\}} B[t, l] \cdot C[k, l] \\
 &= B[t, i_k] \cdot 1 + 1 \cdot C[k, j_t] + 0 \\
 &= B[t, i_k] - B[t, i_k] = 0.
 \end{aligned}$$

Daher gilt  $Z(C) \subseteq N(B)$ .

Bevor wir die Inklusion  $N(B) \subseteq Z(C)$  beweisen, zeigen wir als Vorbereitung folgende Aussage:

Wenn

$$x = (x(1), x(2), \dots, x(n))$$

und

$$y = (y(1), y(2), \dots, y(n))$$

Vektoren in  $\mathbb{R}^n$  sind, sodass  $B \cdot x = 0$ , und  $B \cdot y = 0$  und  $x(i_l) = y(i_l)$  für alle  $l \in \{1, 2, \dots, n-r\}$  gilt, so gilt  $x = y$ .

Das begründen wir so: wir zeigen, dass  $x$  und  $y$  auch an den Stellen  $j_1, \dots, j_r$  übereinstimmen. Sei also  $k \in \{1, \dots, r\}$ . Dann gilt

$$\sum_{j=1}^n B(k, j) \cdot x(j) = 0.$$

Das bedeutet

$$B(k, j_k) \cdot x(j_k) + \sum_{s \in \{1, \dots, r\} \setminus \{k\}} B(k, j_s) \cdot x(j_s) = - \sum_{l=1}^{n-r} B(k, i_l) \cdot x(i_l),$$

also

$$x(j_k) = - \sum_{l=1}^{n-r} B(k, i_l) \cdot x(i_l).$$

Ebenso errechnen wir  $y(j_k) = - \sum_{l=1}^{n-r} B(k, i_l) \cdot y(i_l)$ . Also gilt  $x = y$ .

Nach dieser Vorbereitung zeigen wir  $N(B) \subseteq Z(C)$ . Sei dazu  $x \in N(B)$ . Wir setzen

$$\alpha = (\alpha(1), \dots, \alpha(n-r)) := (x(i_1), \dots, x(i_{n-r}))$$

und

$$y := C^T \cdot \alpha.$$

Da  $B \cdot C^T = 0$ , gilt  $B \cdot y = 0$ . Wir zeigen nun, dass für alle  $l \in \{1, 2, \dots, n-r\}$  gilt:

$$y(i_l) = x(i_l).$$

Dazu berechnen wir

$$\begin{aligned} y(i_l) &= (C^T \cdot \alpha)[i_l] \\ &= \sum_{k=1}^{n-r} C(k, i_l) \cdot \alpha(k) \\ &= C(l, i_l) \cdot \alpha(l) \\ &= 1 \cdot x(i_l). \end{aligned}$$

Aus unserer vorbereitenden Bemerkung erhalten wir

$$x = y.$$

Der Vektor  $y$  liegt offensichtlich im Zeilenraum von  $C$ , also gilt  $x \in Z(C)$ .

Wir wissen also jetzt, dass die lineare Hülle der Zeilenvektoren von  $C$  genau  $N(B)$  ist. Jetzt zeigen wir noch, dass die Zeilen von  $C$  linear unabhängig sind. Sei  $\alpha =$

$(\alpha(1), \dots, \alpha(n-r))$  so, dass  $C^T \cdot \alpha = 0$ . Sei  $l \in \{1, 2, \dots, n-r\}$ . Dann gilt

$$\begin{aligned} 0 &= (C^T \cdot \alpha)[i_l] \\ &= \sum_{k=1}^{n-r} C(k, i_l) \cdot \alpha(k) \\ &= C(l, i_l) \cdot \alpha(l) \\ &= 1 \cdot \alpha(l). \end{aligned}$$

Daher gilt  $\alpha(l) = 0$ . ■

Wir haben also folgenden Satz gezeigt:

**SATZ 4.38.** *Sei  $B$  eine  $m \times n$ -Matrix in Zeilenstaffelnormalform, und sei  $r$  die Anzahl der Zeilen von  $B$ , die nicht 0 sind. Dann hat  $N(B)$  eine Basis, die genau  $n-r$  Vektoren enthält.*

Wir fassen den konstruktiven Teil des Beweises des Satzes 4.37 nocheinmal zusammen.

**ALGORITHMUS 4.39** (Nullraum einer Matrix in Zeilenstaffelnormalform).

Eingabe: Eine  $m \times n$ -Matrix  $B$  in Zeilenstaffelnormalform.

Ausgabe: Eine Matrix  $C$ , deren Zeilen eine Basis des Nullraumes von  $B$  sind.

```

1   $r \leftarrow$  Anzahl der Zeilen  $\neq 0$  von  $B$ 
2  for  $s = 1$  to  $r$ 
3      do  $J[s] \leftarrow \min\{k \in \mathbb{N} \mid B[s, k] \neq 0\}$ 
4   $C \leftarrow$  die  $(n-r) \times n$ -Matrix mit allen Einträgen 0
5   $freieVariablen \leftarrow$  aufsteigend geordnete Liste der Elemente von  $\{1, \dots, n\} \setminus \{J[s] \mid s \in \{1, \dots, r\}\}$ 
6  for  $k = 1$  to  $n-r$ 
7      do  $i \leftarrow freieVariablen[k]$ 
8          (* die  $i$ -te Variable wird frei gewählt *)
9           $C[k, i] \leftarrow 1$ 
10     for  $s = 1$  to  $r$ 
11         do  $C[k, J[s]] \leftarrow -B[s, i]$ 

```

Als Beispiel berechnen wir den Nullraum von zwei Matrizen in Zeilenstaffelnormalform.

**AUFGABE 4.40.** `In[68] := (* 1. Beispiel *)`

`In[69] := << RowRed9.m`

`In[70] := B = RowReduce[A6];`

`Out[70] = MatrixForm[B]`

$$\text{In}[71] := \begin{pmatrix} 1 & 2 & 0 & -17 & 0 & -22 \\ 0 & 0 & 1 & -5 & 0 & -5 \\ 0 & 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

`Out[71]= CC = NullSpaceViaREF2[B];`

`MatrixForm [CC]`

$$\text{In}[72] := \begin{pmatrix} -2 & 1 & 0 & 0 & 0 & 0 \\ 17 & 0 & 5 & 1 & 0 & 0 \\ 22 & 0 & 5 & 0 & -2 & 1 \end{pmatrix}$$

`In[73] :=`

**(\* 2. Beispiel \*)**

`In[74] := B = RowReduce [A5];`

`Out[74]= MatrixForm [B]`

$$\text{In}[75] := \begin{pmatrix} 1 & 2 & 0 & 0 & 0 & -\frac{32}{67} & 0 \\ 0 & 0 & 1 & 0 & 0 & -\frac{15}{67} & 0 \\ 0 & 0 & 0 & 0 & 1 & \frac{76}{67} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

`In[76] := CC = NullSpaceViaREF2 [B];`

`Out[76]= MatrixForm [CC]`

$$\text{In}[77] := \begin{pmatrix} -2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ \frac{32}{67} & 0 & \frac{15}{67} & 0 & -\frac{76}{67} & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

#### ÜBUNGSAUFGABEN 4.41.

- (1) Bestimmen Sie eine Basis für den Unterraum  $U$  des  $\mathbb{R}^4$ , der durch

$$U = \{(x_1, x_2, x_3, x_4) \in \mathbb{R}^4 \mid \begin{pmatrix} 1 & 0 & -2 & 3 \\ 2 & 1 & 0 & 4 \end{pmatrix} \cdot (x_1, x_2, x_3, x_4) = \begin{pmatrix} 0 \\ 0 \end{pmatrix}\}$$

gegeben ist.

Jede Matrix hat den gleichen Zeilenraum wie eine Matrix in Zeilenstaffelnormalform.

**SATZ 4.42.** Sei  $m \in \mathbb{N}$ , und sei  $A$  eine  $m \times (m + 1)$ -Matrix. Dann enthält der Nullraum von  $A$  einen von 0 verschiedenen Vektor.

### 7. Die Dimension eines Unterraumes

Wir werden jetzt sehen, dass alle Basen eines Unterraums von  $\mathbb{R}^n$  gleich viele Elemente haben.

**SATZ 4.43.** Seien  $k, n \in \mathbb{N}$ , sei  $m \in \mathbb{N}_0$ , sei  $B = (b_1, \dots, b_m)$  eine Basis des Unterraums  $T$  von  $\mathbb{R}^n$ , und sei  $C = (c_1, \dots, c_k)$  eine Folge von Vektoren in  $T$  mit  $k > m$ . Dann ist  $(c_1, \dots, c_k)$  linear abhängig.

*Beweisskizze.* Wenn  $m = 0$ , so gilt  $T = \{0\}$ . Dann ist jede Folge aus  $T$  mit zumindest einem Vektor linear abhängig. Wir betrachten nun den Fall  $m > 0$ : wir zeigen, daß bereits  $C' := (c_1, \dots, c_{m+1})$  linear abhängig ist. (Daraus folgt sofort die lineare Abhängigkeit von  $C$ , denn wir können  $\lambda_{m+2} = \dots = \lambda_k = 0$  setzen.) Sei  $\bar{C}$  die  $n \times (m+1)$ -Matrix  $(c_1, \dots, c_{m+1})$ , das heißt, die Matrix, deren Spaltenvektoren genau die Vektoren  $c_1, \dots, c_{m+1}$  sind.

Zu zeigen ist, daß  $\bar{C} \cdot x = 0$  eine Lösung  $x \neq 0$  besitzt.

Wir finden eine  $m \times (m+1)$ -Matrix  $Y$  mit  $\bar{B} \cdot Y = \bar{C}$ . Es gibt nun einen Vektor  $x \neq 0$  mit  $Y \cdot x = 0$ , also  $\bar{C} \cdot x = \bar{B} \cdot Y \cdot x = \bar{B} \cdot 0 = 0$ . Somit sind die Spaltenvektoren von  $\bar{C}$  linear abhängig. ■

**KOROLLAR 4.44.** Sei  $n \in \mathbb{N}$ . Dann gilt: Jede Folge von mehr als  $n$  Vektoren im  $\mathbb{R}^n$  ist linear abhängig.

*Beweis.*  $\mathbb{R}^n$  hat die sogenannte *kanonische Basis*

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, e_2 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \dots, e_n = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}.$$

Aus Satz 4.43 folgt, dass eine Folge aus mehr als  $n$  Vektoren linear abhängig ist. ■

**SATZ 4.45.** Sei  $n \in \mathbb{N}$ , und sei  $T$  ein Unterraum des  $\mathbb{R}^n$ . Dann hat  $T$  eine Basis.

*Beweisskizze.* Wir beginnen mit  $t_1 \neq 0, t_1 \in T$ . Falls  $L(t_1) \neq T$  gilt, existiert  $t_2 \neq 0$ , sodaß  $(t_1, t_2)$  linear unabhängig ist. Solange  $L(t_1, \dots, t_k) \neq T$  ist, können wir wegen Satz 4.16 ein  $t_{k+1} \in T \setminus \{0\}$  finden, sodaß  $(t_1, \dots, t_{k+1})$  linear unabhängig ist. Da im  $\mathbb{R}^n$  eine Folge von  $n+1$  Vektoren immer linear abhängig ist, muss irgendwann  $L(t_1, \dots, t_m) = T$  eintreten. Dann ist  $(t_1, \dots, t_m)$  Basis von  $T$ . ■

**KOROLLAR 4.46.** Sei  $T$  ein Unterraum des  $\mathbb{R}^n$ . Dann gibt es ein  $m \in \mathbb{N}_0$  und linear unabhängige Vektoren  $t_1, \dots, t_m \in T$ , sodass  $L(t_1, \dots, t_m) = T$ .

Jeder Unterraum des  $\mathbb{R}^n$  ist also die lineare Hülle endlich vieler Vektoren.

**LEMMA 4.47.** Seien  $B$  und  $C$  Basen von  $T$  mit  $|B| = k$ . Dann gilt  $|C| \leq k$ .

Da wir diesem Lemma die Rollen von  $B$  und  $C$  aber auch vertauschen können, folgt:

**SATZ 4.48.** Sei  $n \in \mathbb{N}$ , und sei  $T$  ein Unterraum von  $\mathbb{R}^n$ . Dann haben alle Basen von  $T$  gleich viele Elemente.



Der Satz 4.48 ermöglicht folgende Definition:

**DEFINITION 4.49 (Dimension).** Sei  $T$  ein Unterraum des  $\mathbb{R}^n$ . Dann ist die *Dimension* von  $T$  die Anzahl der Elemente einer Basis von  $T$ . Wir kürzen die Dimension von  $T$  mit  $\dim(T)$  ab.

**SATZ 4.50.** Sei  $n \in \mathbb{N}$ , sei  $k \in \mathbb{N}_0$ , sei  $T$  ein Unterraum des  $\mathbb{R}^n$  mit Dimension  $k$ , und sei  $S$  ein Unterraum von  $\mathbb{R}^n$  mit  $S \subseteq T$  und  $\dim(S) = k$ . Dann gilt  $S = T$ .

*Beweis.* Sei  $(s_1, \dots, s_k)$  eine Basis von  $S$ . Falls  $L(s_1, \dots, s_k) = T$ , so gilt  $S = T$ . Wenn es ein  $t \in T \setminus L(s_1, \dots, s_k)$  gibt, so ist nach Satz 4.16 die Folge  $(s_1, \dots, s_k, t)$  linear unabhängig. Dann haben wir  $k + 1$  linear unabhängige Vektoren in einem Vektorraum mit einer  $k$ -elementigen Basis gefunden. Das widerspricht Satz 4.43. ■

**SATZ 4.51.** Seien  $k \in \mathbb{N}_0$ ,  $n \in \mathbb{N}$ , und sei  $M$  eine Teilmenge von  $\mathbb{R}^n$ . Sei

$$B = (b_1, b_2, \dots, b_k)$$

eine linear unabhängige Folge von Vektoren aus  $M$ . Wir nehmen an, dass  $B$  so ist, dass es kein  $m \in M$  gibt, sodass  $(b_1, b_2, \dots, b_k, m)$  ebenfalls linear unabhängig ist. (Wir fordern also, dass  $B$  eine maximale linear unabhängige Folge aus  $M$  ist.) Dann ist  $B$  eine Basis für  $L(M)$ .

*Beweis.* Zu zeigen ist, dass  $L(B) = L(M)$ .  $L(B) \subseteq L(M)$  gilt, da  $B \subseteq M$ . Wir zeigen nun  $L(M) \subseteq L(B)$ . Es genügt zu zeigen:  $M \subseteq L(B)$ . Sei dazu  $m \in M$ . Da  $(b_1, b_2, \dots, b_k, m)$  linear abhängig ist, gilt wegen Satz 4.16, dass  $m$  in der linearen Hülle von  $(b_1, b_2, \dots, b_k)$  liegt. ■

**KOROLLAR 4.52.** Seien  $k, n \in \mathbb{N}$ , und sei  $M = (m_1, m_2, \dots, m_k)$  eine Folge von Vektoren in  $\mathbb{R}^n$ . Dann gibt es  $r \in \{0, \dots, k\}$  und  $i_1, i_2, \dots, i_r \in \{1, \dots, k\}$ , sodass folgendes gilt:  $i_1 < i_2 < \dots < i_r$ , und  $(m_{i_1}, m_{i_2}, \dots, m_{i_r})$  ist eine Basis von  $L(M)$ .

**KOROLLAR 4.53.** Sei  $k \in \mathbb{N}_0$ ,  $n \in \mathbb{N}$ , und sei  $M = (m_1, m_2, \dots, m_k)$  eine Folge von Vektoren in  $\mathbb{R}^n$ . Dann gilt  $\dim(L(M)) \leq k$ .

## 8. Der Rang einer Matrix

**DEFINITION 4.54.** Sei  $A$  eine  $m \times n$ -Matrix. Der *Rang* von  $A$  ist die Dimension des Zeilenraums von  $A$ .

Man berechnet den Rang, indem man aus der Matrix  $A$  eine Matrix  $B$  in Zeilenstufenform erzeugt, die den gleichen Zeilenraum wie  $A$  hat. Die Zeilen von  $B$ , die nicht 0 sind, sind stets linear unabhängig. Sie bilden also eine Basis von  $Z(B) = Z(A)$ .

**ALGORITHMUS 4.55 (Rang einer Matrix).**

Eingabe: eine  $m \times n$ -Matrix  $A$ .

Ausgabe: der Rang von  $A$ .

- 1 Berechne mit Algorithmus 4.21 eine Matrix  $B$  in Zeilenstaffelform, sodass  $Z(B) = Z(A)$ .
- 2 **return** Anzahl der Zeilen von  $B$ , die nicht 0 sind.

SATZ 4.56. Seien  $m, n \in \mathbb{N}$ , sei  $A$  eine  $m \times n$ -Matrix, und sei  $k$  der Rang von  $A$ . Dann hat  $N(A)$  die Dimension  $n - k$ .

*Beweis.* Sei  $B$  eine Matrix in Zeilenstaffelnormalform, sodass  $Z(B) = Z(A)$ . Wegen Korollar 4.36 hat  $B \cdot x = 0$  die gleiche Lösungsmenge wie  $A \cdot x = 0$ . Sei  $r$  die Anzahl der Zeilen von  $B$ , die nicht 0 sind. Diese Zeilen sind nach Satz 4.24 linear unabhängig, und bilden somit eine Basis von  $Z(B)$ . Da alle Basen eines Unterraums gleich viele Vektoren enthalten, gilt  $r = k$ . Nach Satz 4.37 hat  $N(B)$  die Dimension  $n - k$ . Da  $N(B) = N(A)$ , hat auch  $N(A)$  die Dimension  $n - k$ . ■

### 9. Die Eindeutigkeit der Zeilenstaffelnormalform

Die Zeilenstaffelnormalform hat folgende wichtige Eigenschaft:

SATZ 4.57. Seien  $m, n \in \mathbb{N}$ , und seien  $B, C$  zwei  $m \times n$ -Matrizen in Zeilenstaffelnormalform. Wir nehmen an, dass  $Z(B) = Z(C)$ . Dann gilt  $B = C$ .

*Beweis.* Wir fixieren  $m, n \in \mathbb{N}$ . Wir zeigen, dass für alle  $r \in \mathbb{N}_0$  folgendes gilt:

Für alle  $a \in \mathbb{N}$  und für alle  $a \times n$ -Matrizen  $B, C$  in Zeilenstaffelnormalform mit  $\dim(Z(B)) = r$  und  $Z(B) = Z(C)$  gilt  $B = C$ .

Diese Aussage beweisen wir durch Induktion nach  $r$ . Für  $r = 0$  gilt  $Z(B) = Z(C) = \{\vec{0}\}$ , also  $B = C = 0$ .

Sei nun  $r \geq 1$ , sei  $a \in \mathbb{N}$ , und seien  $B, C$  zwei  $a \times n$ -Matrizen in Zeilenstaffelnormalform mit  $Z(B) = Z(C)$  und  $\dim(Z(B)) = r$ . Dann haben sowohl  $B$  also auch  $C$  genau  $r$  Zeilen, die nicht 0 sind.

Für einen Unterraum  $U$  von  $\mathbb{R}^n$  und für  $l \in \{1, \dots, n-1\}$  definieren wir eine Teilmenge des  $\mathbb{R}^l$  durch

$$U^{(l)} := \{(u_1, \dots, u_l) \in \mathbb{R}^l \mid \text{es gibt } u_{l+1}, \dots, u_n \in \mathbb{R}, \text{ sodass } (u_1, \dots, u_n) \in U\}.$$

$U^{(n)}$  definieren wir durch  $U^{(n)} := U$ . Außerdem definieren wir für jede  $m \times n$ -Matrix  $A$  und für jedes  $l \in \{1, \dots, n\}$

$A_l :=$  die  $m \times l$ -Matrix, die aus den ersten  $l$  Spalten von  $A$  besteht.

Dann gilt:

$$\text{Für alle } l \in \{1, \dots, n\} : Z(B_l) = Z(B)^{(l)}.$$

Seien  $j_1, \dots, j_r$  wie in der Definition der Zeilenstaffelnormalform. Dann gilt  $\dim(Z(B)^{(j_r)}) = r$ , da die ersten  $r$  Zeilen von  $B_{j_r}$  eine Basis von  $Z(B)^{(j_r)}$  sind. Ebenso gilt  $\dim(Z(B)^{(j_{r-1})}) =$

$r - 1$ , da die ersten  $r - 1$  Zeilen von  $B_{j_r-1}$  eine Basis von  $Z(B)^{(j_r-1)}$  sind. Daher gilt:  $j_r$  ist jenes  $l \in \{1, 2, \dots, n\}$ , sodass  $\dim(Z(B)^{(l)}) = r$  und  $\dim(Z(B)^{(l-1)}) = r - 1$ .

Die Matrix  $C$  hat ebenfalls genau  $r$  Zeilen, die nicht 0 sind. Seien  $j'_1, \dots, j'_r$  wie in der Definition der Zeilenstaffelnormform. Wie oben gilt, dass  $j'_r$  jenes  $l' \in \{1, 2, \dots, n\}$  ist, sodass  $\dim(Z(C)^{(l')}) = r$  und  $\dim(Z(C)^{(l'-1)}) = r - 1$ . Da  $Z(B) = Z(C)$ , gilt also  $j_r = j'_r$ .

Die ersten  $r - 1$  Zeilen der Matrix  $B$  sind in Zeilenstaffelnormform. Sie bilden eine Basis des Raums

$$U = \{(v_1, \dots, v_n) \in Z(B) \mid v_{i_r} = 0\}.$$

Ebenso sind die ersten  $r - 1$  Zeilen der Matrix  $C$  in Zeilenstaffelnormform. Sie sind eine Basis von

$$V = \{(v_1, \dots, v_n) \in Z(C) \mid v_{i_r} = 0\}.$$

Sei  $B'$  die Matrix, die aus den ersten  $r - 1$  Zeilen von  $B$  besteht, und sei  $C'$  die Matrix, die aus den ersten  $r - 1$  Zeilen von  $C$  besteht. Nach Voraussetzung gilt  $Z(B) = Z(C)$ . Daher gilt auch  $U = V$ . Das heißt aber, dass  $Z(B') = Z(C')$ . Nach Induktionsvoraussetzung gilt also  $B' = C'$ .

Es bleibt zu zeigen, dass  $B$  und  $C$  die gleiche  $r$ -te Zeile haben. Sei  $b$  die  $r$ -te Zeile von  $B$  und  $c$  die  $r$ -te Zeile von  $C$ . Der Eintrag an der  $j_r$ -ten Stelle von  $b - c$  ist  $1 - 1 = 0$ ; auch alle Einträge von  $b - c$  vor der  $j_r$ -ten Stelle sind gleich 0. Da  $b, c \in Z(B)$ , gilt  $b - c \in Z(B)$ . Seien  $b_1, \dots, b_r$  die ersten  $r$  Zeilen von  $B$ . Seien  $\lambda_1, \dots, \lambda_r$  so, dass  $\sum_{k=1}^r \lambda_k \cdot b_k = b - c$ . Wenn wir für  $i \in \{1, \dots, r\}$  den  $j_i$ -ten Eintrag betrachten, erhalten wir

$$\sum_{k=1}^r \lambda_k \cdot B(k, j_i) = 0.$$

Da  $B$  in Zeilenstaffelnormform ist, ist nur der  $i$ -te Summand dieser Summe ungleich 0. Wir erhalten also  $\lambda_i = 0$ . Folglich sind alle  $\lambda_i = 0$ , also  $b - c = 0$ . Also sind auch die  $r$ -te Zeile von  $B$  und  $C$  gleich. ■

Dieser Satz hat folgende Anwendung:

ALGORITHMUS 4.58 (Gleichheit von Unterräumen).

Eingabe:  $v_1, \dots, v_k \in \mathbb{R}^n$  und  $w_1, \dots, w_l \in \mathbb{R}^n$ .

Ausgabe: **true**, falls  $L(v_1, \dots, v_k) = L(w_1, \dots, w_l)$ , **false** sonst.

- 1  $m \leftarrow \max(k, l)$
- 2  $\tilde{V} \leftarrow$  die  $m \times n$ -Matrix, deren erste  $k$  Zeilen die Vektoren  $v_1, \dots, v_k$  sind, und deren restliche Zeilen 0 sind
- 3  $\tilde{W} \leftarrow$  die  $m \times n$ -Matrix, deren erste  $l$  Zeilen die Vektoren  $w_1, \dots, w_l$  sind, und deren restliche Zeilen 0 sind
- 4 Berechne eine Matrix  $\tilde{V}'$  in Zeilenstaffelnormform, sodass  $Z(\tilde{V}') = Z(\tilde{V})$
- 5 Berechne eine Matrix  $\tilde{W}'$  in Zeilenstaffelnormform, sodass  $Z(\tilde{W}') = Z(\tilde{W})$
- 6 **return true**, falls  $\tilde{V}' = \tilde{W}'$ , und **false** sonst.

### 10. Die Lösungsmenge inhomogener linearer Gleichungssysteme

DEFINITION 4.59. Sei  $A \in \mathbb{R}^{m \times n}$ , und sei  $b \in \mathbb{R}^m$ . Das Gleichungssystem  $A \cdot x = b$  heißt *homogen*, wenn  $b = 0$ , und *inhomogen*, wenn  $b \neq 0$ .

DEFINITION 4.60. Sei  $T$  ein Unterraum des  $\mathbb{R}^n$ ,  $x_0 \in \mathbb{R}^n$ . Dann ist die *lineare Mannigfaltigkeit*  $x_0 + T$  definiert durch:

$$x_0 + T := \{x_0 + t \mid t \in T\}.$$

Die lineare Mannigfaltigkeit  $x_0 + T$  ist also der um den Vektor  $x_0$  verschobene Unterraum  $T$ . Lösungsmengen linearer Gleichungssysteme sind stets leer oder lineare Mannigfaltigkeiten.

SATZ 4.61. Seien  $m, n \in \mathbb{N}$ , sei  $A$  eine  $m \times n$ -Matrix, und sei  $x_0$  eine Lösung des Systems  $A \cdot x = b$ . Sei  $L$  die Lösungsmenge von  $A \cdot x = b$  und  $N(A)$  der Nullraum von  $A$ . Dann gilt:  $L = x_0 + N(A)$ .

AUFGABE 4.62. Sei  $A = \begin{pmatrix} 3 & 1 & 2 & -5 \\ 0 & 1 & -3 & 8 \end{pmatrix}$  und  $b = \begin{pmatrix} 4 \\ 1 \end{pmatrix}$ . Berechne die Lösungsmenge von  $A \cdot x = b$ .

Wir lösen dieses Beispiel mit Mathematica. Mathematica bietet dazu die Funktionen `NullSpace` und `LinearSolve`.

```
In[78]:= A = {{3, 1, 2, -5}, {0, 1, -3, 8}};
```

```
In[79]:= b = {4, 1};
```

```
In[80]:= NullSpace[A]
```

```
Out[80]= {{13, -24, 0, 3}, {-5, 9, 3, 0}}
```

```
In[81]:= LinearSolve[A, b]
```

```
Out[81]= {1, 1, 0, 0}
```

Die Lösungsmenge ist damit gegeben durch

$$L = \{(1, 1, 0, 0) + s \cdot (13, -24, 0, 3) + t \cdot (-5, 9, 3, 0) \mid s, t \in \mathbb{R}\}.$$

Wir überlegen uns jetzt noch, wie wir algorithmisch bestimmen können, ob ein lineares Gleichungssystem eine Lösung hat. Sei dazu  $A \cdot x = b$  ein lineares Gleichungssystem. Wir bilden die erweiterte Koeffizientenmatrix  $(A \ b)$ , also jene Matrix, die wir erhalten, wenn wir  $A$  um eine Spalte vergrößern und in diese Spalte  $b$  schreiben.

SATZ 4.63. Seien  $A \cdot x = b$  und  $C \cdot x = d$  zwei lineare Gleichungssysteme, und sei  $E = (A \ b)$  und  $F = (C \ d)$ . Wenn  $E$  und  $F$  den gleichen Zeilenraum haben, dann haben die beiden Gleichungssysteme die gleiche Lösungsmenge.

SATZ 4.64. Sei  $A$  eine  $m \times n$ -Matrix, sei  $b \in \mathbb{R}^m$ , sei  $E$  die Matrix  $(A \ b)$ , und sei  $L := \{x \in \mathbb{R}^n \mid A \cdot x = b\}$ . Dann gilt

$$L = \left\{ \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{R}^n \mid \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \\ -1 \end{pmatrix} \in N(E) \right\}.$$

SATZ 4.65. Seien  $m, n \in \mathbb{N}$ , sei  $A \in \mathbb{R}^{m \times n}$ ,  $b \in \mathbb{R}^m$ , und sei  $E := (A \ b)$ . Sei  $F$  eine Matrix in Zeilenstaffelform mit  $Z(F) = Z(E)$ , und seien  $j_1 < \dots < j_r$  wie in Definition 3.1. Wenn  $j_r = n + 1$ , dann hat das System  $A \cdot x = b$  keine Lösung.

*Beweis.* Wenn  $j_r = n + 1$ , dann gilt für alle Elemente  $x \in N(F)$ , dass  $x_{n+1} = 0$  ist. Nach Satz 4.64 hat  $A \cdot x = b$  also keine Lösung. ■

Wir bestimmen jetzt alle Lösungen von  $A \cdot x = b$  folgendermaßen:

ALGORITHMUS 4.66 (Lineare Gleichungssysteme).

Eingabe: Eine  $m \times n$ -Matrix  $A$ , und  $b \in \mathbb{R}^m$ .

Ausgabe: "keine Lösung", falls es kein  $x \in \mathbb{R}^n$  mit  $A \cdot x = b$  gibt. Sonst geben wir einen Vektor  $x_0 \in \mathbb{R}^n$  und eine  $t \times n$ -Matrix  $D$  aus, sodass die Lösungsmenge von  $A \cdot x = b$  gleich  $x_0 + Z(D)$  ist.

```

1  B ← die erweiterte Matrix (A b)
2  C ← die m × (n + 1)-Matrix in Zeilenstaffelnormalform mit Z(C) = Z(B)
3  r ← Anzahl der Zeilen ≠ 0 von B.
4  for s = 1 to r
5      do J[s] ← min{k ∈ ℕ | C[s, k] ≠ 0}
6  if J[r] = n + 1
7      then resultat ← "keine Lösung"
8  else D ← die (n - r) × n-Matrix mit allen Einträgen 0
9      x_0 ← der Nullvektor im ℝ^n
10     I ← aufsteigend geordnete Liste der Elemente von {1, ..., n} \ {J[s] | s ∈
    {1, ..., r}}
11     for k = 1 to n - r
12         do i ← I[k]
13             (* die i-te Variable wird frei gewählt *)
14             D[k, i] ← 1
15             for s = 1 to r
16                 do D[k, J[s]] ← -C[s, i]
17     for s = 1 to r
18         do x_0[J[s]] ← C[s, n + 1]
19     resultat ← (x_0, C)
20 return resultat

```

Wir berechnen jetzt die Lösung von zwei linearen Gleichungssystemen mit Mathematica, indem wir die Zeilenstaffelnormalform von  $(A \ b)$  ausrechnen.

AUFGABE 4.67. *In[82]* := << RowRed9.m

*In[83]* := **MatrixForm** [A1]

$$\text{Out}[83]= \begin{pmatrix} 1 & -5 & 8 & 2 & -2 \\ 1 & -4 & 6 & -2 & 0 \\ -1 & 0 & 2 & 2 & 0 \\ 5 & -8 & 6 & 0 & -5 \end{pmatrix}$$

*In[84]* := **MatrixForm**[b1]

$$\text{Out}[84]= \begin{pmatrix} -9 \\ -4 \\ 0 \\ -18 \end{pmatrix}$$

*In[85]* :=

**LinSolveViaREF** [A1, b1]

$$\begin{pmatrix} 1 & -5 & 8 & 2 & -2 & -9 \\ 1 & -4 & 6 & -2 & 0 & -4 \\ -1 & 0 & 2 & 2 & 0 & 0 \\ 5 & -8 & 6 & 0 & -5 & -18 \end{pmatrix}$$

$$\begin{pmatrix} 1 & -5 & 8 & 2 & -2 & -9 \\ 0 & 1 & -2 & -4 & 2 & 5 \\ 0 & -5 & 10 & 4 & -2 & -9 \\ 0 & 17 & -34 & -10 & 5 & 27 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & -2 & -18 & 8 & 16 \\ 0 & 1 & -2 & -4 & 2 & 5 \\ 0 & 0 & 0 & -16 & 8 & 16 \\ 0 & 0 & 0 & 58 & -29 & -58 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & -2 & -18 & 8 & 16 \\ 0 & 1 & -2 & -4 & 2 & 5 \\ 0 & 0 & 0 & 1 & -\frac{1}{2} & -1 \\ 0 & 0 & 0 & 58 & -29 & -58 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & -2 & 0 & -1 & -2 \\ 0 & 1 & -2 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & -\frac{1}{2} & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

$$\text{Out}[85]= \left\{ \{-2, 1, 0, -1, 0\}, \{\{2, 2, 1, 0, 0\}, \{1, 0, 0, \frac{1}{2}, 1\}\} \right\}$$

Jetzt noch ein System, das keine Lösung hat.

AUFGABE 4.68. *In[86]* := << RowRed9.m

*In[87]* := **MatrixForm** [A2]

$$\text{Out}[87]= \begin{pmatrix} 1 & 5 & 7 & 9 \\ 2 & 10 & 14 & 18 \\ 3 & 2 & 1 & 0 \end{pmatrix}$$

In[88]:= **MatrixForm**[b2]

$$\text{Out}[88]= \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$$

In[89]:=

**LinSolveViaREF** [A2, b2]

$$\begin{pmatrix} 1 & 5 & 7 & 9 & 0 \\ 2 & 10 & 14 & 18 & 1 \\ 3 & 2 & 1 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 5 & 7 & 9 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & -13 & -20 & -27 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 5 & 7 & 9 & 0 \\ 0 & -13 & -20 & -27 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 5 & 7 & 9 & 0 \\ 0 & 1 & \frac{20}{13} & \frac{27}{13} & -\frac{1}{13} \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & -\frac{9}{13} & -\frac{18}{27} & \frac{5}{13} \\ 0 & 1 & \frac{20}{13} & \frac{27}{13} & -\frac{1}{13} \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & -\frac{9}{13} & -\frac{18}{27} & 0 \\ 0 & 1 & \frac{20}{13} & \frac{27}{13} & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Out[89]= NOSOLUTION

## ÜBUNGSAUFGABEN 4.69.

- (1) Widerlegen Sie durch Angabe eines Gegenbeispiels:

Wenn das Gleichungssystem  $A \cdot x = 0$  eine Lösung hat, so besitzt für jede rechte Seite  $b$  das Gleichungssystem  $A \cdot x = b$  zumindest eine Lösung.

## 11. Koordinaten

**SATZ 4.70.** Seien  $n \in \mathbb{N}$ ,  $m \in \mathbb{N}_0$ , und sei  $B = (b_1, \dots, b_m)$  eine Basis von  $T \subseteq \mathbb{R}^n$  und  $t \in T$ . Dann gibt es genau ein  $m$ -Tupel  $(\lambda_1, \dots, \lambda_m) \in \mathbb{R}^m$  mit

$$t = \sum_{i=1}^m \lambda_i \cdot b_i.$$

*Beweis.* Ein solches  $m$ -Tupel existiert, da  $t \in L(b_1, \dots, b_m)$ . Sei nun  $\bar{B}$  die  $n \times m$ -Matrix, in deren Spalten die Vektoren  $(b_1, \dots, b_m)$  stehen. Angenommen,  $\alpha = (\lambda_1, \dots, \lambda_m)$  und  $\beta = (\mu_1, \dots, \mu_m)$  seien zwei verschiedene Tupel mit  $\bar{B} \cdot \alpha = \bar{B} \cdot \beta = t$ . Dann gilt  $\bar{B} \cdot (\alpha - \beta) = 0$  und  $\alpha - \beta \neq 0$ . Das ist ein Widerspruch zur linearen Unabhängigkeit von der Spalten von  $\bar{B}$ . ■

Dieses  $m$ -Tupel gibt also an, wie wir den Vektor  $t$  aus den Basisvektoren zusammenbauen können. Wir nennen dieses Tupel die *Koordinaten* des Vektors  $t$  bezüglich der Basis  $B$ .

DEFINITION 4.71. Sei  $B = (b_1, \dots, b_m)$  Basis von  $T \subseteq \mathbb{R}^n$ , sei  $t \in T$ , und sei  $\bar{B}$  die  $n \times m$ -Matrix, in deren Spalten die Vektoren  $(b_1, \dots, b_m)$  stehen. Dann heißt das  $\alpha = (\lambda_1, \dots, \lambda_m) \in \mathbb{R}^m$  mit

$$\bar{B} \cdot \alpha = t$$

das *Koordinatentupel* von  $t$  bezüglich der Basis  $B$ . Wir schreiben auch  $(t)_B = \alpha$ .

Das Koordinatentupel  $(t)_B$  erfüllt also die Gleichung

$$\bar{B} \cdot (t)_B = t.$$

AUFGABEN 4.72. (1) Sei  $B = ((1, 0, 3), (2, 1, 6))$ ,  $T = L(B)$ , und  $v = (3, 1, 9)$ . Offenbar gilt

$$\begin{pmatrix} 3 \\ 1 \\ 9 \end{pmatrix} = 1 \cdot \begin{pmatrix} 1 \\ 0 \\ 3 \end{pmatrix} + 1 \cdot \begin{pmatrix} 2 \\ 1 \\ 6 \end{pmatrix},$$

woraus  $(v)_B = (1, 1)$  folgt.

(2) Sei  $T = L((3, 2, 1), (0, 1, 2))$ . Für das erste Basiselement gilt offensichtlich

$$\left( \begin{pmatrix} 3 \\ 1 \\ 2 \end{pmatrix} \right)_B = \begin{pmatrix} 1 \\ 0 \end{pmatrix},$$

weilers ist zum Beispiel

$$\left( 3 \cdot \begin{pmatrix} 3 \\ 1 \\ 2 \end{pmatrix} - 2 \cdot \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix} \right)_B = \begin{pmatrix} 3 \\ -2 \end{pmatrix}.$$

ÜBUNGSAUFGABEN 4.73.

(1) Der Vektor  $v$  hat bezüglich der Basis  $A = \left( \begin{pmatrix} 1 \\ 0 \\ -3 \end{pmatrix}, \begin{pmatrix} 2 \\ 8 \\ -4 \end{pmatrix} \right)$  der Ebene  $\varepsilon$  die Koordinaten  $(v)_A = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ . Berechnen Sie seine Koordinaten bezüglich der Basis  $B = \left( \begin{pmatrix} 5 \\ 16 \\ -11 \end{pmatrix}, \begin{pmatrix} 12 \\ 40 \\ -26 \end{pmatrix} \right)$ .

(2) Die Ebene  $\varepsilon$  hat die Basen

$$A = \left( \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ 0 \end{pmatrix} \right)$$

und

$$B = \left( \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix} \right).$$

Der Vektor  $v$  hat bezüglich  $B$  die Koordinaten  $(v)_B = \begin{pmatrix} 7 \\ 3 \end{pmatrix}$ . Berechnen Sie seine Koordinaten bezüglich  $A$ !



- (3) Die Ebene  $e$  ist durch  $e = L\left(\begin{pmatrix} 3 \\ 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ -1 \\ 5 \end{pmatrix}\right)$  gegeben. Sie hat die Basen

$$B = \left(\begin{pmatrix} 3 \\ 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ -1 \\ 5 \end{pmatrix}\right)$$

und

$$C = \left(\begin{pmatrix} 24 \\ -2 \\ 31 \end{pmatrix}, \begin{pmatrix} 18 \\ -2 \\ 24 \end{pmatrix}\right).$$

Der Vektor  $v$  ist gegeben durch  $(v)_C = \begin{pmatrix} -1 \\ -2 \end{pmatrix}$ . Berechnen Sie  $(v)_B$ .

- (4) Sei  $a = \begin{pmatrix} 3 \\ 0 \\ 4 \end{pmatrix}$  und  $b = \begin{pmatrix} 2 \\ 1 \\ 4 \end{pmatrix}$ , und sei  $B = (a, b)$ . Zeigen Sie, dass ein Vektor  $\begin{pmatrix} x \\ y \end{pmatrix}$  bezüglich der Basis  $B$  die Koordinaten  $\begin{pmatrix} \langle \begin{pmatrix} x \\ y \end{pmatrix}, a \rangle \\ \langle \begin{pmatrix} x \\ y \end{pmatrix}, b \rangle \end{pmatrix}$  hat; das heißt, zeigen Sie

$$\begin{pmatrix} x \\ y \end{pmatrix}_B = \begin{pmatrix} \langle \begin{pmatrix} x \\ y \end{pmatrix}, a \rangle \\ \langle \begin{pmatrix} x \\ y \end{pmatrix}, b \rangle \end{pmatrix}.$$

Stimmt diese Formel für jede Basis  $(a, b)$  des  $\mathbb{R}^2$ ?

- (5) Sei  $B = \left(\begin{pmatrix} 3 \\ 0 \\ -1 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ 4 \end{pmatrix}\right)$ , und sei  $E$  die lineare Hülle von  $B$ .  $B$  ist dann eine Basis von  $E$ .

- Welcher Vektor  $w$  hat bezüglich  $B$  die Koordinaten  $(w)_B = \begin{pmatrix} 3 \\ -2 \end{pmatrix}$ ?
- Wie lauten die Koordinaten von  $\begin{pmatrix} -1 \\ 1 \\ 5 \end{pmatrix}$  bezüglich  $B$ ?
- Geben Sie eine Basis  $C$  von  $E$  an, bezüglich der der Punkt  $\begin{pmatrix} -1 \\ 1 \\ 5 \end{pmatrix}$  die Koordinaten  $\begin{pmatrix} 0 \\ 2 \end{pmatrix}$  hat.

## 12. Summen und Durchschnitte von Unterräumen

**SATZ 4.74.** Seien  $U, V$  Unterräume des  $\mathbb{R}^n$ . Dann ist  $U \cap V$  auch ein Unterraum des  $\mathbb{R}^n$ .

**DEFINITION 4.75.** Seien  $U, V$  Unterräume des  $\mathbb{R}^n$ . Wir definieren

$$U + V := \{u + v \mid u \in U, v \in V\}.$$

**SATZ 4.76.** Seien  $U, V$  Unterräume des  $\mathbb{R}^n$ . Dann ist  $U + V$  auch ein Unterraum des  $\mathbb{R}^n$ .

Wir überlegen uns nun, wie wir Basen von  $U \cap V$  und  $U + V$  berechnen können.

**ALGORITHMUS 4.77** (Summe explizit gegebener Unterräume).

Eingabe:  $u_1, \dots, u_l \in \mathbb{R}^n$  und  $v_1, \dots, v_m \in \mathbb{R}^n$  so, dass  $L(u_1, \dots, u_l) = U$  und  $L(v_1, \dots, v_l) = V$ .

Ausgabe: Eine Basis von  $U + V$ .

- Bilde eine  $(l + m) \times n$ -Matrix  $W$ , deren erste  $l$  Zeilen die Vektoren  $u_1, \dots, u_l$  sind, und deren  $(l + 1)$ -te bis  $(l + m)$ -te Zeile die Vektoren  $v_1, \dots, v_l$  sind
- Bestimme eine Matrix  $W'$  in Zeilenstaffelform, sodass  $Z(W') = Z(W)$
- return** die Zeilen von  $W'$ , die nicht 0 sind

**ALGORITHMUS 4.78** (Durchschnitt implizit gegebener Unterräume).

Eingabe: Eine  $r \times n$ -Matrix  $A$  und eine  $s \times n$ -Matrix  $B$ , sodass  $N(A) = U$  und  $N(B) = V$ .

Ausgabe: Eine Basis von  $U \cap V$ .

- Bilde die  $(r + s) \times n$ -Matrix  $C$ , deren erste  $r$  Zeilen die Matrix  $A$  und deren letzte  $s$  Zeilen die Matrix  $B$  sind
- Bestimme eine Basis  $X$  für  $N(C)$

3 **return X**

Um die Summe zweier implizit gegebener Unterräume zu berechnen, können wir uns zuerst von beiden Unterräumen mit den Algorithmen 4.27 und 4.39 eine Basis ausrechnen, und dann Algorithmus 4.77 verwenden.

AUFGABE 4.79. Bestimmen Sie eine Basis des Raums  $U + V$ , wobei

$$U = \{x \in \mathbb{R}^4 \mid \begin{pmatrix} 4 & -3 & 0 & 1 \\ 2 & -2 & 1 & 0 \end{pmatrix} \cdot x = \begin{pmatrix} 0 \\ 0 \end{pmatrix}\},$$

und

$$V = \{x \in \mathbb{R}^4 \mid \begin{pmatrix} 2 & -3 & 0 & 1 \\ -3 & -2 & 1 & 0 \end{pmatrix} \cdot x = \begin{pmatrix} 0 \\ 0 \end{pmatrix}\}.$$

*Lösung:* Wir berechnen Matrizen  $C, D$ , in deren Zeilen Basen von  $U$  bzw.  $V$  stehen.

*In[90]:= A = {{4, -3, 0, 1}, {2, -2, 1, 0}}*

*Out[90]= {{4, -3, 0, 1}, {2, -2, 1, 0}}*

*In[91]:= B = {{2, -3, 0, 1}, {-3, -2, 1, 0}}*

*Out[91]= {{2, -3, 0, 1}, {-3, -2, 1, 0}}*

*In[92]:= CC = NullSpace [A]*

*Out[92]= {{-1, -1, 0, 1}, {3, 4, 2, 0}}*

*In[93]:= DD = NullSpace [B]*

*Out[93]= {{-2, 3, 0, 13}, {3, 2, 13, 0}}*

Jetzt bestimmen wir eine Matrix  $E$ , deren Zeilenraum der Raum  $U + V$  ist.

*In[94]:= EE = Join [CC, DD];*

*In[95]:= MatrixForm [EE]*

*Out[95]=* 
$$\begin{pmatrix} -1 & -1 & 0 & 1 \\ 3 & 4 & 2 & 0 \\ -2 & 3 & 0 & 13 \\ 3 & 2 & 13 & 0 \end{pmatrix}$$

*In[96]:= FF = RowReduce [EE];*

*In[97]:= MatrixForm [FF]*

*Out[97]=* 
$$\begin{pmatrix} 1 & 0 & 0 & -\frac{16}{5} \\ 0 & 1 & 0 & \frac{11}{5} \\ 0 & 0 & 1 & \frac{2}{5} \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Also ist

$$((1, 0, 0, -16/5), (0, 1, 0, 11/5), (0, 0, 1, 2/5))$$

eine Basis von  $U + V$ .

Nun wollen wir den Durchschnitt zweier parametrisiert gegebener Unterräume berechnen.

**SATZ 4.80.** *Sei  $U$  ein Unterraum des  $\mathbb{R}^n$ . Dann gilt  $\dim(U^\perp) = n - \dim(U)$ .*

*Beweis.* Sei  $(u_1, \dots, u_l)$  eine Basis von  $U$ .  $U^\perp$  ist die Lösungsmenge des Gleichungssystems  $\tilde{U} \cdot x = 0$ , wobei  $\tilde{U}$  die  $l \times n$ -Matrix ist, deren Zeilenvektoren  $u_1, \dots, u_l$  sind. Der Rang von  $U$  ist  $l$ , daher ist die Dimension von  $U^\perp$  nach Satz 4.56 gleich  $n - l$ . ■

**SATZ 4.81.** *Sei  $U$  ein Unterraum des  $\mathbb{R}^n$ . Dann gilt  $(U^\perp)^\perp = U$ .*

*Beweis.* Wir zeigen zunächst  $\supseteq$ . Sei  $u \in U$ . Um zu zeigen, dass  $u \in (U^\perp)^\perp$  liegt, ist zu zeigen, dass  $\langle v, u \rangle = 0$  für alle  $v \in U^\perp$ . Sei  $v \in U^\perp$ . Da  $v \in U^\perp$ , gilt  $\langle u, v \rangle = 0$ . Also gilt  $U \subseteq (U^\perp)^\perp$ . Sei  $l$  die Dimension von  $U$ . Es gilt  $\dim((U^\perp)^\perp) = n - \dim(U^\perp) = n - (n - l) = l$ . Wegen Satz 4.50 gilt also  $U = (U^\perp)^\perp$ . ■

**SATZ 4.82.** *Sei  $A$  eine  $m \times n$ -Matrix, und sei  $B$  eine  $n \times l$ -Matrix, in deren Spalten eine Basis für den Nullraum von  $A$  steht. Dann gilt*

$$N(B^T) = Z(A).$$

*Der Nullraum von  $B^T$  ist also der Zeilenraum von  $A$ .*

*Beweis.* In den Spalten von  $B$  steht eine Basis für den Nullraum  $N(A)$  von  $A$ . Der Nullraum  $N(A)$  ist gleichzeitig der Raum  $(Z(A))^\perp$ . In den Spalten von  $B$  steht also eine Basis für  $(Z(A))^\perp$ . Nach Satz 4.35 gilt  $N(B^T) = (Z(B^T))^\perp$ . Da in den Spalten von  $B$  eine Basis von  $(Z(A))^\perp$  steht, sind auch die Zeilen von  $B^T$  eine Basis von  $(Z(A))^\perp$ . Es gilt also  $Z(B^T) = (Z(A))^\perp$ . Somit gilt insgesamt  $N(B^T) = (Z(B^T))^\perp = ((Z(A))^\perp)^\perp$ . Wegen Satz 4.81 gilt also  $N(B^T) = Z(A)$ . ■

Dieser Satz lässt sich noch umformulieren:

**KOROLLAR 4.83.** *Sei  $A$  eine  $m \times n$ -Matrix, und sei  $C$  eine  $l \times n$ -Matrix, in deren Zeilen eine Basis für den Nullraum von  $A$  steht. Dann gilt*

$$N(C) = Z(A).$$

*Der Nullraum von  $C$  ist also der Zeilenraum von  $A$ .*

Das führt zu folgendem Algorithmus:

**ALGORITHMUS 4.84** (Implizitisieren eines Unterraums).

Eingabe: Eine  $m \times n$ -Matrix  $A$ .

Ausgabe: Eine  $l \times n$ -Matrix  $C$ , sodass  $N(C) = Z(A)$ .

- 1  $C \leftarrow$  eine Matrix, in deren Zeilen eine Basis von  $N(A)$  steht
- 2 **return**  $C$

ALGORITHMUS 4.85 (Durchschnitt von explizit gegebenen Unterräumen).

Eingabe:  $u_1, \dots, u_l \in \mathbb{R}^n$  und  $v_1, \dots, v_m \in \mathbb{R}^n$  so, dass  $L(u_1, \dots, u_l) = U$  und  $L(v_1, \dots, v_m) = V$ .

Ausgabe: Eine Basis von  $U \cap V$ .

- 1 Bestimme mit Algorithmus 4.84 eine Matrix  $C_1$ , sodass  $N(C_1) = U$
- 2 Bestimme mit Algorithmus 4.84 eine Matrix  $C_2$ , sodass  $N(C_2) = V$
- 3 Verwende Algorithmus 4.78, um eine Basis von  $N(C_1) \cap N(C_2)$  auszurechnen

Wir verwenden diesen Algorithmus, um folgendes Beispiel zu lösen.

AUFGABE 4.86. Sei  $U = L((-1, -2, -2, -2), (1, 4, 6, 8))$ , und  $V = L((1, 0, 3, -2), (-1, 2, 1, 8))$ . Berechnen Sie eine Basis von  $U \cap V$ .

*Lösung:*

```
In[98]:= CfuerU1 = NullSpace [{{-1, -2, -2, -2}, {1, 4, 6, 8}}]
```

```
Out[98]= {{4, -3, 0, 1}, {2, -2, 1, 0}}
```

```
In[99]:= CfuerU2 = NullSpace [{{1, 0, 3, -2}, {-1, 2, 1, 8}}]
```

```
Out[99]= {{2, -3, 0, 1}, {-3, -2, 1, 0}}
```

```
In[100]:= CfuerU1geschnittenU2 = Join [CfuerU1, CfuerU2]
```

```
Out[100]= {{4, -3, 0, 1}, {2, -2, 1, 0}, {2, -3, 0, 1}, {-3, -2, 1, 0}}
```

```
In[101]:= BasisFuerU1geschnittenU2 = NullSpace [CfuerU1geschnittenU2]
```

```
Out[101]= {{0, 1, 2, 3}}
```

Somit ist  $((0, 1, 2, 3))$  eine Basis von  $U \cap V$ .

Zum Schneiden parametrisiert gegebener linearer Mannigfaltigkeiten hilft folgender Algorithmus.

ALGORITHMUS 4.87 (Implizitisieren einer linearen Mannigfaltigkeit).

Eingabe: Eine  $m \times n$ -Matrix  $A$ , und  $b \in \mathbb{R}^m$ .

Ausgabe: Eine  $l \times n$ -Matrix  $C$  und  $d \in \mathbb{R}^l$ , sodass  $b + Z(A) = \{x \in \mathbb{R}^n \mid C \cdot x = d\}$ .

- 1  $C \leftarrow$  eine Matrix, in deren Zeilen eine Basis von  $N(A)$  steht
- 2  $d \leftarrow C \cdot b$
- 3 **return**  $(C, d)$

## KAPITEL 5

# Orthogonalität

### 1. Der Winkel zwischen zwei Vektoren

DEFINITION 5.1. Für  $x = (x_1, \dots, x_n), y = (y_1, \dots, y_n) \in \mathbb{R}^n$  ist das *Skalarprodukt* von  $x$  und  $y$  definiert als

$$\langle x, y \rangle := x_1 y_1 + x_2 y_2 + \dots + x_n y_n = \sum_{i=1}^n x_i y_i.$$

Es gilt

$$\langle x, x \rangle = \sum_{i=1}^n x_i^2 = \|x\|^2.$$

LEMMA 5.2. Für  $x, y, z \in \mathbb{R}^n$  und  $\lambda \in \mathbb{R}$  gilt:

- (1)  $\langle x + y, z \rangle = \langle x, z \rangle + \langle y, z \rangle$ ,
- (2)  $\langle \lambda x, y \rangle = \lambda \langle x, y \rangle$ .

SATZ 5.3. Der Winkel  $\varphi$  zwischen  $x$  und  $y$  ist gegeben durch

$$\cos \varphi = \frac{\langle x, y \rangle}{\|x\| \cdot \|y\|}.$$

DEFINITION 5.4. Zwei Vektoren *stehen* genau dann *normal aufeinander*, wenn  $\langle x, y \rangle = 0$ . Wir schreiben dann  $x \perp y$ .

### ÜBUNGSAUFGABEN 5.5.

- (1) Bestimmen Sie einen Vektor, der auf  $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$  und  $\begin{pmatrix} -1 \\ 0 \end{pmatrix}$  normal steht.
- (2) Sei  $B = \left( \begin{pmatrix} 3 \\ 0 \\ -1 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ 4 \end{pmatrix} \right)$ , und sei  $E$  die lineare Hülle von  $B$ .  $B$  ist dann eine Basis von  $E$ . Außerdem bezeichnen wir mit  $\bar{B}$  die Matrix

$$\bar{B} := \begin{pmatrix} 3 & 2 \\ 0 & 1 \\ -1 & 4 \end{pmatrix}.$$

- (a) Welches Gleichungssystem muss ein Vektor  $\begin{pmatrix} x \\ y \\ z \end{pmatrix}$  erfüllen, der auf alle Vektoren in  $E$  normal steht? Was hat die Koeffizientenmatrix dieses Systems mit  $\bar{B}$  zu tun?
- (b) Mit welchem Gleichungssystem können Sie feststellen, ob ein Vektor  $v$  in  $E$  liegt? Was hat die Koeffizientenmatrix dieses Systems mit  $\bar{B}$  zu tun?
- (c) Sei  $w = \begin{pmatrix} 16 \\ 44 \\ -6 \end{pmatrix}$ . Finden Sie einen Vektor  $e$ , der in  $E$  liegt, sodass  $w - e$  normal auf alle Vektoren in  $E$  steht.

## 2. Der Normalraum auf eine Menge von Vektoren

Wenn  $U$  eine Teilmenge des  $\mathbb{R}^n$  ist, dann bezeichnen wir den Raum  $U^\perp$  auch als “ $U$  orthogonal” und verwenden anstelle von  $U^\perp$  die Bezeichnung  $U^\perp$ . Für eine Teilmenge  $A$  des  $\mathbb{R}^n$  ist  $A^\perp$  also definiert durch

$$A^\perp := \{x \in \mathbb{R}^n \mid x \perp a \text{ für alle } a \in A\}.$$

Für jede Teilmenge  $A$  von  $\mathbb{R}^n$  gilt  $A^\perp = L(A)^\perp$  und  $(A^\perp)^\perp = L(A)$ .

### ÜBUNGSAUFGABEN 5.6.

- (1) Gegeben seien die Vektoren

$$x = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad y = \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix}, \quad z = \begin{pmatrix} 6 \\ 4 \\ 2 \end{pmatrix}.$$

Berechnen Sie

- (a)  $\{x\}^\perp$ ,  
 (b)  $\{x, y\}^\perp$ ,  
 (c)  $\{x, y, z\}^\perp$ ,

und jeweils die Dimension davon.

- (2) Welche Vektoren des  $\mathbb{R}^4$  stehen auf alle drei Vektoren

$$(1, 2, 0, 0), (0, 1, 2, -1), (1, 0, 2, 0)$$

normal? (Zwei Vektoren im  $\mathbb{R}^4$  stehen aufeinander normal, wenn ihr Skalarprodukt gleich 0 ist.)

## 3. Orthonormalbasen

DEFINITION 5.7. Sei  $T$  ein Unterraum des  $\mathbb{R}^n$  und  $B = (b_1, \dots, b_k)$  eine Basis von  $T$ .  $B$  ist eine *Orthonormalbasis* (ONB), wenn

- (1)  $\langle b_i, b_j \rangle = 0$  für alle  $i, j \in \{1, 2, \dots, k\}$  mit  $i \neq j$ .  
 (2)  $\|b_i\| = \sqrt{\langle b_i, b_i \rangle} = 1$  für alle  $i \in \{1, 2, \dots, k\}$ .

### BEISPIELE 5.8.

- (1) Die kanonische Basis  $((1, 0, 0), (0, 1, 0), (0, 0, 1))$  ist ONB des  $\mathbb{R}^3$ .  
 (2)  $B = ((\frac{1}{2}, \frac{-\sqrt{3}}{2}, 0), (\frac{\sqrt{3}}{2}, \frac{1}{2}, 0), (0, 0, 1))$  ist ONB des  $\mathbb{R}^3$ .  
 (3)  $B = (\frac{1}{2}(1, -1, 1, -1), \frac{1}{2}(1, 1, 1, 1))$  ist ONB von  $L((1, -1, 1, -1), (1, 1, 1, 1))$ .  
 (4) Sei  $b_1 = (3, 4)$ ,  $b_2 = (-4, 3)$ . Dann ist  $(\frac{b_1}{5}, \frac{b_2}{5})$  ONB des  $\mathbb{R}^2$ .

### ÜBUNGSAUFGABEN 5.9.

- (1) (Orthonormalbasen) Welche der folgenden Basen sind ONB?

- (a)  $(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \frac{1}{\sqrt{13}}\begin{pmatrix} 0 \\ 3 \end{pmatrix}, \frac{-1}{\sqrt{13}}\begin{pmatrix} 0 \\ 3 \end{pmatrix})$ .  
 (b)  $(\frac{1}{\sqrt{3}}\begin{pmatrix} 1 \\ 1 \end{pmatrix})$ .  
 (c)  $(\begin{pmatrix} 0.6 \\ 0.8 \end{pmatrix}, \begin{pmatrix} -0.8 \\ 0.6 \end{pmatrix})$ .

SATZ 5.10. Sei  $B = (b_1, \dots, b_k)$  eine ONB und  $v \in L(B)$  mit den Koordinaten  $(v)_B = (\lambda_1, \dots, \lambda_k)$ . Dann gilt

$$\|v\|^2 = \lambda_1^2 + \dots + \lambda_k^2.$$

*Beweis.* Da  $B$  eine ONB ist, gilt

$$\begin{aligned}\|v\|^2 = \langle v, v \rangle &= \left\langle \sum_{i=1}^k \lambda_i b_i, \sum_{j=1}^k \lambda_j b_j \right\rangle = \sum_{i=1}^k \sum_{j=1}^k \lambda_i \lambda_j \langle b_i, b_j \rangle = \sum_{i=1}^k \lambda_i \lambda_i \langle b_i, b_i \rangle \\ &= \sum_{i=1}^k \lambda_i^2 \cdot 1.\end{aligned}$$

■

Wir wenden diesen Satz an:

Sei  $b_1 = (0.6, 0.8)$ ,  $b_2 = (-0.8, 0.6)$ . Berechnen Sie die Länge von  $v = 12 \cdot b_1 + 5 \cdot b_2$ !

Lösung: Da  $(b_1, b_2)$  eine ONB des  $\mathbb{R}^2$  ist, gilt

$$\|v\| = \sqrt{12^2 + 5^2} = 13.$$

Wir kontrollieren das Ergebnis, indem wir  $v$  berechnen. Da

$$v = 12 \cdot (0.6, 0.8) + 5 \cdot (-0.8, 0.6) = (3.2, 12.6),$$

gilt

$$\|v\| = \sqrt{(3.2)^2 + (12.6)^2} = 13.$$

**SATZ 5.11.** Sei  $T$  ein Unterraum des  $\mathbb{R}^n$  mit der ONB  $B = (b_1, \dots, b_k)$ . Sei  $v \in L(B)$  mit den Koordinaten  $(v)_B = (\lambda_1, \dots, \lambda_k)$ . Dann gilt

$$\lambda_i = \langle v, b_i \rangle \text{ für alle } i \in \{1, \dots, k\}.$$

*Beweis.* Sei  $i \in \{1, \dots, k\}$ . Wir wissen, dass

$$\sum_{j=1}^k \lambda_j b_j = v,$$

und somit

$$\left\langle \sum_{j=1}^k \lambda_j b_j, b_i \right\rangle = \langle v, b_i \rangle.$$

Daraus folgt, dass

$$\sum_{j=1}^k \lambda_j \langle b_j, b_i \rangle = \langle v, b_i \rangle$$

oder

$$\lambda_i \langle b_i, b_i \rangle = \langle v, b_i \rangle.$$

Somit gilt

$$\lambda_i = \langle v, b_i \rangle.$$

■

Bei Orthonormalbasen müssen wir also kein Gleichungssystem lösen, um die Koordinaten eines Vektors zu bestimmen. Dazu folgendes Beispiel: Gegeben sei die ONB  $B = ((0.6, 0.8), (-0.8, 0.6))$ . Gesucht sind die Koordinaten  $(\lambda_1, \lambda_2)$  von  $v = (2, 1)$  bzgl.  $B$ .

$$\lambda_1 = \langle v, b_1 \rangle = 2, \quad \lambda_2 = \langle v, b_2 \rangle = -1.$$

Also gilt:

$$(v)_B = \begin{pmatrix} 2 \\ -1 \end{pmatrix}.$$

Eine Orthonormalbasis besitzt also zwei wesentliche Vorteile gegenüber normalen Basen:

(1) Mit  $(v)_B = (\lambda_1, \dots, \lambda_k)$  kann die Länge des Vektors  $v$  als

$$\|v\| = \sqrt{\lambda_1^2 + \dots + \lambda_k^2}$$

berechnet werden.

(2) Die Koordinaten eines Vektors  $v$  erhält man als

$$(v)_B = \begin{pmatrix} \langle v, b_1 \rangle \\ \vdots \\ \langle v, b_k \rangle \end{pmatrix}.$$

#### 4. Das Gram-Schmidtsche Orthonormalisierungsverfahren

Gegeben ist ein Unterraum  $T$  mit der Basis  $B = (b_1, \dots, b_m)$ . Gesucht ist eine ONB  $(d_1, \dots, d_m)$  von  $T$ .

Wir konstruieren  $d_1, \dots, d_m$  mit folgenden Eigenschaften:

- (1)  $d_i \perp d_j$  für  $i \neq j$ ,
- (2)  $\|d_i\| = 1$  für alle  $i$ ,
- (3) für alle  $k \leq m$  gilt  $L(b_1, \dots, b_k) = L(d_1, \dots, d_k)$ .

(1) und (2) sollen garantieren, dass wir eine ONB erhalten. (3) fordert, dass die ersten  $k$  Vektoren der gesuchten ONB den gleichen Vektorraum aufspannen wie die ersten  $k$  Vektoren der Basis  $B$ .

ALGORITHMUS 5.12.

- (1) *Konstruktion von  $d_1$* : Wir setzen  $c_1 = b_1$  und  $d_1 = \frac{c_1}{\|c_1\|}$ .
- (2) *Konstruktion von  $d_2$* : Um (3) erfüllen zu können, machen wir den Ansatz

$$c_2 = b_2 + \alpha_1 \cdot d_1$$

mit  $\langle c_2, d_1 \rangle = 0$ . Aus

$$\langle b_2 + \alpha_1 \cdot d_1, d_1 \rangle = \langle b_2, d_1 \rangle + \alpha_1 \langle d_1, d_1 \rangle = \langle b_2, d_1 \rangle + \alpha_1 = 0$$



folgt

$$\alpha_1 = -\langle b_2, d_1 \rangle.$$

Also erhalten wir mittels

$$c_2 = b_2 - \langle b_2, d_1 \rangle \cdot d_1,$$

$$d_2 = \frac{c_2}{\|c_2\|}$$

den gewünschten Vektor  $d_2$ .

(3) *Konstruktion von  $d_3$* : Für  $c_3$  machen wir analog zu  $c_2$  den Ansatz

$$c_3 = b_3 + \alpha_1 \cdot d_1 + \alpha_2 \cdot d_2.$$

Fordern wir dann Normalität zu den ersten beiden Vektoren, so erhalten wir

$$\langle c_3, d_1 \rangle = \langle b_3, d_1 \rangle + \alpha_1 \underbrace{\langle d_1, d_1 \rangle}_{=1} + \alpha_2 \underbrace{\langle d_2, d_1 \rangle}_{=0} = 0,$$

also

$$\alpha_1 = -\langle b_3, d_1 \rangle,$$

und

$$\langle c_3, d_2 \rangle = \langle b_3, d_2 \rangle + \alpha_1 \underbrace{\langle d_1, d_2 \rangle}_{=0} + \alpha_2 \underbrace{\langle d_2, d_2 \rangle}_{=1} = 0,$$

also

$$\alpha_2 = -\langle b_3, d_2 \rangle.$$

Somit ergibt sich  $c_3$  als

$$c_3 = b_3 - \langle b_3, d_1 \rangle \cdot d_1 - \langle b_3, d_2 \rangle \cdot d_2$$

und der gesuchte Vektor  $d_3$  der Länge 1 als

$$d_3 = \frac{c_3}{\|c_3\|}.$$

(4) *Konstruktion von  $d_i$* : Seien  $d_1, \dots, d_{i-1}$  bereits bekannt. Dann setzen wir

$$c_i = b_i - \langle b_i, d_1 \rangle \cdot d_1 - \dots - \langle b_i, d_{i-1} \rangle \cdot d_{i-1}$$

und erhalten mit

$$d_i = \frac{c_i}{\|c_i\|}$$

den gewünschten Vektor.

AUFGABEN 5.13. (1) Sei

$$B = \left( \begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \\ 3 \\ -3 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \right).$$

Gesucht ist eine ONB von  $L(B)$ .

Offenbar ist  $c_1 = (1, -1, 1, -1)$  und somit

$$d_1 = \frac{c_1}{\|c_1\|} = \frac{1}{2} \begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix}.$$

Dann ist

$$c_2 = \begin{pmatrix} -1 \\ 1 \\ 3 \\ -3 \end{pmatrix} - \langle (-1, 1, 3, -3), d_1 \rangle \frac{1}{2} \begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix} = \begin{pmatrix} -2 \\ 2 \\ 2 \\ -2 \end{pmatrix}$$

und

$$d_2 = \frac{c_2}{\|c_2\|} = \frac{1}{2} \begin{pmatrix} -1 \\ 1 \\ 1 \\ -1 \end{pmatrix}.$$

Schließlich ist

$$c_3 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} - \langle (1, 0, 0, 0), d_1 \rangle d_1 - \langle (1, 0, 0, 0), d_2 \rangle d_2 = \frac{1}{2} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

und

$$d_3 = \frac{c_3}{\|c_3\|} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}.$$

(2) Sei  $B = ((3, 4), (5, 6))$ . Gesucht ist eine ONB von  $L(B)$ .

Wir erhalten

$$d_1 = \frac{1}{5} \begin{pmatrix} 3 \\ 4 \end{pmatrix} = \begin{pmatrix} 0.6 \\ 0.8 \end{pmatrix},$$

$$d_2 = \begin{pmatrix} 0.8 \\ -0.6 \end{pmatrix}.$$

Man prüft leicht nach, dass die beiden Vektoren tatsächlich normal aufeinander stehen.

**SATZ 5.14.** Sei  $T$  ein Unterraum des  $\mathbb{R}^n$ . Dann hat  $T$  eine ONB.

*Beweis.* Aus einer beliebigen Basis von  $T$  kann mit dem Gram-Schmidtschen Orthogonalisierungsverfahren eine ONB berechnet werden. ■

**ÜBUNGSAUFGABEN 5.15.**

- (1) Orthonormalisieren Sie die folgende Familie von Vektoren mit dem Verfahren von Gram-Schmidt!

$$A = \left( \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 3 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right).$$

- (2) Bestimmen Sie jeweils eine Orthonormalbasis (ONB) für folgende Unterräume des  $\mathbb{R}^3$ !

(a)  $U = L\left(\begin{pmatrix} 1 \\ 2 \\ -2 \end{pmatrix}, \begin{pmatrix} 3 \\ 2 \\ -1 \end{pmatrix}\right).$

(b)  $V = \{(x_1, x_2, x_3, x_4) \in \mathbb{R}^4 \mid x_1 + 2x_3 + 2x_4 = 0 \text{ und } x_2 - 2x_3 + 2x_4 = 0\}$ . (Hinweis: Berechnen Sie zuerst eine Basis von  $V$  und orthonormalisieren Sie diese mit dem Verfahren von Gram-Schmidt).

- (3) Geben Sie eine Orthonormalbasis der Ebene  $e : x - 2y + 3z = 0$  an.

- (4) Bestimmen Sie mithilfe des Verfahrens von Gram-Schmidt eine Orthonormalbasis von

$$\{(x_1, x_2, x_3, x_4) \in \mathbb{R}^4 \mid x_1 - x_2 + x_3 - x_4 = 0\}.$$

## 5. Orthogonalprojektionen

**SATZ 5.16.** Sei  $T$  ein Unterraum des  $\mathbb{R}^n$ ,  $v \in \mathbb{R}^n$ . Dann gibt es genau ein  $x \in \mathbb{R}^n$  mit den Eigenschaften

- (1)  $x \in T$ ,
- (2)  $v - x \in T^\perp$ .

Für den Beweis benötigen wir folgendes Lemma.

**LEMMA 5.17.** Seien  $b_1, \dots, b_k \in \mathbb{R}^n$  linear unabhängig.  $B$  sei definiert als die  $n \times k$ -Matrix mit den Spalten  $b_1, \dots, b_k$ . Dann ist  $B^T \cdot B$  invertierbar.

Man kann zeigen, dass die Spaltenvektoren von  $B^T \cdot B$  linear unabhängig sind. Später werden wir sehen (im Satz 10.13), dass jede quadratische Matrix mit linear unabhängigen Spaltenvektoren invertierbar ist.

*Beweis von Satz 5.16.*

- Zunächst zeigen wir, dass so ein  $x$  existiert. Sei  $(b_1, \dots, b_k)$  eine Basis von  $T$ , und sei  $B$  die  $n \times k$ -Matrix, in deren Spalten die Vektoren  $b_1, \dots, b_k$  stehen. Wir versuchen  $(\alpha_1, \dots, \alpha_k)$  zu finden, sodass

$$x := \sum_{i=1}^k \alpha_i \cdot b_i = B \cdot \underbrace{\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_k \end{pmatrix}}_{\alpha}$$

die Eigenschaft  $v - B \cdot \alpha \in T^\perp$  erfüllt. Dann muss gelten:  $\langle b_j, v - x \rangle = \langle b_j, v - B \cdot \alpha \rangle = 0$  für alle  $j$ , oder, anders ausgedrückt,

$$\begin{pmatrix} \langle b_1, v - B \cdot \alpha \rangle \\ \langle b_2, v - B \cdot \alpha \rangle \\ \vdots \\ \langle b_k, v - B \cdot \alpha \rangle \end{pmatrix} = B^T \cdot (v - B \cdot \alpha) = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

und somit

$$B^T \cdot v - B^T \cdot B \cdot \alpha = 0,$$

also

$$B^T \cdot v = (B^T \cdot B) \cdot \alpha.$$

Da die Basisvektoren linear unabhängig sind, ist nach Lemma 5.17 die Matrix  $B^T \cdot B$  invertierbar. Somit muss  $\alpha$  die Gleichung

$$(B^T \cdot B)^{-1} \cdot B^T \cdot v = (B^T \cdot B)^{-1} (B^T \cdot B) \cdot \alpha = \alpha$$

erfüllen. Wir erhalten als Kandidaten für  $x$  also

$$x = B \cdot (B^T \cdot B)^{-1} \cdot B^T \cdot v.$$

Wir überprüfen jetzt, ob  $v - x$  wirklich in  $T^\perp$  liegt, und erhalten

$$\begin{aligned} B^T(v - x) &= B^T(v - B \cdot (B^T \cdot B)^{-1} \cdot B^T \cdot v) \\ &= B^T \cdot v - B^T \cdot B \cdot (B^T \cdot B)^{-1} \cdot B^T \cdot v \\ &= B^T v - B^T v = 0. \end{aligned}$$

- Eindeutigkeit: Seien  $x, y$  zwei Vektoren, die den Bedingungen des Satzes 5.16 genügen, d.h.

- (1)  $x, y \in T$ ,

- (2)  $v - x, v - y \in T^\perp$ .

Wegen (1) gilt  $x - y \in T$ . Aus (2) erhalten wir  $(v - x) - (v - y) = -x + y \in T^\perp$ . Daher gilt auch  $-(-x + y) = x - y \in T^\perp$ . Da  $x - y \in T$  und  $x - y \in T^\perp$ , gilt  $\langle x - y, x - y \rangle = 0$ . Also gilt  $\|(x - y)\|^2 = 0$ , und folglich  $x = y$ .

Somit existiert genau ein  $x$ , das die obigen Eigenschaften erfüllt. ■

DEFINITION 5.18. Sei  $n \in \mathbb{N}$ , sei  $T$  ein Unterraum des  $\mathbb{R}^n$ , und sei  $v \in \mathbb{R}^n$ . Das  $x \in T$  mit  $v - x \in T^\perp$  nennen wir *orthogonale Projektion* von  $v$  auf  $T$  und schreiben  $x = P_T(v)$ .

Wenn  $T$  der Spaltenraum der Matrix  $B$  mit linear unabhängigen Spalten  $(b_1, \dots, b_k)$  ist, also  $T = S(B)$ , dann ist  $(b_1, \dots, b_k)$  eine Basis von  $T$ . Wie im Beweis von Satz 5.16 ermittelt, gilt dann

$$P_T(v) = B \cdot (B^T \cdot B)^{-1} \cdot B^T v.$$

AUFGABEN 5.19.

- (1) Gesucht ist die orthogonale Projektion von  $(4, 2)$  auf die Gerade  $G = \{(x, y) \mid 3x - 4y = 0\}$ .

Lösung: Für  $B = \begin{pmatrix} 4 \\ 3 \end{pmatrix}$  gilt  $G = S(B)$ . Wegen  $B^T \cdot B = (4^2 + 3^2) = (25)$  und  $B^T \cdot v = (16 + 6) = (22)$  ist

$$P_G(v) = B \cdot (B^T \cdot B)^{-1} \cdot B^T \cdot v = \frac{22}{25} \begin{pmatrix} 4 \\ 3 \end{pmatrix}.$$

- (2) Wir berechnen die orthogonale Projektion des Vektors  $v = (6, 0, 0)$  auf die Ebene  $e = L((1, 2, 1), (-1, 0, 1))$ . Wir bilden eine Matrix  $B$ , in deren Spalten wir die Basisvektoren von  $e$  schreiben. In diesem Fall gilt

$$B^T \cdot B = \begin{pmatrix} 1 & 2 & 1 \\ -1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 2 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 6 & 0 \\ 0 & 2 \end{pmatrix},$$

$$B^T \cdot v = \begin{pmatrix} 1 & 2 & 1 \\ -1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 6 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 6 \\ -6 \end{pmatrix}$$

$$\begin{aligned} P_e(v) &= B \cdot (B^T \cdot B)^{-1} \cdot B^T \cdot v = \begin{pmatrix} 1 & -1 \\ 2 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{6} & 0 \\ 0 & \frac{1}{2} \end{pmatrix} \begin{pmatrix} 6 \\ -6 \end{pmatrix} \\ &= \begin{pmatrix} 1 & -1 \\ 2 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ -3 \end{pmatrix} = \begin{pmatrix} 4 \\ 2 \\ -2 \end{pmatrix}. \end{aligned}$$

### ÜBUNGS-AUFGABEN 5.20.

Wir wollen die Pyramide mit der quadratischen Grundfläche  $(A, B, C, D)$  und der Spitze  $S$  als 2D-Graphik auf dem Bildschirm darstellen. Lösen Sie dazu folgende Probleme:

- (1) Sei die Ebene  $e = L(B)$  durch ihre Basis

$$B = \left( \frac{1}{\sqrt{10}} \begin{pmatrix} 3 \\ 0 \\ -1 \end{pmatrix}, \frac{1}{\sqrt{19}} \begin{pmatrix} 1 \\ -3 \\ 3 \end{pmatrix} \right)$$

gegeben. Bestimmen Sie für  $v = \begin{pmatrix} 2 \\ 2 \\ 0 \end{pmatrix}$  die Projektion von  $v$  auf  $L(B)$ , also  $P_{L(B)}(v)$ .

- (2) Bestimmen Sie die Koordinaten von  $P_{L(B)}(v)$  bezüglich  $B$ .  
 (3) Bestimmen Sie eine Orthonormalbasis der Ebene  $e$ , die durch

$$e : x - 2y + 2z = 0$$

gegeben ist.

- (4) Welcher Punkt auf  $e$  hat von  $\begin{pmatrix} -2 \\ -5 \end{pmatrix}$  den geringsten Abstand?

**SATZ 5.21.** Sei  $T$  ein Unterraum des  $\mathbb{R}^n$ ,  $v \in \mathbb{R}^n$ . Dann gilt

$$P_{T^\perp}(v) = v - P_T(v).$$

*Beweisskizze.* Wir definieren  $y := v - P_T(v)$ . Man kann zeigen, dass  $y$  die Eigenschaften der Projektion von  $v$  auf  $T^\perp$  erfüllt. ■

Aus diesem Satz können wir sofort eine Formel für die Projektion auf  $T^\perp$  ableiten. Sei  $B$  eine Matrix mit linear unabhängigen Spalten, sodass  $T = S(B)$ . Dann gilt:

$$P_{T^\perp}(v) = (E_n - B \cdot (B^T \cdot B)^{-1} \cdot B^T) \cdot v.$$

### ÜBUNGS-AUFGABEN 5.22.

- (1) (a) Bestimmen Sie für jeden Vektor  $v = (x, y, z) \in \mathbb{R}^3$  die Projektion auf  $U := \{(x, y, z) \mid -x + 2y + 2z = 0\}$ .  
 (b) Bestimmen Sie eine Matrix  $P_U$ , sodass die Projektion von  $v$  auf  $U$  gleich  $P_U \cdot v$  ist.  
 (c) Bestimmen Sie  $P_U \cdot P_U$ !

- (2) Sei  $U := \{(x, y, z) \mid -x + 2y + 2z = 0\}$ .
- Bestimmen sie für jeden Vektor  $v = (x, y, z) \in \mathbb{R}^3$  die Projektion von  $v$  auf den Orthogonalraum von  $U$ , also auf  $U^\perp$ .
  - Bestimmen Sie eine Matrix  $P_{U^\perp}$ , sodass die Projektion von  $v$  auf  $U^\perp$  gleich  $P_{U^\perp} \cdot v$  ist.
  - Bestimmen Sie  $P_{U^\perp} \cdot P_{U^\perp}$ .

## 6. Abstandsberechnungen mit Hilfe der Orthogonalprojektion

**6.1. Abstand eines Punktes von einem Unterraum.** Gegeben sei ein Unterraum  $T$  des  $\mathbb{R}^n$  sowie ein Vektor  $v \in \mathbb{R}^n$ . Gesucht ist jenes  $x \in T$ , das von  $v$  den kleinsten Abstand hat.

**SATZ 5.23.** Sei  $T$  ein Unterraum des  $\mathbb{R}^n$ ,  $v \in \mathbb{R}^n$ , und sei  $x \in T$ . Dann sind äquivalent:

- $\|v - x\| = \inf\{\|v - t\| : t \in T\}$ .
- Der Vektor  $x$  ist die Projektion von  $v$  auf  $T$ , also  $x = P_T(v)$ .

*Beweis.* (2) $\Rightarrow$ (1): Wir nehmen an,  $x = P_T(v)$ . Sei  $t \in T$ . Dann gilt

$$\|v - t\|^2 = \|(v - x) + (x - t)\|^2.$$

Da  $v - x \in T^\perp$  und  $x - t \in T$ , gilt

$$\|(v - x) + (x - t)\|^2 = \|v - x\|^2 + \|x - t\|^2.$$

Es gilt also

$$\text{Für alle } t \in T: \|v - t\| \geq \|v - x\|.$$

Also gilt

$$\|v - x\| = \inf\{\|v - t\| : t \in T\}.$$

(1) $\Rightarrow$ (2): Sei  $x$  so, dass  $\|v - x\| = \inf\{\|v - t\| : t \in T\}$ , und sei  $y = P_T(v)$ . Es gilt dann  $\|v - x\| \leq \|v - y\|$  und  $\|v - x\|^2 = \|(v - y) + (y - x)\|^2 = \|v - y\|^2 + \|y - x\|^2$ . Das ergibt insgesamt  $\|v - y\|^2 \geq \|v - y\|^2 + \|y - x\|^2$ , also  $\|y - x\|^2 = 0$ . Somit gilt  $x = y = P_T(v)$ . ■

### ÜBUNGSAUFGABEN 5.24.

- (1) Welcher Punkt auf der Geraden

$$g = L\left(\begin{pmatrix} 1 \\ 2 \\ -2 \end{pmatrix}\right)$$

hat von  $\begin{pmatrix} 2 \\ -1 \\ 9 \end{pmatrix}$  den kleinsten Abstand?

- (2) Wir betrachten den Punkt  $p \in \mathbb{R}^4$  und den Unterraum  $U$  des  $\mathbb{R}^4$ .

$$p = (8, 10, 1, 14),$$

$$U = L((-1, -2, 0, 3)).$$

Welcher Punkt  $p_0$  aus  $U$  hat von  $p$  den kleinsten Abstand?

**6.2. Abstand zwischen zwei linearen Mannigfaltigkeiten.** Wenn  $A$  und  $B$  nicht-leere Teilmengen des  $\mathbb{R}^n$  sind, dann kann man ihren *Abstand* durch

$$\text{dist}(A, B) = \inf\{\|a - b\| \mid a \in A, b \in B\}$$

definieren.

Gegeben sind zwei lineare Mannigfaltigkeiten  $M_1 = v_1 + T_1$  und  $M_2 = v_2 + T_2$ . Dabei sind  $v_1, v_2 \in \mathbb{R}^n$ , und  $T_1, T_2$  sind Unterräume des  $\mathbb{R}^n$ . Wir suchen  $p_1 \in M_1$  und  $p_2 \in M_2$ , sodass

$$\|p_1 - p_2\| = \text{dist}(M_1, M_2).$$

Dazu bestimmen wir  $t_1 \in T_1$  und  $t_2 \in T_2$ , sodass

$$\|(v_1 + t_1) - (v_2 + t_2)\| = \text{dist}(M_1, M_2).$$

Nun gilt

$$\begin{aligned} \text{dist}(M_1, M_2) &= \inf\{\|(v_1 + t_1) - (v_2 + t_2)\| \mid t_1 \in T_1, t_2 \in T_2\} \\ &= \inf\{\|(v_1 - v_2) - (t_2 - t_1)\| \mid t_1 \in T_1, t_2 \in T_2\} \\ &= \inf\{\|(v_1 - v_2) - s\| \mid s \in T_1 + T_2\}. \end{aligned}$$

Wir wissen, dass  $(v_1 - v_2) - \bar{s}$  genau dann das Infimum von  $\{(v_1 - v_2) - s \mid s \in T_1 + T_2\}$  annimmt, wenn  $\bar{s} = P_{T_1+T_2}(v_1 - v_2)$ . Also berechnen wir

$$\bar{s} := P_{T_1+T_2}(v_1 - v_2).$$

Folglich gilt für  $\bar{t}_1 \in T_1$  und  $\bar{t}_2 \in T_2$  die Gleichung

$$(v_1 + \bar{t}_1) - (v_2 + \bar{t}_2) = \inf\{(v_1 + t_1) - (v_2 + t_2) \mid t_1 \in T_1, t_2 \in T_2\}$$

genau dann, wenn  $\bar{t}_2 - \bar{t}_1 = \bar{s}$ . Wir müssen also alle  $(\bar{t}_1, \bar{t}_2) \in T_1 \times T_2$  bestimmen, sodass  $\bar{t}_2 - \bar{t}_1 = \bar{s}$ . Wir bestimmen uns also ein  $t'_1 \in T_1$  und ein  $t'_2 \in T_2$ , sodass  $t'_2 - t'_1 = \bar{s}$ . Dann gilt

$$\{(t_1, t_2) \in T_1 \times T_2 \mid t_1 - t_2 = s\} = \{t'_1 + r, t'_2 + r \mid r \in T_1 \cap T_2\}.$$

Damit erhalten wir

$$\{(p_1, p_2) \in M_1 \times M_2 \mid \|p_1 - p_2\| = \text{dist}(M_1, M_2)\} = \{(v_1 + t'_1 + r, v_2 + t'_2 + r) \mid r \in T_1 \cap T_2\}.$$

**AUFGABE 5.25.** Bestimmen Sie jene Punkte auf den Mannigfaltigkeiten

$$M_1 := (5, 0, 0, 0) + L((1, 2, -1, 0), (1, 1, 1, 1))$$

und

$$M_2 := (11, 27, 2, 11) + L((1, -1, -1, 1), (1, 0, 0, 1)),$$

die voneinander geringsten Abstand haben.

Sei  $T_1 = L((1, 2, -1, 0), (1, 1, 1, 1))$  und  $T_2 = L((1, -1, -1, 1), (1, 0, 0, 1))$ . Wir berechnen eine Basis von  $T_1 + T_2$ .

$$In[102] := \mathbf{B1} = \{\{1, 2, -1, 0\}, \{1, 1, 1, 1\}\};$$

$$\mathbf{B2} = \{\{1, -1, -1, 1\}, \{1, 0, 0, 1\}\};$$

`Out[102]= {{1, -1, -1, 1}, {1, 0, 0, 1}}`

`In[103]:= BasisVonT1PlusT2 = RowReduce [B1 ~Join~ B2]`

`Out[103]= {{1, 0, 0, 1}, {0, 1, 0, -1/3}, {0, 0, 1, 1/3}, {0, 0, 0, 0}}`

Also erhalten wir

$$B = ((1, 0, 0, 1), (0, 1, 0, -1/3), (0, 0, 1, 1/3))$$

als Basis von  $T_1 + T_2$ . Jetzt können wir die Projektion von  $v_1 - v_2$  auf  $T_1 + T_2$  ausrechnen.

Sei  $C$  die Matrix

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

Dann gilt

$$P_{T_1+T_2}(v_1 - v_2) = C \cdot (C^T \cdot C)^{-1} \cdot C^T \cdot (v_1 - v_2) = \begin{pmatrix} -12 \\ -25 \\ -4 \\ -5 \end{pmatrix}.$$

Also gilt  $\bar{s} = (-12, -25, -4, -5)$ . Dieses  $\bar{s}$  wollen wir als  $-t'_1 + t'_2$  mit  $t'_1 \in T_1$  und  $t'_2 \in T_2$  darstellen. Durch die folgenden Mathematica-Berechnungen erhalten wir

$$\bar{s} = -7 \cdot (1, 2, -1, 0) - 8 \cdot (1, 1, 1, 1) + 3 \cdot (1, -1, -1, 1) + 0 \cdot (1, 0, 0, 1).$$

`In[104]:= s`

`Out[104]= {-12, -25, -4, -5}`

`In[105]:= B1B2 = B1 ~Join~ B2`

`Out[105]= {{1, 2, -1, 0}, {1, 1, 1, 1}, {1, -1, -1, 1}, {1, 0, 0, 1}}`

`In[106]:= M = Transpose [B1B2]`

`Out[106]= {{1, 1, 1, 1}, {2, 1, -1, 0}, {-1, 1, -1, 0}, {0, 1, 1, 1}}`

`In[107]:= MatrixForm [M]`

$$\text{Out[107]= } \begin{pmatrix} 1 & 1 & 1 & 1 \\ 2 & 1 & -1 & 0 \\ -1 & 1 & -1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

`In[108]:= LinearSolve [M, s]`

`Out[108]= {-7, -8, 3, 0}`

Für  $t'_1 = 7 \cdot (1, 2, -1, 0) + 8 \cdot (1, 1, 1, 1)$  und  $t'_2 = 3 \cdot (1, -1, -1, 1)$  gilt also

$$\bar{s} = -t'_1 + t'_2.$$

Wir erhalten

$$t'_1 = (15, 22, 1, 8), \quad t'_2 = (3, -3, -3, 3).$$

Also sind die Punkte

$$p_1 = (5, 0, 0, 0) + (15, 22, 1, 8) = (20, 22, 1, 8)$$



und

$$p_2 = (11, 27, 2, 11) + (3, -3, -3, 3) = (14, 24, -1, 14)$$

so, dass  $p_1 \in M_1$ ,  $p_2 \in M_2$ , und  $\|p_1 - p_2\| = \text{dist}(M_1, M_2)$ .

Um alle Punkte zu erhalten, für die der Abstand minimal wird, müssen wir noch  $T_1 \cap T_2$  berechnen.

```
In[109]:= C1 = NullSpace [{1, 2, -1, 0}, {1, 1, 1, 1}];
          MatrixForm[C1]
```

```
Out[109]=  $\begin{pmatrix} -2 & 1 & 0 & 1 \\ -3 & 2 & 1 & 0 \end{pmatrix}$ 
```

```
In[110]:= C2 = NullSpace [{1, -1, -1, 1}, {1, 0, 0, 1}];
          MatrixForm[C2]
```

```
Out[110]=  $\begin{pmatrix} -1 & 0 & 0 & 1 \\ 0 & -1 & 1 & 0 \end{pmatrix}$ 
```

```
In[111]:= NullSpace [Join[C1, C2]]
```

```
Out[111]= {{1, 1, 1, 1}}
```

Wir erhalten  $T_1 \cap T_2 = L((1, 1, 1, 1))$ . Somit ist die Menge aller Paare in  $M_1 \times M_2$ , die minimalen Abstand voneinander haben, gegeben als

$$\{(20, 22, 1, 8) + t \cdot (1, 1, 1, 1), (14, 24, -1, 14) + t \cdot (1, 1, 1, 1) \mid t \in \mathbb{R}\}.$$

Folgendes Mathematica-Programm liefert zwei Punkte mit minimaler Distanz. Achtung: die Basisvektoren von  $T_1$  und  $T_2$  stehen hier in den *Zeilen* der Argumente  $B_1$  und  $B_2$ .

```
Proj [B_, v_] :=
  Transpose [B] . Inverse [B . Transpose[B]]. B . v;

PointsWithMinimalDistance [v1_, B1_, v2_, B2_] :=
Module[{ },
  B12 = RowReduce [B1 ~Join~ B2];
  If [MatrixRank[B12] == 0,
    {v1, v2},
    Basis12 = Take [B12, MatrixRank [B12]];
    s = Proj [Basis12, v1 - v2];
    t1 = - Transpose [B1].Take [LinearSolve
      [Transpose [B1 ~Join~ B2], s], Length [B1]];
    t2 = s + t1;
    {v1 + t1, v2 + t2}
  ]
];
```

Wir testen dieses Programm:

```
In[112]:= << abstand2.m
```

```
In[113]:= v1 = {5, 0, 0, 0};
```

```
      v2 = {11, 27, 2, 11};
```

```
      T1 = {{1, 1, 1, 1}, {1, 2, -1, 0}};
```

```
      T2 = {{1, 0, 0, 1}, {1, -1, -1, 1}};
```

```
In[114]:= PointsWithMinimalDistance [v1, T1, v2, T2]
```

```
Out[114]= {{23, 25, 4, 11}, {17, 27, 2, 17}}
```

### ÜBUNGSAUFGABEN 5.26.

- (1) Welcher Punkt auf der Geraden

$$g : X = \begin{pmatrix} 0 \\ 0 \end{pmatrix} + \lambda \cdot \begin{pmatrix} 1 \\ -4 \end{pmatrix}$$

hat von  $\begin{pmatrix} 6 \\ -7 \end{pmatrix}$  den geringsten Abstand?

- (2) Bestimmen Sie den Punkt auf  $L\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix} + L\left(\begin{pmatrix} 1 \\ -2 \end{pmatrix}\right)\right)$ , der am nächsten beim Punkt  $\begin{pmatrix} 2 \\ 3 \end{pmatrix}$  liegt.

- (3) (a) Bestimmen Sie eine Orthonormalbasis des Unterraums  $W$  von  $\mathbb{R}^4$ , der durch

$$W = \{(x_1, x_2, x_3, x_4) \mid -x_1 + x_3 = 0 \text{ und } -x_2 + x_4 = 0\}.$$

gegeben ist.

- (b) Welcher Punkt in  $W$  hat von  $(4, -1, 6, -1)$  den geringsten Abstand?

- (4) Bestimmen Sie den Abstand des Punktes  $\begin{pmatrix} -6 \\ 4 \\ -2 \end{pmatrix}$  von der Geraden  $g$ , die durch den Punkt  $\begin{pmatrix} 0 \\ 0 \\ 10 \end{pmatrix}$  geht, und deren Richtungsvektor gleich  $\begin{pmatrix} 1 \\ -2 \\ 3 \end{pmatrix}$  ist.

- (5) Bestimmen Sie den Abstand des Punktes  $(8, 2, 11, 17)$  von der Geraden  $g$ , die durch

$$g : X = (1, 2, -4, 7) + t \cdot (12, 0, 3, 4)$$

gegeben ist. Welcher Geradenpunkt ist diesem Punkt am nächsten?

- (6) (a) Welcher Punkt  $p$  auf der Geraden

$$g : -2x + z = 0 \text{ und } 2x + y = 0$$

hat vom Punkt  $v = \begin{pmatrix} -10 \\ -25 \\ 25 \end{pmatrix}$  den geringsten Abstand?

- (b) Wie groß ist dieser Abstand?

- (c) Berechnen Sie  $v - p$ ! Welchen Winkel schließen  $p$  und  $v - p$  miteinander ein?

- (7) Welcher Punkt der Ebene

$$e : X = \begin{pmatrix} -24 \\ -53 \\ 13 \end{pmatrix} + \lambda \cdot \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + \mu \cdot \begin{pmatrix} -1 \\ 7 \\ 2 \end{pmatrix}$$

kommt dem Punkt  $\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$  am nächsten ?

- (8) Welche Punkte der Geraden

$$g_1 : X = \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix} + \lambda \cdot \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}$$

und

$$g_2 : X = \begin{pmatrix} -24 \\ -52 \\ 15 \end{pmatrix} + \mu \cdot \begin{pmatrix} -1 \\ 7 \\ 2 \end{pmatrix}$$

kommen einander am nächsten?

- (9) Welcher Punkt der Ebene

$$e : X = \begin{pmatrix} -24 \\ -53 \\ 13 \end{pmatrix} + \lambda \cdot \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} + \mu \cdot \begin{pmatrix} -1 \\ 7 \\ 2 \end{pmatrix}$$

kommt dem Punkt  $\begin{pmatrix} -47 \\ -95 \\ 34 \end{pmatrix}$  am nächsten?

(10) Welcher Punkt der Ebene

$$e : X = (5, 2, 1, 0) + \lambda \cdot (1, 2, 0, 0) + \mu \cdot (0, 1, 2, -1)$$

kommt der Geraden

$$g : X = (5, 3, 0, 5) + \alpha \cdot (1, 0, 2, 0)$$

am nächsten?

(11) Berechnen Sie den Inkreismittelpunkt  $I = \begin{pmatrix} i_1 \\ i_2 \end{pmatrix}$  des Dreiecks  $ABC$  mit  $A = \begin{pmatrix} -3 \\ 2 \end{pmatrix}$ ,  $B = \begin{pmatrix} 4 \\ 0 \end{pmatrix}$  und  $C = \begin{pmatrix} 2 \\ 4 \end{pmatrix}$ , indem Sie die Bedingung, dass  $I$  gleich weit von  $AB$ ,  $BC$  und  $AC$  entfernt ist, in Gleichungen in den Variablen  $i_1$  und  $i_2$  umwandeln. Verwenden Sie zur Lösung der auftretenden Gleichungen den Mathematica-Befehl `Solve`.

## 7. Die bestapproximierende Lösung eines linearen Gleichungssystems

Oft trifft man auf Gleichungssysteme, die keine Lösung besitzen, wie z.B.

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

In solchen Fällen wird man ein  $x$  suchen, das dem Gleichungssystem “möglichst gut” genügt. Naheliegender ist es, jenes  $x$  als “Lösung” zu betrachten, das den kleinsten Fehler liefert, d.h. für das  $\|A \cdot x - b\|$  minimal ist.

DEFINITION 5.27. Sei  $A \in \mathbb{R}^{m \times n}$ ,  $b \in \mathbb{R}^m$ . Eine *bestapproximierende Lösung* des Gleichungssystems  $A \cdot x = b$  ist ein  $x^* \in \mathbb{R}^n$ , sodass  $\|A \cdot x^* - b\|$  minimal ist.

Wir wissen, dass  $\{A \cdot x \mid x \in \mathbb{R}^n\}$  genau der Spaltenraum von  $A$  ist. Wir suchen also jenes Element des Spaltenraumes von  $A$ , das von  $b$  minimalen Abstand hat. Dazu sollte  $A \cdot x$  die Projektion von  $b$  auf den Spaltenraum von  $A$  sein. Dann steht  $b - A \cdot x$  auf dem Spaltenraum von  $A$  normal. Es gilt also

$$A^T \cdot (b - A \cdot x) = 0.$$

Wenn  $A^T \cdot A$  invertierbar ist, dann können wir  $x$  durch  $x = (A^T \cdot A)^{-1} \cdot A^T \cdot b$  bestimmen.

SATZ 5.28. Sei  $A$  eine Matrix, deren Spaltenvektoren linear unabhängig sind, und sei  $b$  ein Vektor. Dann ist die bestapproximierende Lösung  $x^*$  von  $A \cdot x = b$  gegeben durch

$$x^* = (A^T \cdot A)^{-1} \cdot A^T \cdot b.$$

AUFGABE 5.29. Wir bestimmen die bestapproximierende Lösung von

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

Hier ist

$$A^T \cdot A = \begin{pmatrix} 6 & 1 \\ 1 & 2 \end{pmatrix} \quad \text{und} \quad (A^T \cdot A)^{-1} = \frac{1}{11} \begin{pmatrix} 2 & -1 \\ -1 & 6 \end{pmatrix}.$$

Also erhalten wir

$$x^* = \frac{1}{11} \begin{pmatrix} 8 \\ 7 \end{pmatrix}.$$

### ÜBUNGS-AUFGABEN 5.30.

- (1) Das Gleichungssystem  $A \cdot x = b$  ist für folgendes  $A$  und  $b$  unlösbar:

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

Bestimmen Sie die "beste Näherungslösung". Warum (bzw. in welchem Sinn) ist diese Lösung "besser" als  $(1, 1)$ ?

Nun versuchen wir, die "beste Gerade durch eine Punktwolke" zu legen.

Gegeben seien die Punkte  $(x_1, y_1), \dots, (x_n, y_n)$ . Gesucht ist die bestapproximierende Gerade  $y = kx + d$  durch diese Punktwolke.

Dafür berechnet man die bestapproximierende Lösung des Gleichungssystems

$$\begin{pmatrix} x_1 & 1 \\ \vdots & \vdots \\ x_n & 1 \end{pmatrix} \begin{pmatrix} k \\ d \end{pmatrix} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

wie oben beschrieben. Wir überlegen uns noch, welcher "Abstand" zwischen Punkten und Gerade hier wirklich minimiert wird. Die bestapproximierende Lösung minimiert

$$\left\| \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} - \begin{pmatrix} x_1 & 1 \\ \vdots & \vdots \\ x_n & 1 \end{pmatrix} \begin{pmatrix} k \\ d \end{pmatrix} \right\| = \left\| \begin{pmatrix} y_1 - (kx_1 + d) \\ \vdots \\ y_n - (kx_n + d) \end{pmatrix} \right\|,$$

also die Vertikalabstände zwischen den Punkten und der Gerade.

### ÜBUNGS-AUFGABEN 5.31.

- (1) Bestimmen Sie jene Gerade der Form  $y = kx + d$ , die die Punkte  $(0, 3)$ ,  $(1, 4)$  und  $(2, 7)$  bestmöglich approximiert. "Bestmöglich" heißt dabei, dass  $k$  und  $d$  so zu bestimmen sind, dass

$$(y_1 - (kx_1 + d))^2 + (y_2 - (kx_2 + d))^2 + (y_3 - (kx_3 + d))^2$$

minimal wird.

- (2) Bestimmen Sie jene Gerade der Form  $y = kx + d$ , die die Punkte  $(2, 3)$ ,  $(3, 0)$  und  $(6, 5)$  bestmöglich approximiert. "Bestmöglich" heißt dabei, dass  $k$  und  $d$  so zu bestimmen sind, dass

$$(y_1 - (kx_1 + d))^2 + (y_2 - (kx_2 + d))^2 + (y_3 - (kx_3 + d))^2$$

minimal wird.

## KAPITEL 6

### Rechnen in den ganzen Zahlen

#### 1. Teilbarkeit

DEFINITION 6.1 (Primzahl). Eine Zahl  $p \in \mathbb{N}$  ist genau dann eine *Primzahl*, wenn folgende beiden Bedingungen gelten:

- (1) Es gilt  $p > 1$ .
- (2) Für alle  $a, b \in \mathbb{N}$  mit  $p = a \cdot b$  gilt  $a = 1$  oder  $b = 1$ .

DEFINITION 6.2 (Teilbarkeit). Für  $x, y \in \mathbb{Z}$  gilt

$$x \text{ teilt } y$$

genau dann, wenn es ein  $z \in \mathbb{Z}$  gibt, sodass  $y = z \cdot x$  ist.

Wir schreiben dann auch  $x|y$ ; die Zahl  $y$  heißt ein *Vielfaches* von  $x$ .

SATZ 6.3. Seien  $a \in \mathbb{Z}$  und  $n \in \mathbb{N}$ . Dann gibt es genau ein Paar von Zahlen  $(q, r)$ , sodass  $a = q \cdot n + r$  und  $r \in \{0, \dots, n-1\}$ .

Wir bezeichnen den Rest  $r$  mit  $a \bmod n$ .

DEFINITION 6.4 (Größter gemeinsamer Teiler). Für zwei Zahlen  $a, b \in \mathbb{Z}$  (nicht beide 0) ist  $\text{ggT}(a, b)$  die größte Zahl  $z \in \mathbb{N}$  mit  $z | a$  und  $z | b$ .

SATZ 6.5. Seien  $a, b \in \mathbb{Z}$  nicht beide 0, und sei  $z \in \mathbb{Z}$ . Dann gilt:

$$\text{ggT}(a, b) = \text{ggT}(a + z \cdot b, b).$$

So gilt zum Beispiel  $\text{ggT}(25, 15) = \text{ggT}(40, 15)$ .

*Beweis:* Wir zeigen, dass nicht nur der ggT, sondern sogar die Mengen der gemeinsamen Teiler der beiden Zahlenpaare gleich sind. Wir zeigen also

$$\{t \in \mathbb{Z} : t | a \text{ und } t | b\} = \{t \in \mathbb{Z} : t | a + zb \text{ und } t | b\}.$$

“ $\subseteq$ ”: Falls  $t$  sowohl  $a$  als auch  $b$  teilt, dann auch  $a + zb$  und  $b$ . “ $\supseteq$ ”: Falls  $t$  sowohl  $a + zb$ , als auch  $b$  teilt, dann auch  $a + zb - zb$  und  $b$ , also auch  $a$  und  $b$ . ■

Das nützen wir jetzt möglichst geschickt aus, um  $\text{ggT}(147, 33)$  zu berechnen:

$$\begin{aligned}\text{ggT}(147, 33) &= \text{ggT}(147 - 4 \cdot 33, 33) \\ &= \text{ggT}(15, 33) \\ &= \text{ggT}(15, 33 - 2 \cdot 15) \\ &= \text{ggT}(15, 3) \\ &= \text{ggT}(0, 3) \\ &= 3.\end{aligned}$$

Günstig ist es also,  $z$  so zu wählen, dass  $a + zb$  der Rest von  $a$  bei der Division durch  $b$  wird.

Mit Hilfe des *erweiterten Euklidischen Algorithmus* findet man nicht nur den  $\text{ggT}$  von  $a$  und  $b$ , sondern auch  $u, v \in \mathbb{Z}$ , sodass gilt:

$$\text{ggT}(a, b) = u \cdot a + v \cdot b.$$

**Beispiel:** Wir berechnen  $\text{ggT}(147, 33)$ , und schreiben das so:

	147	33	
147	1	0	(147 = 1 \cdot 147 + 0 \cdot 33)
33	0	1	(33 = 0 \cdot 147 + 1 \cdot 33)
15	1	-4	(15 = 1 \cdot 147 - 4 \cdot 33)
3	-2	9	(3 = -2 \cdot 147 + 9 \cdot 33)
0			

Berechnet man  $\text{ggT}(a, b)$  mithilfe dieses Algorithmus, sieht man, dass sich die Zahlen in der linken Spalte immer als Linearkombination von  $a$  und  $b$  schreiben lassen. Als Konsequenz davon erhalten wir folgenden Satz:

**SATZ 6.6.** Seien  $a, b \in \mathbb{Z}$  (nicht beide 0). Dann gibt es  $u, v \in \mathbb{Z}$ , sodass

$$\text{ggT}(a, b) = u \cdot a + v \cdot b.$$

Eine Folgerung davon ist:

**SATZ 6.7.** Seien  $a, b \in \mathbb{Z}$ , nicht beide 0, und sei  $t \in \mathbb{Z}$  so, dass  $t|a$  und  $t|b$ . Dann gilt auch  $t|\text{ggT}(a, b)$ .

*Beweis:* Seien  $u, v \in \mathbb{Z}$  so, dass  $\text{ggT}(a, b) = ua + vb$ . Da  $t$  die Zahl  $a$  teilt, ist auch  $ua$  ein Vielfaches von  $t$ . Ebenso ist  $vb$  ein Vielfaches von  $t$ . Somit ist auch die Summe  $ua + vb$  ein Vielfaches von  $t$ . Die Zahl  $t$  ist also ein Teiler von  $\text{ggT}(a, b)$ .

Wenn  $a$  und  $b$  größten gemeinsamen Teiler 1 haben, so heißen sie *teilerfremd* oder *relativ prim*.

**SATZ 6.8.** Seien  $a, b, c \in \mathbb{Z}$ , und sei zumindest eine der Zahlen  $a$  und  $b$  nicht 0. Wir nehmen an, dass  $a$  die Zahl  $b \cdot c$  teilt, und dass  $\text{ggT}(a, b) = 1$  gilt. Dann gilt:  $a$  teilt  $c$ .

*Beweis:* Es gibt  $u, v \in \mathbb{Z}$ , sodass

$$1 = u \cdot a + v \cdot b.$$

Es gilt  $a \mid uac$ . Da nach Voraussetzung  $a \mid bc$  gilt, gilt auch  $a \mid vbc$ . Daraus erhalten wir

$$a \mid (ua + vb)c,$$

und somit  $a \mid c$ . ■

Daraus kann man folgenden Satz herleiten:

SATZ 6.9.

(1) Jede natürliche Zahl  $a \geq 2$  besitzt eine Zerlegung in Primfaktoren

$$a = p_1 \cdot \dots \cdot p_n.$$

(2) Die Primfaktorenzerlegung einer natürlichen Zahl  $a \geq 2$  ist bis auf die Reihenfolge der Primfaktoren eindeutig. Wenn also

$$a = p_1 \cdot \dots \cdot p_n = q_1 \cdot \dots \cdot q_m$$

und alle  $p_i, q_i$  Primzahlen sind, dann gilt  $m = n$ , und es gibt eine bijektive Abbildung  $\pi : \{1, \dots, n\} \rightarrow \{1, \dots, m\}$ , sodass  $p_i = q_{\pi(i)}$ .

Sind  $a, b \in \mathbb{Z}$ , so nennt man jede Zahl  $c \in \mathbb{Z}$ , die von  $a$  und  $b$  geteilt wird, ein gemeinsames Vielfaches von  $a$  und  $b$ . Unter allen gemeinsamen Vielfachen zeichnen wir das kleinste aus.

DEFINITION 6.10. Es seien  $a, b \in \mathbb{Z} \setminus \{0\}$ . Dann ist  $\text{kgV}(a, b)$  definiert durch

$$\text{kgV}(a, b) = \min \{v \in \mathbb{N} : a \mid v \text{ und } b \mid v\}.$$

Die Menge aller positiven gemeinsamen Vielfachen ist ja für  $a, b \in \mathbb{Z} \setminus \{0\}$  bestimmt nicht leer, da sie  $|a \cdot b|$  enthält.

SATZ 6.11. Seien  $a, b \in \mathbb{Z} \setminus \{0\}$ , und sei  $s \in \mathbb{Z}$  so, dass  $a \mid s$  und  $b \mid s$ . Dann gilt:

$$\text{kgV}(a, b) \mid s.$$

Jedes gemeinsame Vielfache ist also ein Vielfaches des  $\text{kgV}$ .

*Beweis:* Wir dividieren  $s$  durch  $\text{kgV}(a, b)$  und erhalten somit  $r \in \{0, \dots, \text{kgV}(a, b) - 1\}$  und  $q \in \mathbb{Z}$ , sodass

$$s = q \cdot \text{kgV}(a, b) + r.$$

Also gilt  $r = s - q \cdot \text{kgV}(a, b)$ . Sowohl  $s$  also auch  $q \cdot \text{kgV}(a, b)$  sind Vielfache von  $a$  und Vielfache von  $b$ . Ihre Differenz  $r$  ist also ebenfalls ein Vielfaches von  $a$  und von  $b$ . Da  $r < \text{kgV}(a, b)$ , und da  $\text{kgV}(a, b)$  das kleinste gemeinsame Vielfache ist, muss  $r = 0$  gelten. Also ist  $s$  ein Vielfaches von  $\text{kgV}(a, b)$ . ■

Zwischen ggT und kgV gilt folgender Zusammenhang.

SATZ 6.12. Seien  $a, b \in \mathbb{N}$ . Dann gilt

$$\text{ggT}(a, b) \cdot \text{kgV}(a, b) = a \cdot b.$$

*Beweis:* Wir verwenden die Primfaktorzerlegung von  $a$  und  $b$ . Sei  $(p_1, p_2, p_3, \dots) = (2, 3, 5, \dots)$  die Folge der Primzahlen, und seien  $(v_i)_{i \in \mathbb{N}}$  und  $(\sigma_i)_{i \in \mathbb{N}}$  so dass  $a = \prod_{i \in \mathbb{N}} p_i^{v_i}$  und  $b = \prod_{i \in \mathbb{N}} p_i^{\sigma_i}$ . Aus der Eindeutigkeit der Primfaktorzerlegung kann man herleiten, dass dann gelten muss:

$$\begin{aligned} \text{ggT}(a, b) &= \prod_{i \in \mathbb{N}} p_i^{\min(v_i, \sigma_i)} \\ \text{kgV}(a, b) &= \prod_{i \in \mathbb{N}} p_i^{\max(v_i, \sigma_i)}. \end{aligned}$$

Daraus folgt:

$$\begin{aligned} \text{ggT}(a, b) \cdot \text{kgV}(a, b) &= \prod_{i \in \mathbb{N}} p_i^{(\min(v_i, \sigma_i) + \max(v_i, \sigma_i))} \\ &= \prod_{i \in \mathbb{N}} p_i^{(v_i + \sigma_i)} \\ &= a \cdot b. \end{aligned}$$

■

SATZ 6.13. Seien  $a, b, c \in \mathbb{N}$ . Dann gilt:

- (1)  $\text{ggT}(\text{ggT}(a, b), c) = \text{ggT}(a, \text{ggT}(b, c))$ .
- (2)  $\text{kgV}(\text{kgV}(a, b), c) = \text{kgV}(a, \text{kgV}(b, c))$ .
- (3)  $\text{ggT}(\text{kgV}(a, b), c) = \text{kgV}(\text{ggT}(a, c), \text{ggT}(b, c))$ .
- (4)  $\text{kgV}(\text{ggT}(a, b), c) = \text{ggT}(\text{kgV}(a, c), \text{kgV}(b, c))$ .

## 2. Das Lösen von Kongruenzen

DEFINITION 6.14. Sei  $n \in \mathbb{Z}$ . Dann definieren wir eine Relation  $\equiv_n$  auf  $\mathbb{Z}$  durch

$$a \equiv_n b : \Leftrightarrow n \mid a - b \text{ für } a, b \in \mathbb{Z}.$$

Für  $a \equiv_n b$  schreiben wir auch  $a \equiv b \pmod{n}$  und sagen: “ $a$  ist kongruent  $b$  modulo  $n$ .”

SATZ 6.15. Seien  $a, c \in \mathbb{Z}$  (nicht beide = 0), und sei  $b \in \mathbb{Z}$ . Dann sind die folgenden Bedingungen äquivalent:

- (1) Die Kongruenz

$$ax \equiv b \pmod{c}$$

ist lösbar, das heißt, es gibt  $y \in \mathbb{Z}$  sodass  $c \mid a \cdot y - b$ .

- (2)  $\text{ggT}(a, c)$  teilt  $b$ .



*Beweis:* “(1)  $\Rightarrow$  (2)”: Sei  $x$  eine Lösung, d.h.  $c \mid ax - b$ . Falls  $c$  die Zahl  $ax - b$  teilt, dann gilt erst recht

$$\text{ggT}(a, c) \mid ax - b.$$

$\text{ggT}(a, c)$  teilt  $a$ , also gilt  $\text{ggT}(a, c) \mid b$ .

“(2)  $\Rightarrow$  (1)”: Aufgrund der Voraussetzungen existiert ein  $z \in \mathbb{Z}$ , sodass

$$\text{ggT}(a, c) \cdot z = b.$$

Aus dem erweiterten Euklidischen Algorithmus bekommen wir  $u, v \in \mathbb{Z}$  mit

$$\text{ggT}(a, c) = u \cdot a + v \cdot c.$$

Es gilt dann

$$(ua + vc) \cdot z = b,$$

also

$$a \cdot uz + c \cdot vz = b,$$

und somit

$$a \cdot (uz) \equiv b \pmod{c}.$$

Also ist  $x := uz$  Lösung von  $ax \equiv b \pmod{c}$ . ■

SATZ 6.16. Seien  $a, c \in \mathbb{Z}$  (nicht beide = 0), und sei  $b \in \mathbb{Z}$ . Sei  $x_0$  eine Lösung von

$$(6.1) \quad ax \equiv b \pmod{c}.$$

Dann ist die Lösungsmenge von (6.1) gegeben durch:

$$L = \left\{ x_0 + k \cdot \frac{c}{\text{ggT}(a, c)} \mid k \in \mathbb{Z} \right\}.$$

*Beweis:* “ $\supseteq$ ”: Wir setzen zunächst  $x_0 + k \frac{c}{\text{ggT}(a, c)}$  ein und erhalten

$$\begin{aligned} a \left( x_0 + k \frac{c}{\text{ggT}(a, c)} \right) &= ax_0 + ak \frac{c}{\text{ggT}(a, c)} \\ &\equiv_c b + ak \frac{c}{\text{ggT}(a, c)} \\ &= b + ck \frac{a}{\text{ggT}(a, c)} \\ &\equiv_c b. \end{aligned}$$

Daher ist  $x_0 + k \frac{c}{\text{ggT}(a, c)}$  wirklich eine Lösung.

“ $\subseteq$ ”: Sei  $x_1$  Lösung von  $ax \equiv b \pmod{c}$ . Zu zeigen ist:  $\frac{c}{\text{ggT}(a, c)} \mid (x_1 - x_0)$ . Da  $x_1$  und  $x_0$  Lösungen sind, gilt  $ax_1 \equiv b \pmod{c}$  und  $ax_0 \equiv b \pmod{c}$ . Daher gilt

$$a(x_1 - x_0) \equiv 0 \pmod{c},$$

oder, äquivalent dazu,

$$c \mid a(x_1 - x_0).$$

Daher gilt auch

$$\frac{c}{\text{ggT}(a, c)} \mid \frac{a}{\text{ggT}(a, c)} \cdot (x_1 - x_0).$$

Da

$$\text{ggT}\left(\frac{c}{\text{ggT}(a, c)}, \frac{a}{\text{ggT}(a, c)}\right) = 1,$$

gilt

$$\frac{c}{\text{ggT}(a, c)} \mid (x_1 - x_0).$$

■

**Bemerkung:** Das System  $ax \equiv b \pmod{c}$  ist also äquivalent zu

$$x \equiv x_0 \left( \text{mod } \frac{c}{\text{ggT}(a, c)} \right),$$

wobei  $x_0$  eine spezielle Lösung von  $ax \equiv b \pmod{c}$  ist.

Wir betrachten nun Systeme von zwei Kongruenzen, also Systeme der Form

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2}, \end{aligned}$$

wobei  $m_1, m_2 \in \mathbb{N}$  und  $a_1, a_2 \in \mathbb{Z}$ .

**Beispiele:** Das System

$$\begin{aligned} x &\equiv 1 \pmod{2} \\ x &\equiv 0 \pmod{4} \end{aligned}$$

kann nicht lösbar sein, denn eine Lösung  $x \in \mathbb{Z}$  müsste sowohl gerade als auch ungerade sein. Das System

$$\begin{aligned} x &\equiv 1 \pmod{2} \\ x &\equiv 2 \pmod{5} \end{aligned}$$

hat zum Beispiel die Lösung  $x = 7$ .

**SATZ 6.17.** Seien  $a_1, a_2 \in \mathbb{Z}$ ,  $m_1, m_2 \in \mathbb{N}$ . Das System

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \end{aligned}$$

ist genau dann lösbar, wenn gilt

$$\text{ggT}(m_1, m_2) \mid a_1 - a_2.$$

*Beweis:* “ $\Rightarrow$ ”: Wir nehmen an, dass  $x$  Lösung ist. Dann gilt:  $m_1 \mid (x - a_1)$  und  $m_2 \mid (x - a_2)$ . Daher gilt auch  $\text{ggT}(m_1, m_2) \mid (x - a_1)$  und  $\text{ggT}(m_1, m_2) \mid (x - a_2)$ , und somit

$$\text{ggT}(m_1, m_2) \mid (x - a_2) - (x - a_1) = (a_1 - a_2).$$

“ $\Leftarrow$ ” Es gibt  $u, v \in \mathbb{Z}$ , sodass

$$\begin{aligned} u \cdot m_1 + v \cdot m_2 &= \text{ggT}(m_1, m_2) \\ k \cdot u \cdot m_1 + k \cdot v \cdot m_2 &= a_1 - a_2 \\ a_2 + k \cdot v \cdot m_2 &= \underbrace{a_1 - k \cdot u \cdot m_1}_{=x} \end{aligned}$$

daher ist  $x := a_1 - kum_1$  Lösung des Systems.  $\square$

Der Beweis liefert auch gleich ein Lösungsverfahren.

**Beispiel:** Wir lösen:

$$x \equiv 2 \pmod{15}$$

$$x \equiv 8 \pmod{21}$$

Da  $\text{ggT}(15, 21) = 3$  und  $3 \mid (2 - 8)$  ist das System lösbar. Wir berechnen jetzt diesen  $\text{ggT}$  und *Kofaktoren* (d.h. Koeffizienten für eine Linearkombination von 15 und 21, die den  $\text{ggT}$  ergibt).

$$\begin{array}{r|rr} & 21 & 15 \\ \hline 21 & 1 & 0 \\ 15 & 0 & 1 \\ 6 & 1 & -1 \\ 3 & -2 & 3 \end{array}$$

und erhalten daraus  $3 = 3 \cdot 15 - 2 \cdot 21$ .

$$\begin{aligned} 3 \cdot 15 - 2 \cdot 21 &= 3 \\ (-6) \cdot 15 + 4 \cdot 21 &= 2 - 8 \\ \underline{8 + 4 \cdot 21} &= \underline{2 + 6 \cdot 15} \\ &=92 \qquad \qquad \qquad =92 \end{aligned}$$

Daher erhalten wir eine Lösung:  $x = 92$ .

Der folgende Satz gibt an, wie wir aus einer Lösung der Kongruenz alle Lösungen erhalten.

**SATZ 6.18.** Sei  $x_0$  eine Lösung von

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2}. \end{aligned}$$

Dann gilt für die Lösungsmenge  $L$

$$L = \{x_0 + k \cdot \text{kgV}(m_1, m_2) \mid k \in \mathbb{Z}\}.$$

*Beweis:* “ $\supseteq$ ”: Wir setzen

$$x_0 + k \cdot \text{kgV}(m_1, m_2)$$

in die erste Kongruenz ein und erhalten

$$(x_0 + k \cdot \text{kgV}(m_1, m_2)) \equiv a_1 \pmod{m_1}.$$

Das gleiche gilt für die zweite Kongruenz.

“ $\subseteq$ ”: Wir fixieren  $x_1 \in L$ . Um zu zeigen, dass  $x_1 \in \{x_0 + k \cdot \text{kgV}(m_1, m_2) \mid k \in \mathbb{Z}\}$ , zeigen wir, dass  $x_1 - x_0$  ein Vielfaches von  $\text{kgV}(m_1, m_2)$  ist. Wir wissen ja, dass

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \end{aligned}$$

Daher gilt  $(x_1 - x_0) \equiv 0 \pmod{m_1}$  und somit  $m_1 \mid (x_1 - x_0)$ . Ebenso zeigt man, dass  $m_2 \mid (x_1 - x_0)$  gilt.

Da das  $\text{kgV}$  jedes gemeinsame Vielfache teilt, gilt  $\text{kgV}(m_1, m_2) \mid (x_1 - x_0)$ . ■

## KAPITEL 7

### Ringe, Körper und Vektorräume

Nachrichten codiert man gerne als Listen von Bits. Deswegen wird es sich als günstig herausstellen, dass man nicht nur mit Vektoren, deren Einträge reelle Zahlen sind, rechnen kann, sondern auch mit Vektoren, deren Einträge nur 0 oder 1 sein können. Unser Wissen über das Lösen linearer Gleichungssysteme lässt sich auf solche 0/1-Vektoren verallgemeinern; das ist in der Codierungstheorie hilfreich.

#### 1. Ringe

Unser Ziel ist, anstelle der reellen Zahlen auch andere Objekte verwenden zu können, solange man diese Objekte sinnvoll addieren und multiplizieren kann.

DEFINITION 7.1. Das 6-Tupel  $\langle R, +, -, 0, \cdot, 1 \rangle$  ist ein *Ring*, falls gilt:

- (1)  $R$  ist eine nichtleere Menge,
- (2)  $+$  und  $\cdot$  sind Funktionen von  $R^2$  nach  $R$ ,
- (3)  $-$  ist eine Funktion von  $R$  nach  $R$ ,
- (4)  $0, 1$  sind Elemente von  $R$ ,
- (5) für alle  $x, y, z \in R$  gilt:
  - (a)  $(x + y) + z = x + (y + z)$ ,
  - (b)  $0 + x = x$ ,
  - (c)  $(-x) + x = 0$ ,
  - (d)  $x + y = y + x$ ,
  - (e)  $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ ,
  - (f)  $1 \cdot x = x \cdot 1 = x$ ,
  - (g)  $x \cdot (y + z) = x \cdot y + x \cdot z$ ,
  - (h)  $(x + y) \cdot z = x \cdot z + y \cdot z$ .

In manchen Büchern fordert man nicht, dass ein Ring ein Einselement  $1$  haben muss; dort schreibt man dann "Ring mit Eins", wenn man die Existenz eines Einselementes fordert.

BEISPIELE 7.2.

- (1) Die reellen Zahlen bilden einen Ring; genauer:  $\langle \mathbb{R}, +, -, 0, \cdot, 1 \rangle$  ist ein Ring.
- (2) Die  $2 \times 2$ -Matrizen bilden einen Ring; genauer:  $\langle \mathbb{R}^{2 \times 2}, +, -, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \cdot, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \rangle$  ist ein Ring.

(3) Die Polynome über  $\mathbb{R}$  bilden einen Ring; genauer:  $\langle \mathbb{R}[x], +, -, 0, \cdot, 1 \rangle$  ist ein Ring.

**SATZ 7.3.** Sei  $\langle R, +, -, 0, \cdot, 1 \rangle$  ein Ring. Dann gelten für alle  $x, y \in R$  folgende Eigenschaften:

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

**DEFINITION 7.4.** Sei  $\mathbf{R} = \langle R, +, -, 0, \cdot, 1 \rangle$  ein Ring. Ein Element  $a \in R$  heißt *invertierbar*, wenn es ein  $b \in R$  gibt, sodass  $a \cdot b = b \cdot a = 1$ .

**DEFINITION 7.5.** Ein Ring  $\mathbf{R} = \langle R, +, -, 0, \cdot, 1 \rangle$  ist *kommutativ*, wenn für alle  $r, s \in R$  gilt:  $r \cdot s = s \cdot r$ .

## 2. Der Ring $\mathbb{Z}_n$

In  $\mathbb{Z}$  definieren wir für  $n \in \mathbb{N}$  die Relation  $\equiv_n$  durch

$$a \equiv_n b \Leftrightarrow n \mid b - a.$$

Die Relation  $\equiv_n$  ist eine Äquivalenzrelation, d.h. reflexiv, symmetrisch und transitiv. Die Äquivalenzklasse von  $a \in \mathbb{Z}$  ist

$$\{a + z \cdot n \mid z \in \mathbb{Z}\} =: [a]_n.$$

Die Menge aller Äquivalenzklassen (die Faktormenge) bezeichnen wir mit

$$\mathbb{Z}_n := \{[a]_n \mid a \in \mathbb{Z}\}.$$

$\mathbb{Z}_n$  hat  $n$  Elemente, und zwar  $[0]_n, [1]_n, \dots, [n-1]_n$ . Auf  $\mathbb{Z}_n$  definieren wir  $\oplus$  und  $\odot$  durch:

$$\begin{aligned} [a]_n \oplus [b]_n &:= [a + b]_n \\ [a]_n \odot [b]_n &:= [a \cdot b]_n. \end{aligned}$$

Wir müssen zeigen, dass  $\oplus$  und  $\odot$  wohldefiniert sind; wir geben hier nur den Beweis für die Wohldefiniertheit von  $\odot$ . Wir wählen also  $a, a', b, b' \in \mathbb{Z}$  sodass  $[a]_n = [a']_n$  und  $[b]_n = [b']_n$ . Zu zeigen ist, dass dann

$$[a \cdot b]_n = [a' \cdot b']_n$$

gilt. Es ist also zu zeigen, dass

$$n \mid a \cdot b - a' \cdot b'.$$

Klarerweise ist

$$ab - a'b' = ab - ab' + ab' - a'b' = a(b - b') + (a - a')b'.$$

Da  $n \mid (b - b')$  und  $n \mid (a - a')$ , gilt also  $n \mid ab - a'b'$ . Daher ist  $[a \cdot b]_n = [a' \cdot b']_n$ , und somit ist das Ergebnis von  $[a]_n \odot [b]_n$  unabhängig von der Auswahl der Repräsentanten.

Wir geben nun ein Beispiel für eine *nicht* wohldefinierte Operation. Auf der Menge  $\mathbb{Q}$  definieren wir die Relation

$$a \sim b :\Leftrightarrow [a] = [b].$$

Mit  $[a]$  bezeichnen wir hier die größte ganze Zahl, die kleiner gleich  $a$  ist. Wir definieren:

$$[a] \odot [b] := [a \cdot b].$$

$$\begin{array}{lll} a = 0.1 & b = 100 & [0.1 \cdot 100] = 10 \\ a' = 0 & b' = 100 & [0 \cdot 100] = 0 \end{array}$$

Da  $0 \sim 10$  nicht gilt, ist die Operation  $\odot$  also nicht wohldefiniert.

Die Operation  $\odot$  zuerst zu definieren, und dann zu zeigen, dass die Definition funktioniert, ist nicht sauber (aber üblich). Richtig ist, die Operation  $\odot$  zuerst als Relation zu definieren, also

$$\odot := \{([a]_n, [b]_n), [a \cdot b]_n \mid a, b \in \mathbb{Z}\},$$

und dann zu zeigen, dass die Relation  $\odot$  eine Funktion von  $\mathbb{Z}_n \times \mathbb{Z}_n$  nach  $\mathbb{Z}_n$  ist.

Die algebraische Struktur  $\langle \mathbb{Z}_n, \oplus, \ominus, [0]_n, \odot, [1]_n \rangle$  ist ein Ring.

Eine andere Möglichkeit, einen endlichen Ring mit  $n$  Elementen zu definieren, ist folgende: Wir wählen die Menge  $R = \{0, 1, 2, \dots, n-1\}$ . Wir definieren für alle  $a \in \mathbb{Z}$  die Zahl  $a \bmod n$  als jenes  $a' \in \{0, 1, \dots, n-1\}$  mit  $a' \equiv_n a$ . Die Zahl  $a'$  ist dann genau der Rest der Division von  $a$  durch  $n$ . Dann definieren wir für  $x, y \in \{0, 1, \dots, n-1\}$

$$\begin{aligned} x +_n y &:= (x + y) \bmod n, \\ -_n x &:= (-x) \bmod n, \\ x \circ_n y &:= (xy) \bmod n. \end{aligned}$$

Die algebraische Struktur  $\langle R, +_n, -_n, 0, \circ_n, 1 \rangle$  ist dann ein Ring. "Im wesentlichen", das heißt, bis auf Umbenennung der Elemente, ist dieser Ring der gleiche Ring wie  $\langle \mathbb{Z}_n, \oplus, \ominus, [0]_n, \circ_n, [1]_n \rangle$ .

Der folgende Satz gibt an, welche Elemente in  $\mathbb{Z}_n$  invertierbar sind.

**SATZ 7.6 (Invertierbarkeit).** Sei  $n \in \mathbb{N}$  und  $a \in \mathbb{Z}$ . Dann ist  $[a]_n$  genau dann invertierbar in  $\mathbb{Z}_n$ , wenn  $\text{ggT}(a, n) = 1$ .

**SATZ 7.7.** Seien  $a, b$  invertierbare Elemente aus  $\mathbb{Z}_n$ . Dann ist auch  $a \cdot b$  invertierbar.

*Beweis:* Seien  $u, v \in \mathbb{Z}_n$  so, dass  $a \cdot u = [1]_n$  und  $b \cdot v = [1]_n$ . Dann gilt:  $a \cdot b \cdot v \cdot u = [1]_n$ .

■

DEFINITION 7.8 (Euler'sche  $\varphi$ -Funktion). Sei  $n \in \mathbb{N}$ ,  $n > 1$ . Dann ist  $\varphi(n)$  definiert durch

$$\begin{aligned}\varphi(n) &:= \left| \{a \in \mathbb{Z}_n \mid a \text{ invertierbar} \} \right| = \\ &= \left| \{x \in \{1, 2, \dots, n-1\} \mid \text{ggT}(x, n) = 1\} \right|.\end{aligned}$$

Wir berechnen  $\varphi(12) = |\{1, 5, 7, 11\}| = 4$  und  $\varphi(8) = |\{1, 3, 5, 7\}| = 4$ .

SATZ 7.9 (Satz von Euler). Sei  $n \in \mathbb{N}$ ,  $n > 1$ ,  $a \in \mathbb{Z}$ ,  $\text{ggT}(a, n) = 1$ . Dann gilt:

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Wir überprüfen diesen Satz durch zwei Beispiele:

- Gilt  $7^{\varphi(12)} \equiv 1 \pmod{12}$ ? Ja, denn es ist  $7^4 \equiv 1 \pmod{12}$ ,
- Gilt  $3^{\varphi(5)} \equiv 1 \pmod{5}$ ? Ja, denn es gilt  $3^4 \equiv 1 \pmod{5}$ .

*Beweis von Satz 7.9:* Wir wählen  $n \in \mathbb{N}$  und  $a \in \mathbb{Z}$  und nehmen an, dass  $\text{ggT}(a, n) = 1$ . Sei

$$I := \{x \in \mathbb{Z}_n \mid x \text{ ist invertierbar}\}.$$

Wir wissen bereits, dass  $|I| = \varphi(n)$ . Wir definieren

$$\begin{aligned}f &: I \longrightarrow \mathbb{Z}_n \\ x &\longmapsto x \odot [a]_n\end{aligned}$$

und zeigen, dass  $f$  injektiv ist. Dazu fixieren wir  $x, y \in I$  mit  $f(x) = f(y)$ . Das heißt:  $x \cdot [a]_n = y \cdot [a]_n$ . Da  $\text{ggT}(a, n) = 1$ , gibt es  $b \in \mathbb{Z}$  mit  $[a]_n \cdot [b]_n = [1]_n$ . Wir erhalten also  $x \cdot [a]_n \cdot [b]_n = y \cdot [a]_n \cdot [b]_n$  und damit  $x = y$ . Daher ist  $f$  injektiv. Weil das Produkt invertierbarer Elemente invertierbar ist, wissen wir, dass  $f(I) \subseteq I$  ist. Die Funktion  $f$  ist also eine injektive Abbildung von  $I$  nach  $I$ . Da  $I$  endlich ist, ist  $f$  bijektiv. Es gilt also:

$$\begin{aligned}\prod_{x \in I} x &= \prod_{x \in I} f(x) \\ \prod_{x \in I} x &= \prod_{x \in I} (x \cdot [a]_n) \\ \prod_{x \in I} x &= \left( \prod_{x \in I} x \right) \cdot ([a]_n)^{\varphi(n)}\end{aligned}$$

Sei  $y \in \mathbb{Z}_n$  das Inverse zu  $\prod_{x \in I} x$ . Dann gilt:

$$y \cdot \prod_{x \in I} x = y \cdot \left( \prod_{x \in I} x \right) \cdot ([a]_n)^{\varphi(n)}$$

$$\begin{aligned}[1]_n &= ([a]_n)^{\varphi(n)} \\ 1 &\equiv a^{\varphi(n)} \pmod{n}.\end{aligned}$$



■

KOROLLAR 7.10. Sei  $p$  eine Primzahl, und sei  $z \in \mathbb{Z}$ . Dann gilt

$$z^p \equiv z \pmod{p}.$$

Falls  $p$  kein Teiler von  $z$  ist, gilt

$$z^{p-1} \equiv 1 \pmod{p}.$$

*Beweis:* Wir wählen eine Primzahl  $p$  und  $z \in \mathbb{Z}$  und nehmen an, dass  $p$  die Zahl  $z$  nicht teilt. Wir wissen, dass  $\varphi(p) = p - 1$ , und daher gilt nach dem Satz von Euler

$$z^{p-1} \equiv 1 \pmod{p}.$$

Da  $p|(z^{p-1} - 1)$ , gilt auch  $p|(z^p - z)$ , und somit  $z^p \equiv z \pmod{p}$ .

Wenn  $p | z$ , dann teilt  $p$  sowohl  $z$  als auch  $z^p$ . ■

KOROLLAR 7.11. Für alle  $a, b \in \mathbb{Z}_p$  gilt:  $(a + b)^p = a^p + b^p$ .

Der folgende Satz ist eine Grundlage für das RSA-Verfahren zur Verschlüsselung mit öffentlichem Schlüssel.

SATZ 7.12. Seien  $p, q$  Primzahlen,  $p \neq q$  und seien  $a \in \mathbb{Z}$ ,  $s \in \mathbb{N}_0$ . Dann gilt:

$$a^{1+s(p-1)(q-1)} \equiv a \pmod{p \cdot q}.$$

*Beweis:*

- 1. Fall:  $\text{ggT}(a, pq) = 1$ : Wir wissen ja, dass  $a^{p-1} \equiv 1 \pmod{p}$  gilt (Satz von Euler), daher gilt auch  $(a^{p-1})^{(q-1)s} \equiv 1 \pmod{p}$ . Somit ist  $p$  ein Teiler von  $a^{(p-1)(q-1)s} - 1$  und damit auch von  $a^{(p-1)(q-1)s+1} - a$ . Ebenso zeigen wir

$$q | a^{(p-1)(q-1)s+1} - a.$$

Damit gilt insgesamt:

$$pq | a^{(p-1)(q-1)s+1} - a.$$

- 2. Fall:  $\text{ggT}(a, pq) = p$ : Da der  $\text{ggT}(a, q) = 1$  ist, gilt mit dem Satz von Euler  $a^{q-1} \equiv 1 \pmod{q}$ , und somit  $a^{(q-1)(p-1)} \equiv 1 \pmod{q}$ . Das heißt

$$q | a^{(q-1)(p-1)s} - 1.$$

Wir wissen ja, dass  $p | a$ . Daher gilt  $p \cdot q | (a^{(q-1)(p-1)s} - 1) \cdot a$ .

- 3. Fall:  $\text{ggT}(a, pq) = q$ : Beweis genauso wie im 2. Fall.
- 4. Fall:  $\text{ggT}(a, pq) = p \cdot q$ : Dann ist zu zeigen, dass  $0 \equiv 0 \pmod{pq}$ . ■

### 3. Das RSA-Verschlüsselungsverfahren

RSA ist ein asymmetrisches Verschlüsselungsverfahren. Wenn ein Teilnehmer, Alice, einem zweiten Teilnehmer, Bob, eine verschlüsselte Nachricht übermitteln will, dann beschafft sich Alice zunächst den öffentlichen Schlüssel von Bob. Alice verschlüsselt dann die Nachricht mit Bobs öffentlichem Schlüssel und schickt sie an Bob. Bob kann die empfangene Nachricht mit seinem privaten (geheimen) Schlüssel entschlüsseln. Wichtig dabei ist, dass es praktisch unmöglich ist, Bobs privaten Schlüssel aus seinem öffentlichen Schlüssel zu rekonstruieren.

#### Schlüsselerzeugung für das RSA-Verfahren:

- (1) Bob wählt Primzahlen  $p, q$ . Sei  $n := pq$ . (In der Praxis soll die Binärdarstellung von  $n$  mindestens 1024 Bits haben.)
- (2) Bob wählt  $e \in \mathbb{N}$  mit  $1 < e < (p-1)(q-1)$ , sodass  $\text{ggT}(e, (p-1)(q-1)) = 1$ .
- (3) Mit dem Euklidischem Algorithmus bestimmt Bob  $d \in \mathbb{N}$ , sodass  $ed \equiv 1 \pmod{(p-1)(q-1)}$ .
- (4) Bobs öffentlicher Schlüssel lautet  $(n, e)$ .
- (5) Bobs privater Schlüssel lautet  $(n, d)$ .

#### RSA Verschlüsselung:

- (1) Alice holt sich Bobs öffentlichen Schlüssel  $(n, e)$ .
- (2) Um eine Nachricht  $m \in \{0, \dots, n-1\}$  zu verschlüsseln, berechnet Alice  $c := m^e \pmod n$  und schickt  $c$  an Bob.

#### RSA Entschlüsselung:

- (1) Bob erhält eine mit seinem öffentlichen Schlüssel  $(n, e)$  verschlüsselte Nachricht  $c \in \{0, \dots, n-1\}$ .
- (2) Um  $c$  zu entschlüsseln, berechnet Bob  $m = c^d \pmod n$  mit seinem privaten Schlüssel  $(n, d)$ .

Die Entschlüsselung ist korrekt, weil nach Satz 7.12 gilt, dass  $m^{ed} \equiv m \pmod n$  für alle  $m \in \{0, \dots, n-1\}$ .

Für große Primzahlen ist kein effizientes Verfahren bekannt ist, um aus dem öffentlichen Schlüssel  $(n, e)$  die Zahl  $(p-1)(q-1)$  und damit  $d$  zu berechnen.

### 4. Die Multiplikatitivität der Eulerschen $\varphi$ -Funktion

**SATZ 7.13** (Multiplikatitivität der  $\varphi$ -Funktion). *Seien  $n, m \in \mathbb{N}$ ,  $n \geq 2$ ,  $m \geq 2$ . Wenn  $n, m$  relativ prim sind, dann gilt*

$$\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m).$$

Der Beweis der Multiplikatitivität erfordert noch etwas Information über Ringe.

SATZ 7.14. Falls  $R_1$  und  $R_2$  Ringe sind, dann ist

$$\langle R_1 \times R_2, +_{R_1 \times R_2}, -_{R_1 \times R_2}, 0_{R_1 \times R_2}, \cdot_{R_1 \times R_2}, 1_{R_1 \times R_2} \rangle$$

wieder ein Ring. Dabei sind die Verknüpfungen auf  $R_1 \times R_2$  definiert durch

$$\begin{aligned} & \bullet \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} +_{R_1 \times R_2} \begin{pmatrix} s_1 \\ s_2 \end{pmatrix} := \begin{pmatrix} r_1 +_{R_1} s_1 \\ r_2 +_{R_2} s_2 \end{pmatrix} \\ & \bullet \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} \cdot_{R_1 \times R_2} \begin{pmatrix} s_1 \\ s_2 \end{pmatrix} := \begin{pmatrix} r_1 \cdot_{R_1} s_1 \\ r_2 \cdot_{R_2} s_2 \end{pmatrix} \\ & \bullet -_{R_1 \times R_2} \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} := \begin{pmatrix} -_{R_1} r_1 \\ -_{R_2} r_2 \end{pmatrix} \\ & \bullet 0_{R_1 \times R_2} := \begin{pmatrix} 0_{R_1} \\ 0_{R_2} \end{pmatrix} \\ & \bullet 1_{R_1 \times R_2} := \begin{pmatrix} 1_{R_1} \\ 1_{R_2} \end{pmatrix}. \end{aligned}$$

$R_1 \times R_2$  mit diesen Operationen ist dann wieder ein Ring.

Rechnen wir zum Beispiel in  $\mathbb{Z}_4 \times \mathbb{Z}_5$ .

$$\begin{pmatrix} [3]_4 \\ [4]_5 \end{pmatrix} \cdot \begin{pmatrix} [2]_4 \\ [3]_5 \end{pmatrix} = \begin{pmatrix} [2]_4 \\ [2]_5 \end{pmatrix}$$

$R_1 \times R_2$  heißt das *direkte Produkt* von  $R_1$  und  $R_2$ .

DEFINITION 7.15.  $R, S$  seien Ringe. Die Abbildung  $\varphi : R \rightarrow S$  heißt genau dann *Ring-Homomorphismus*, wenn für alle  $r_1, r_2 \in R$  gilt:

$$\begin{aligned} \varphi(r_1 +_R r_2) &= \varphi(r_1) +_S \varphi(r_2), \\ \varphi(-_R r_1) &= -_S \varphi(r_1), \\ \varphi(r_1 \cdot_R r_2) &= \varphi(r_1) \cdot_S \varphi(r_2), \\ \varphi(0_R) &= 0_S, \\ \varphi(1_R) &= 1_S. \end{aligned}$$

DEFINITION 7.16. Ein Homomorphismus  $\varphi$  heißt:

- *Epimorphismus* :  $\Leftrightarrow \varphi$  ist surjektiv;
- *Monomorphismus* :  $\Leftrightarrow \varphi$  ist injektiv;
- *Isomorphismus* :  $\Leftrightarrow \varphi$  ist bijektiv.

*Beispiel:* Wollen wir uns dies zunächst an zwei Beispielen veranschaulichen.

- $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}_5, z \mapsto [z]_5$  ist surjektiv, aber nicht injektiv. Also ist  $\varphi$  ein Epimorphismus.

- Wir untersuchen  $\alpha : \mathbb{Z}_5 \rightarrow \mathbb{Z}$ ,  $[x]_5 \mapsto x$ . Hier ergibt sich folgendes Problem:  $\alpha([3]_5) = 3$ , und  $\alpha([3]_5) = \alpha([8]_5) = 8$ . — Das Problem ist, dass  $\alpha$  nicht wohldefiniert ist. Man kann das auch so ausdrücken, dass man sagt, dass die Relation

$$\alpha = \{([x]_5, x) \mid x \in \mathbb{Z}\}$$

nicht funktional (d. h. eine Funktion = Graph einer Funktion) ist. Sie ist nicht funktional, weil  $([2]_5, 2) \in \alpha$  und  $([2]_5, 7) \in \alpha$ .

SATZ 7.17. Seien  $n, m \in \mathbb{N}$  mit  $\text{ggT}(n, m) = 1$ . Dann ist die Abbildung

$$\begin{aligned} \varphi : \mathbb{Z}_{m \cdot n} &\longrightarrow \mathbb{Z}_n \times \mathbb{Z}_m \\ [x]_{m \cdot n} &\longmapsto ([x]_n, [x]_m) \end{aligned}$$

ein Ring-Isomorphismus.

*Beweis:* Wir führen den Beweis in drei Schritten.

- (1)  $\varphi$  ist wohldefiniert: Zu zeigen ist, dass für alle  $y, z \in \mathbb{Z}$  mit  $[y]_{m \cdot n} = [z]_{m \cdot n}$  die Gleichheiten  $[y]_n = [z]_n$  und  $[y]_m = [z]_m$  gelten. Zu zeigen ist also, dass für alle  $y, z \in \mathbb{Z}$  gilt:

$$m \cdot n \mid y - z \Rightarrow (m \mid y - z \wedge n \mid y - z).$$

Das ist aber offensichtlich.

- (2)  $\varphi$  ist Homomorphismus: Wir überprüfen die Homomorphismeigenschaft für  $+$ . Wir berechnen dazu

$$\begin{aligned} \varphi([x]_{n \cdot m} + [y]_{n \cdot m}) &= \varphi([x + y]_{n \cdot m}) \\ &= ([x + y]_n, [x + y]_m) \\ &= ([x]_n + [y]_n, [x]_m + [y]_m) \\ &= \begin{pmatrix} [x]_n \\ [x]_m \end{pmatrix} + \begin{pmatrix} [y]_n \\ [y]_m \end{pmatrix} \\ &= \varphi([x]_{n \cdot m}) + \varphi([y]_{n \cdot m}). \end{aligned}$$

- (3)  $\varphi$  ist bijektiv: Da beide Mengen endlich und gleich groß sind, reicht es, zu zeigen, dass  $\varphi$  injektiv ist. Wir nehmen also an  $\varphi([x]_{nm}) = \varphi([y]_{nm})$ . Das heißt  $([x]_n, [x]_m) = ([y]_n, [y]_m)$ . Daher gilt  $n \mid x - y$  und  $m \mid x - y$ . Da der  $\text{ggT}(n, m) = 1$  ist, gilt:  $n \cdot m \mid x - y$ . Wir erhalten daher  $[x]_{nm} = [y]_{nm}$ . Die Abbildung  $\varphi$  ist also injektiv, somit surjektiv und damit bijektiv. ■

Wenn der  $\text{ggT}(n, m) = 1$  ist, dann ist  $\mathbb{Z}_n \times \mathbb{Z}_m$  also isomorph zu  $\mathbb{Z}_{n \cdot m}$ . Da Isomorphismen die Invertierbarkeit erhalten, haben beide Ringe gleich viele invertierbare Elemente. Daraus können wir jetzt die Multiplikativität der  $\varphi$ -Funktion, also Satz 7.13, herleiten.

*Beweis von Satz 7.13:*

- (1) Anzahl der invertierbaren Elemente von  $\mathbb{Z}_n \times \mathbb{Z}_m$ : Wir zeigen, dass  $\begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{Z}_n \times \mathbb{Z}_m$  genau dann invertierbar ist, wenn  $a$  invertierbar in  $\mathbb{Z}_n$  und  $b$  invertierbar in  $\mathbb{Z}_m$  ist. Dazu fixieren wir zunächst  $\begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{Z}_n \times \mathbb{Z}_m$  und nehmen an, dass  $\begin{pmatrix} a \\ b \end{pmatrix}$  invertierbar ist; es gibt also  $\begin{pmatrix} c \\ d \end{pmatrix} \in \mathbb{Z}_n \times \mathbb{Z}_m$ , sodass  $\begin{pmatrix} a \\ b \end{pmatrix} \cdot \begin{pmatrix} c \\ d \end{pmatrix} = 1_{\mathbb{Z}_n \times \mathbb{Z}_m} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ . Daher ist  $a$  in  $\mathbb{Z}_n$  invertierbar (mit Inversem  $c$ ), ebenso  $b$  in  $\mathbb{Z}_m$  (mit Inversem  $d$ ).

Nun fixieren wir  $a \in \mathbb{Z}_n$ ,  $b \in \mathbb{Z}_m$ , beide invertierbar. Falls  $a \cdot c = [1]_n$ , und  $b \cdot d = [1]_m$ , dann ist  $\begin{pmatrix} c \\ d \end{pmatrix}$  das Inverse zu  $\begin{pmatrix} a \\ b \end{pmatrix}$ . In  $\mathbb{Z}_n$  gibt es  $\varphi(n)$  invertierbare Elemente, in  $\mathbb{Z}_m$  gibt es  $\varphi(m)$  invertierbare Elemente, und somit gibt es in  $\mathbb{Z}_n \times \mathbb{Z}_m$  genau  $\varphi(n) \cdot \varphi(m)$  invertierbare Elemente.

- (2) Anzahl der invertierbaren Elemente in  $\mathbb{Z}_{n \cdot m}$ : Hier gibt es  $\varphi(n \cdot m)$  invertierbare Elemente (nach der Definition von  $\varphi$ ).

Damit ist

$$\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$$

für  $n, m \in \mathbb{N}$  mit  $\text{ggT}(n, m) = 1$  bewiesen. ■

Aus der Primfaktorzerlegung von  $n$  und aus  $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$  kann man jetzt leicht  $\varphi(n)$  durch

$$\begin{aligned} \varphi(n) &= \varphi\left(\prod p_i^{\alpha_i}\right) \\ &= \prod \varphi\left(p_i^{\alpha_i}\right) \\ &= \prod p_i^{\alpha_i} \left(1 - \frac{1}{p_i}\right) \\ &= \prod p_i^{\alpha_i} \cdot \prod \left(1 - \frac{1}{p_i}\right) \\ &= n \cdot \prod \left(1 - \frac{1}{p_i}\right) \end{aligned}$$

berechnen. Dazu noch ein Beispiel:

$$\text{Beispiel: } \varphi(12) = 12 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) = 4 = 2 \cdot 2 = \varphi(3) \cdot \varphi(4).$$

## 5. Körper

DEFINITION 7.18. Sei  $\mathbf{R} = \langle R, +, -, 0, \cdot, 1 \rangle$  ein Ring.  $\mathbf{R}$  ist ein *Körper*, wenn folgendes gilt:

- (1)  $|R| \geq 2$ ,
- (2) für alle  $x, y \in R$ :  $x \cdot y = y \cdot x$ ,
- (3) für alle  $x \in R$  mit  $x \neq 0$  gibt es ein  $y \in R$ , sodass  $x \cdot y = 1$ .

ÜBUNGSAUFGABEN 7.19.

- (1) Zeigen Sie, dass es in einem Körper für jedes  $x$  höchstens ein  $y$  mit  $x \cdot y = 1$  geben kann.
- (2) Zeigen Sie, dass das Produkt zweier Elemente in einem Körper nur dann 0 ist, wenn einer der Faktoren gleich 0 ist.

In einem Körper hat jedes Element  $a \neq 0$  genau ein multiplikativ inverses Element; wir bezeichnen es mit  $a^{-1}$ .

**SATZ 7.20.** Sei  $n \in \mathbb{N}$ . Der Ring  $\mathbb{Z}_n$  ist genau dann ein Körper, wenn  $n$  eine Primzahl ist.

**Beweis:** Wir nehmen an  $n$  ist eine Primzahl. Um zu zeigen, dass  $\mathbb{Z}_n$  ein Körper ist, zeigen wir, dass jedes  $x \in \mathbb{Z}_n$  mit  $x \neq [0]_n$  invertierbar ist. Sei  $a \in \mathbb{Z}$  so, dass  $x = [a]_n$ . Da  $x \neq [0]_n$ , ist  $a$  kein Vielfaches von  $n$ . Da  $n$  eine Primzahl ist, gilt also  $\text{ggT}(a, n) = 1$ . Es gibt also  $u, v \in \mathbb{Z}$  sodass  $ua + vn = 1$ . Dann gilt  $[u]_n \cdot [a]_n = [1]_n$ . Somit ist  $[a]_n$  invertierbar mit Inversem  $[u]_n$ . Also ist  $\mathbb{Z}_n$  ein Körper.

Sei nun  $n$  so, dass  $\mathbb{Z}_n$  ein Körper ist. Da ein Körper zumindest zwei Elemente haben muss, gilt  $n \geq 2$ . Wir nehmen an,  $n$  ist keine Primzahl. Dann gibt es  $a, b \in \mathbb{N}$  mit  $a < n$ ,  $b < n$  und  $ab = n$ . Da  $\mathbb{Z}_n$  ein Körper ist, ist  $[a]_n$  invertierbar, und es gibt damit ein  $u \in \mathbb{Z}$ , sodass  $[u]_n \cdot [a]_n = [1]_n$ . Dann gilt  $[u]_n \cdot [a]_n \cdot [b]_n = [b]_n$ , also  $[0]_n = [b]_n$ , im Widerspruch zu  $b < n$ . ■

Also ist der zweielementige Ring  $\mathbb{Z}_2$  ein Körper. Wir schreiben  $\mathbf{0} := [0]_2$ ,  $\mathbf{1} := [1]_2$ . Dann gilt  $\mathbf{0} \oplus \mathbf{0} = \mathbf{0}$ ,  $\mathbf{0} \oplus \mathbf{1} = \mathbf{1}$ ,  $\mathbf{1} \oplus \mathbf{0} = \mathbf{1}$ ,  $\mathbf{1} \oplus \mathbf{1} = \mathbf{0}$ ,  $\mathbf{0} \odot \mathbf{0} = \mathbf{0}$ ,  $\mathbf{0} \odot \mathbf{1} = \mathbf{0}$ ,  $\mathbf{1} \odot \mathbf{0} = \mathbf{0}$ ,  $\mathbf{1} \odot \mathbf{1} = \mathbf{1}$ .

## 6. Vektorräume

**DEFINITION 7.21.** Sei  $K$  ein Körper. Ein Tupel  $\langle V, +, -, \mathbf{0}, * \rangle$  heißt *Vektorraum* über  $K$ , wenn  $+$  :  $V \times V \rightarrow V$ ,  $-$  :  $V \rightarrow V$ ,  $\mathbf{0} \in V$  und  $*$  :  $K \times V \rightarrow V$ , und für alle  $x, y, z \in V$  und  $\alpha, \beta \in K$  gilt:

- (1)  $(x + y) + z = x + (y + z)$ ,
- (2)  $\mathbf{0} + x = x$ ,
- (3)  $(-x) + x = \mathbf{0}$ ,
- (4)  $x + y = y + x$ ,
- (5)  $\alpha * (\beta * x) = (\alpha \cdot \beta) * x$ ,
- (6)  $(\alpha + \beta) * x = \alpha * x + \beta * x$ ,
- (7)  $\alpha * (x + y) = \alpha * x + \alpha * y$ ,
- (8)  $1 * x = x$ .

**BEISPIELE 7.22.**

- (1) Für jeden Körper  $K$  und jedes  $n \in \mathbb{N}$  ist  $K^n$  (mit geeignet definierten Operationen) ein Vektorraum über  $K$ .
- (2) Für jeden Unterraum  $U$  des  $\mathbb{R}^n$  ist  $U$  (mit geeignet definierten Operationen) ein Vektorraum über  $\mathbb{R}$ .

**DEFINITION 7.23.** Sei  $K$  ein Körper und  $V$  ein Vektorraum über  $K$ . Sei  $U$  eine Teilmenge von  $V$ .  $U$  ist ein *Unterraum* von  $V$ , wenn  $U \neq \emptyset$ , und für alle  $u, v \in U$  und  $\alpha \in K$  gilt  $u + v \in U$  und  $\alpha * u \in U$ .

Wenn  $U$  ein Unterraum von  $V = \langle V, +, -, 0, * \rangle$  ist, dann ist  $U = \langle U, +|_{U \times U}, -|_U, 0, *|_{K \times U} \rangle$  ebenfalls ein Vektorraum über  $K$ .





## KAPITEL 8

# Polynome und endliche Körper

### 1. Polynome

DEFINITIONSVERSUCH 8.1. Sei  $K$  kommutativer Ring. Dann ist  $K[x]$  die Menge aller Ausdrücke

$$a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots + a_nx^n$$

mit  $n \in \mathbb{N}_0$  und  $a_0, a_1, \dots, a_n \in K$ . Die Elemente von  $K[x]$  nennen wir *Polynome*.

Was heißt aber *Ausdruck*? Und welche Rolle spielt  $x$ ? Mit folgender Definition stehen wir auf dem sicheren Boden der Mengenlehre.

DEFINITION 8.2. Sei  $K$  kommutativer Ring. Dann ist  $K[x]$  die Menge aller Folgen  $(a_0, a_1, a_2, a_3, \dots)$ , sodass es ein  $i \in \mathbb{N}$  gibt, sodass für alle  $j \in \mathbb{N}$  mit  $j \geq i$  gilt:  $a_j = 0$ .

Wir haben also Polynome als unendliche Liste ihrer Koeffizienten definiert.

DEFINITION 8.3. Sei  $K$  ein kommutativer Ring, und seien  $(a_0, a_1, a_2, \dots)$ ,  $(b_0, b_1, b_2, \dots) \in K[x]$ . Wir definieren

- (1)  $(a_0, a_1, a_2, \dots) + (b_0, b_1, b_2, \dots) := (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots)$
- (2)  $(a_0, a_1, a_2, \dots) \cdot (b_0, b_1, b_2, \dots) := (c_0, c_1, c_2, \dots)$  mit

$$c_k := \sum_{\substack{(i,j) \in \{0, \dots, k\} \times \{0, \dots, k\} \\ i+j=k}} a_i \cdot b_j$$

für alle  $k \in \mathbb{N}_0$ .

DEFINITION 8.4. Für  $f := (a_0, a_1, a_2, \dots) \in K[x] \setminus \{0\}$  ist der *Grad* von  $f$ ,  $\deg f$ , jenes  $n \in \mathbb{N}$ , sodass  $a_n \neq 0$  und  $a_i = 0$  für alle  $i > n$ . Dann nennen wir  $a_n$  den *führenden Koeffizienten* von  $f$ . Wir definieren  $\deg 0 := -1$ .

DEFINITION 8.5. Sei  $K$  Körper, und seien  $f, g \in K[x]$ .

- (1)  $f$  *teilt*  $g$ , wenn es  $q \in K[x]$  gibt, sodass  $g = q \cdot f$ .
- (2)  $f$  ist *irreduzibel über  $K$*  (ein irreduzibles Polynom in  $K[x]$ ), wenn  $\deg f \geq 1$  und für alle  $a, b \in K[x]$  mit  $a \cdot b = f$  entweder  $a$  oder  $b$  Grad 0 hat.
- (3)  $f$  ist *normiert*, wenn es führenden Koeffizienten 1 hat.

## 2. Teilbarkeit von Polynomen

**SATZ 8.6.** Sei  $K$  Körper, und seien  $f, g \in K[x]$ . Wenn  $f \neq 0$ , so gibt es  $q, r \in K[x]$  mit  $g = q \cdot f + r$  und  $\deg r < \deg f$ .

**DEFINITION 8.7** (ggT in  $K[x]$ ). Sei  $K$  ein Körper, und seien  $f, g \in K[x]$ , nicht beide 0. Dann ist  $d \in K[x]$  ein *größter gemeinsamer Teiler* von  $f$  und  $g$ , wenn folgende Bedingungen gelten:

- (1)  $d|f$  und  $d|g$ ,
- (2) Für alle  $h \in K[x]$  mit  $h|f$  und  $h|g$  gilt  $\deg(h) \leq \deg(d)$ ,
- (3)  $d$  ist normiert.

Wir bezeichnen den Rest von  $g$  bei der Division durch  $f$  mit  $g \bmod f$ . Da das Paar  $(g, f)$  die gleichen gemeinsamen Teiler wie das Paar  $(f, g \bmod f)$  hat, können wir einen größten gemeinsamen Teiler mithilfe des Euklidischen Algorithmus berechnen.

Wir rechnen dazu drei Beispiele:

**AUFGABE 8.8.** Wir berechnen einen größten gemeinsamen Teiler von  $f, g \in \mathbb{R}[x]$  für

$$f = -8x + 4x^2 + 6x^3 - 5x^4 + x^5$$

und

$$g = 4 - 4x - x^2 + x^3.$$

Wir bilden die gleiche Tabelle wie beim Euklidischen Algorithmus für ganze Zahlen und erhalten:

$-8x + 4x^2 + 6x^3 - 5x^4 + x^5$	1	0
$4 - 4x - x^2 + x^3$	0	1
$-24 + 32x - 10x^2$	1	$-6 + 4x - x^2$
$-\left(\frac{32}{25}\right) + \frac{16x}{25}$	$\frac{11}{50} + \frac{x}{10}$	$-\left(\frac{8}{25}\right) + \frac{7x}{25} + \frac{9x^2}{50} - \frac{x^3}{10}$
0		

Um einen normierten gemeinsamen Teiler zu erhalten, multiplizieren wir die vorletzte Zeile dieser Tabelle mit  $\frac{25}{16}$  und erhalten  $-2 + x$  als einen größten gemeinsamen Teiler. Außerdem gilt

$$-2 + x = \left(\frac{11}{32} + \frac{5x}{32}\right) \cdot f + \left(-\left(\frac{1}{2}\right) + \frac{7x}{16} + \frac{9x^2}{32} - \frac{5x^3}{32}\right) \cdot g.$$

**AUFGABE 8.9.** Wir berechnen den größten gemeinsamen Teiler der Polynome

$$f = 1 + x^3 + x^5$$

und

$$g = 1 + x + x^3$$

in  $\mathbb{Z}_2[x]$ . Wir erhalten

$$\begin{array}{r} 1 + x^3 + x^5 \quad 1 \quad 0 \\ 1 + x + x^3 \quad 0 \quad 1 \\ 1 + x^2 \quad 1 \quad x^2 \\ 1 \quad x \quad 1 + x^3 \\ 0 \end{array}$$

Daher ist 1 ein größter gemeinsamer Teiler, und es gilt

$$1 = x \cdot f + (1 + x^3) \cdot g.$$

AUFGABE 8.10. Wir berechnen den größten gemeinsamen Teiler der Polynome

$$f = 1 + x^3 + x^5$$

und

$$g = 1 + x + x^3$$

in  $\mathbb{Z}_3[x]$ . Wir erhalten

$$\begin{array}{r} 1 + x^3 + x^5 \quad 1 \quad 0 \\ 1 + x + x^3 \quad 0 \quad 1 \\ 1 + 2x^2 \quad 1 \quad 2x^2 \\ 1 + 2x \quad x \quad 1 + 2x^3 \\ 0 \end{array}$$

Daher ist  $2 \cdot (1 + 2x) = 2 + x$  ein größter gemeinsamer Teiler, und es gilt

$$2 + x = 2x \cdot f + (2 + x^3) \cdot g.$$

Wir können also einen größten gemeinsamen Teiler mithilfe des Euklidischen Algorithmus bestimmen. Daraus ergibt sich:

**SATZ 8.11.** Sei  $\mathbf{K}$  ein Körper, und seien  $f, g \in K[x]$ , nicht beide 0. Dann gibt es einen größten gemeinsamen Teiler  $d$  von  $f$  und  $g$ , für den es  $u, v \in K[x]$  gibt, sodass  $u \cdot f + v \cdot g = d$ .

**SATZ 8.12.** Sei  $\mathbf{K}$  ein Körper, und seien  $f, g \in K[x]$ , nicht beide 0, und sei  $d \in K[x]$ . Wir nehmen an, dass es  $u, v \in K[x]$  gibt, sodass  $d = u \cdot f + v \cdot g$ . Dann teilt jeder gemeinsame Teiler von  $f$  und  $g$  auch das Polynom  $d$ .

*Beweis:* Sei  $h$  ein gemeinsamer Teiler von  $f$  und  $g$ . Dann gilt  $h|uf + vg$ , also  $h|d$ . ■

**KOROLLAR 8.13.** Sei  $\mathbf{K}$  ein Körper, und seien  $f, g \in K[x]$ , nicht beide 0. Seien  $d_1, d_2 \in K[x]$  beide ggT von  $f$  und  $g$ . Dann gilt  $d_1 = d_2$ .

*Beweis:* Nach Satz 8.11 gibt es einen größten gemeinsamen Teiler  $d$  von  $f$  und  $g$ , der sich als  $uf + vg$  mit  $u, v \in K[x]$  schreiben lässt. Wegen Satz 8.12 gilt  $d_1|d$ . Sowohl  $d_1$  als auch  $d$  haben den maximal möglichen Grad unter allen gemeinsamen Teilern von  $f$  und  $g$ . Also gilt  $\deg(d_1) = \deg(d)$ . Somit gibt es ein  $\alpha \in K$ , sodass  $d = \alpha d_1$ . Da  $d$  und  $d_1$  normiert sind, gilt  $\alpha = 1$  und somit  $d = d_1$ . Ebenso gilt  $d = d_2$ , also  $d_1 = d_2$ . ■

### 3. Polynomfunktionen und Nullstellen

DEFINITION 8.14. Sei  $K$  ein Körper, und sei  $f \in K[x]$ . Seien  $n \in \mathbb{N}$  und  $a_0, a_1, \dots, a_n \in K$  so, dass

$$f = a_0 + a_1x + a_2x^2 + \dots + a_nx^n.$$

Dann ist  $\bar{f}$  die Funktion, die durch

$$\begin{aligned} \bar{f} : K &\longrightarrow K \\ k &\longmapsto a_0 + a_1k + a_2k^2 + \dots + a_nk^n \end{aligned}$$

definiert ist. Sie heißt *die von  $f$  induzierte Polynomfunktion*.

DEFINITION 8.15. Sei  $K$  ein Körper, sei  $f \in K[x]$ , und sei  $\alpha \in K$ . Die Zahl  $\alpha$  ist eine *Nullstelle* von  $f$ , wenn  $\bar{f}(\alpha) = 0$ .

SATZ 8.16. Sei  $K$  ein Körper, sei  $f \in K[x]$ , und sei  $\alpha \in K$ . Dann ist  $\alpha$  genau dann eine Nullstelle von  $f$ , wenn  $x - \alpha \mid f$  gilt.

SATZ 8.17. Sei  $K$  ein Körper, sei  $n \in \mathbb{N}$ , und sei  $f \in K[x]$  ein Polynom mit  $\deg(f) = n$ . Dann hat  $f$  höchstens  $n$  Nullstellen.

*Beweis:* Die Aussage stimmt für  $n = 1$ : ein Polynom der Form  $\alpha_1x + \alpha_2$  hat, wenn  $\alpha_1 \neq 0$ , nur die Nullstelle  $-\alpha_2 \cdot (\alpha_1)^{-1}$ .

Wir nehmen nun an, dass  $n \geq 1$  ist, und dass jedes Polynom vom Grad  $n$  höchstens  $n$  Nullstellen hat. Wir zeigen, dass dann jedes Polynom vom Grad  $n + 1$  höchstens  $n + 1$  Nullstellen haben kann. Sei dazu  $f$  ein Polynom vom Grad  $n + 1$ . Wenn  $f$  keine Nullstellen hat, dann sind wir fertig, denn "keine Nullstellen" heißt natürlich auch "weniger als  $n + 2$  Nullstellen". Wenn  $f$  zumindest eine Nullstelle hat, dann wählen wir eine Nullstelle  $\alpha$ . Wir können dann ein Polynom  $g$  vom Grad  $n$  finden, sodass

$$f = (x - \alpha) \cdot g.$$

Sei nun  $\beta$  eine Nullstelle von  $f$  mit  $\beta \neq \alpha$ . Dann gilt  $\bar{f}(\beta) = (\beta - \alpha) \cdot \bar{g}(\beta)$ . Also gilt  $0 = (\beta - \alpha) \cdot \bar{g}(\beta)$ . Wegen  $\beta - \alpha \neq 0$  gilt  $\bar{g}(\beta) = 0$ . Das Element  $\beta$  ist daher eine Nullstelle von  $g$ .

Da wir angenommen haben, dass jedes Polynom vom Grad  $n$  höchstens  $n$  Nullstellen hat, hat  $g$  höchstens  $n$  Nullstellen. Jede Nullstelle von  $f$  ist entweder gleich  $\alpha$  oder unter diesen  $n$  Nullstellen von  $g$ . Somit hat  $f$  höchstens  $n + 1$  Nullstellen. ■

### 4. Körper aus Polynomringen

Sei  $f$  ein Polynom in  $K[x]$ . Für  $a, b \in K[x]$  definieren wir

$$a \equiv b \pmod{f},$$

falls  $f \mid a - b$ . Das ist genau dann der Fall, wenn  $a \bmod f = b \bmod f$ . Wir definieren

$$[a]_f := \{a + q \cdot f \mid q \in K[x]\}.$$

Jede Restklasse modulo  $f$  enthält genau ein Polynom, dessen Grad kleiner als  $\deg(f)$  ist.

**SATZ 8.18.** Sei  $K$  ein Körper, sei  $f \in K[x]$  mit  $\deg(f) \geq 1$ , und sei  $a \in K[x]$ . Dann gibt es genau ein  $b \in K[x]$ , sodass  $\deg(b) < \deg(f)$  und  $[a]_f = [b]_f$ .

*Beweis:* Wir zeigen als erstes, dass es so ein  $b$  gibt: Durch Division erhalten wir  $q$  und  $r$  in  $K[x]$ , sodass

$$a = q \cdot f + r \text{ und } \deg(r) < \deg(f).$$

Wir setzen  $b := r$ . Es gilt  $[a]_f = [a - q \cdot f]_f = [r]_f = [b]_f$ . Nun zeigen wir, dass es höchstens ein solches  $b$  geben kann. Seien  $b_1, b_2 \in K[x]$  so, dass  $[b_1]_f = [b_2]_f$  und  $\deg(b_1) < \deg(f)$ ,  $\deg(b_2) < \deg(f)$ . Dann gilt  $f | b_2 - b_1$ . Da  $b_2 - b_1$  kleineren Grad als  $f$  hat, gilt  $b_2 - b_1 = 0$ . ■

Wir kürzen den Rest  $r$  der Division von  $a$  durch  $f$  mit

$$a \bmod f$$

ab. Es gilt also  $a \equiv b \pmod{f}$  genau dann, wenn  $a \bmod f = b \bmod f$ .

Wenn  $f$  ein Polynom in  $\mathbb{Z}_p[x]$  vom Grad  $n$  ist, gibt es genau  $p^n$  Restklassen modulo  $f$ . Um zu bestimmen, ob zwei Polynome zur gleichen Restklasse modulo  $f$  gehören, kann man ihren Rest bei der Division durch  $f$  bestimmen. Die folgende Mathematica-Funktionen berechnen Quotient und Rest einer Division in  $\mathbb{Z}_p[x]$ .

```
Deg [f_, var_] := Length [ CoefficientList [ f, var ] ] - 1;
(* Berechnet den Grad des Polynoms f in der Variablen var *)
```

```
Lcf [f_, var_] := CoefficientList [f, var] [[Deg[f,var] + 1]];
(* Liefert den fuhrenden Koeffizienten von f
in der Variablen var *)
```

```
PolynomialQuotientP [f_,g_,var_,p_] :=
(* Liefert das q, sodass es r mit deg r < deg g gibt, sodass
f = q*g + r. Alle Rechnungen in Z_p [x]. *)
Module[{lf, lg, f1, g1,q},
f1 = PolynomialMod[f,p];
g1 = PolynomialMod[g,p];
If [Deg[g1, var] > Deg[f1, var],
0,
lf = Lcf [f1, var];
lg = Lcf [g1, var];
q = lf * PowerMod[lg, -1, p] * var^(Deg[f1,var]-Deg[g1,var]);
(* compute return value *)
q + PolynomialQuotientP [
PolynomialMod [f1 - q * g1, p],
```

```

    g1,
    var,
    p]
]];
```

```

PolynomialRemainderP [f_,g_,var_,p_] :=
(* Liefert den Rest bei der Division von f durch g *)
PolynomialMod [f - g * PolynomialQuotientP [f,g,var,p], p];
```

Sei  $K[x]/f$  definiert durch

$$K[x]/f := \{[a]_f \mid a \in K[x]\}.$$

Auf  $K[x]/f$  definieren wir  $+$ ,  $-$ ,  $\cdot$  durch

$$\begin{aligned} [a]_f + [b]_f &:= [a + b]_f \\ [a]_f - [b]_f &:= [a - b]_f \\ [a]_f \cdot [b]_f &:= [a \cdot b]_f. \end{aligned}$$

**SATZ 8.19.** Sei  $K$  ein Körper, und sei  $f \in K[x]$ . Dann ist  $\langle K[x]/f, +, -, [0]_f, \cdot, [1]_f \rangle$  ein Ring.

**SATZ 8.20.** Sei  $K$  ein Körper, und sei  $f \in K[x]$  irreduzibel über  $K$ . Dann ist  $K[x]/f$  ein Körper.

$K[x]/f$  wieder ein kommutativer Ring. Es bleibt zu zeigen, dass jedes  $h \in K[x]/f$  mit  $h \neq [0]_f$  invertierbar ist. Sei  $h' \in K[x]$  so, dass  $h = [h']_f$ . Da  $f$  irreduzibel ist, und  $h'$  kein Vielfaches von  $f$  ist, gilt  $\text{ggT}(h', f) = 1$ . Es gibt also  $u, v \in K[x]$ , sodass  $u \cdot h' + v \cdot f = 1$ . Es gilt also  $[u]_f \cdot [h']_f = [u \cdot h']_f = [1 - v \cdot f]_f = [1]_f$ . ■

Wenn  $K$  ein endlicher Körper mit  $q$  Elementen ist, und  $f$  ein über  $K$  irreduzibles Polynom vom Grad  $n$ , dann ist  $K[x]/f$  ein Körper mit  $q^n$  Elementen. Wenn wir also irreduzible Polynome über  $\mathbb{Z}_p$  finden, können wir daraus größere endliche Körper konstruieren. Es gibt die folgende untere Schranke für die Anzahl der irreduziblen Polynome über einem endlichen Körper.

**SATZ 8.21.** Sei  $K$  ein endlicher Körper mit  $q$  Elementen. Von den  $q^n$  normierten Polynomen vom Grad  $n$  über  $K$  sind zumindest  $\frac{1}{2n}q^n$  Polynome irreduzibel.

Der folgende Satz liefert einen Test, ob ein Polynom irreduzibel über einem endlichen Körper mit  $q$  Elementen ist.

**SATZ 8.22.** Sei  $K$  ein Körper mit  $q$  Elementen, sei  $n \in \mathbb{N}$  und sei  $f \in K[x]$  mit  $\deg(f) = n$ . Äquivalent sind:

(1) Für alle  $i \in \{1, 2, \dots, \lfloor \frac{n}{2} \rfloor\}$  gilt:

$$\text{ggT}(f, x^{2^i} - x) = 1.$$

(2)  $f$  ist irreduzibel über  $K$ .

## 5. Eigenschaften endlicher Körper

Für  $n \in \mathbb{N}$  kürzen wir  $\underbrace{1 + 1 + \dots + 1}_{n \text{ mal}}$  mit  $n * 1$  ab.

DEFINITION 8.23. Sei  $K$  ein Körper und sei  $N$  die Menge, die durch

$$N = \{n \in \mathbb{N} \mid n * 1 = 0\}$$

definiert ist. Wenn  $N$  leer ist, dann definieren wir die *Charakteristik* von  $K$  als 0, wenn  $N$  nicht leer ist, dann definieren wir die *Charakteristik* von  $K$  als das kleinste Element in  $N$ .

Für einen endlichen Körper ist die Charakteristik also das kleinste  $a \in \mathbb{N}$  mit  $a * 1 = 0$ . Die Charakteristik von  $\mathbb{Z}_p$  ist  $p$ .

SATZ 8.24. Sei  $K$  ein endlicher Körper. Dann ist seine Charakteristik eine Primzahl.

*Beweis:* Da  $K$  endlich ist, gibt es  $a, b \in \mathbb{N}$  mit  $a > b$  und  $a * 1 = b * 1$ , also  $(a - b) * 1 = 0$ . Wir zeigen nun, dass

$$\min\{n \in \mathbb{N} \mid n * 1 = 0\}$$

eine Primzahl ist. Sei  $p$  dieses Minimum. Wenn es  $c, d < p$  gibt, sodass  $cd = p$ , dann gilt  $(c * 1) \cdot (d * 1) = 0$ , also entweder  $c * 1 = 0$  oder  $d * 1 = 0$ . Das widerspricht der Minimalität von  $p$ . Also ist  $p$  eine Primzahl. ■

SATZ 8.25. Sei  $K$  ein endlicher Körper mit  $q$  Elementen, und sei  $p$  die Charakteristik von  $K$ . Dann gibt es ein  $n \in \mathbb{N}$ , sodass  $q = p^n$ .

SATZ 8.26. Sei  $E$  ein Körper der Charakteristik  $p$  mit  $q = p^m$  Elementen. Dann gilt für alle  $x, y \in E$ :

- (1)  $(x + y)^p = x^p + y^p$ .
- (2)  $x^q = x$ .

*Beweis:* (1): Nach dem binomischen Lehrsatz gilt

$$(x + y)^p = x^p + \sum_{i=1}^{p-1} \binom{p}{i} * x^i y^{p-i} + y^p.$$

Da  $\binom{p}{i}$  für alle  $i \in \{1, 2, \dots, p-1\}$  Vielfache von  $p$  sind, gilt  $(x + y)^p = x^p + y^p$ .

(2): Mit der Idee aus dem Beweis des Satzes von Euler (Satz 7.9) kann man zeigen, dass alle  $x \neq 0$  die Gleichung  $x^{q-1} = 1$  erfüllen. ■

## ÜBUNGS-AUFGABEN 8.27.

- (1) Sei  $K$  ein Körper der Charakteristik  $p$ , sei  $m \in \mathbb{N}$ , und seien  $x, y \in K$ . Zeigen Sie:  $(x + y)^{p^m} = x^{p^m} + y^{p^m}$ .
- (2) Sei  $K$  ein Körper, und sei  $f \in K[x]$ . Seien  $\alpha_1, \alpha_2, \dots, \alpha_k \in K$  paarweise verschiedene Nullstellen von  $f$ . Zeigen Sie, dass  $\prod(x - \alpha_i)$  ein Teiler von  $f$  in  $K[x]$  ist.
- (3) Zeigen Sie, dass ein Polynom in  $K[x]$  vom Grad  $\leq n$ , das  $n + 1$  verschiedene Nullstellen hat, automatisch das Nullpolynom sein muss.

**DEFINITION 8.28.** Sei  $K$  ein endlicher Körper mit  $q$  Elementen. Ein Element  $\alpha \in K$  ist ein *primitives Element* von  $K$ , wenn

$$K = \{0\} \cup \{1, \alpha, \alpha^2, \alpha^3, \dots, \alpha^{q-2}\}.$$

Ein Element ist also genau dann primitiv, wenn jedes von Null verschiedene Körperelement eine Potenz von  $\alpha$  ist.

**DEFINITION 8.29.** Sei  $K$  ein endlicher Körper, und sei  $\alpha \in K \setminus \{0\}$ . Die *Ordnung* von  $\alpha$  in  $K$  ist gegeben durch

$$\text{ord}(\alpha) := \min\{k \in \mathbb{N} \mid \alpha^k = 1\}.$$

**LEMMA 8.30.** Sei  $K$  ein endlicher Körper mit  $q$  Elementen, und sei  $\alpha \in K \setminus \{0\}$ , und sei  $m \in \mathbb{N}$  so, dass  $\alpha^m = 1$ . Dann gilt:

- (1) Die Ordnung von  $\alpha$  ist ein Teiler von  $m$ .
- (2) Die Ordnung von  $\alpha$  ist ein Teiler von  $q - 1$ .

Für  $n \in \mathbb{N}$  ist  $\varphi(n)$  die Anzahl der zu  $n$  teilerfremden Elemente in  $\{1, 2, \dots, n - 1\}$ .

**SATZ 8.31.** Sei  $K$  ein endlicher Körper mit  $q$  Elementen. Dann gibt es genau  $\varphi(q - 1)$  primitive Elemente in  $K$ .

*Beweis:* Wir zeigen zunächst, dass  $K$  zumindest ein primitives Element  $\alpha$  besitzt. Sei  $h := q - 1$ . Für  $h = 1$  und  $q = 2$  ist 1 ein primitives Element. Wir nehmen also nun  $h \geq 2$  an. Wir bilden die Primfaktorzerlegung von  $h$  und finden also  $N \in \mathbb{N}$ , Primzahlen  $p_1, p_2, \dots, p_N$  und  $r_1, r_2, \dots, r_N \in \mathbb{N}$  sodass

$$h = \prod_{m=1}^N p_m^{r_m}.$$

Wir werden nun für jedes  $i \in \{1, 2, \dots, N\}$  ein Element  $a_i$  und ein Element  $b_i \in K \setminus \{0\}$  wählen: Es gilt  $\frac{h}{p_i} < h$ . Da das Polynom  $x^{\frac{h}{p_i}} - 1$  höchstens  $\frac{h}{p_i}$  Nullstellen hat, gibt es ein Element  $a_i \in K \setminus \{0\}$ , sodass  $a_i^{\frac{h}{p_i}} \neq 1$ . Wir setzen

$$b_i := a_i^{\frac{h}{p_i r_i}}.$$

Es gilt dann

$$(8.1) \quad b_i^{p_i^{r_i}} = 1.$$



Sei nun  $k$  die Ordnung von  $b_i$ , also das kleinste  $n \in \mathbb{N}$ , sodass  $(b_i)^n = 1$ . Aus Gleichung (8.1) folgt, dass

$$k | p_i^{r_i}.$$

Folglich gibt es ein  $s_i \in \{0, 1, \dots, r_i\}$ , sodass  $k = p_i^{s_i}$ . Wir zeigen nun

$$(8.2) \quad s_i = r_i.$$

Nehmen wir an  $s_i \leq r_i - 1$ . Dann gilt

$$b_i^{p_i^{r_i-1}} = 1,$$

also

$$a_i^{\frac{h}{p_i}} = 1.$$

Das widerspricht der Wahl von  $a_i$ ; dieser Widerspruch beweist (8.2). Die Ordnung von  $b_i$  ist also  $p_i^{r_i}$ . Wir bilden nun

$$c = \prod_{i=1}^N b_i.$$

Klarerweise gilt  $c^h = 1$ . Wir zeigen nun, dass  $c$  wirklich Ordnung  $h$  hat. Wenn  $c$  kleinere Ordnung hätte, dann gibt es ein  $j \in \{1, \dots, N\}$ , sodass  $c^{\frac{h}{p_j}} = 1$ . Daher gilt

$$(8.3) \quad \prod_{i=1}^N b_i^{\frac{h}{p_j}} = 1.$$

Falls  $i \neq j$ , so gilt  $p_i^{r_i} | \frac{h}{p_j}$ . Wegen (8.1) sind also Faktoren in (8.3) mit  $i \neq j$  gleich 1. Wir erhalten also

$$b_j^{\frac{h}{p_j}} = 1.$$

Da  $b_j$  wegen (8.2) die Ordnung  $p_j^{r_j}$  hat, gilt  $p_j^{r_j} | \frac{h}{p_j}$ . Daher gilt  $p_j^{r_j+1} | h$ , was im Widerspruch zur Primfaktorzerlegung von  $h$  steht. Das Element  $c$  hat also wirklich Ordnung  $h$ , und ist somit ein primitives Element von  $\mathbf{K}$ .

Man kann dann zeigen, dass die primitiven Elemente von  $\mathbf{K}$  genau die Elemente in  $\{c^i \mid i \in \{1, 2, \dots, q-1\} \text{ und } \text{ggT}(i, q-1) = 1\}$  sind. ■

**SATZ 8.32.** Sei  $n \in \mathbb{N}$ ,  $n \geq 6$ . Dann gilt  $\varphi(n) \geq \frac{n}{6 \log(\log(n))}$ . (Dabei nehmen wir den Logarithmus zur Basis  $e$ .)

**SATZ 8.33.** Sei  $\mathbf{K}$  ein Körper mit  $q$  Elementen, und sei  $\alpha \in \mathbf{K}$ . Dann ist  $\alpha$  genau dann primitiv, wenn für jede Primzahl  $p$ , die  $q-1$  teilt, folgendes gilt:

$$\alpha^{\frac{q-1}{p}} \neq 1.$$

**SATZ 8.34.** Sei  $p$  eine Primzahl, sei  $m \in \mathbb{N}$ , und sei  $q = p^m$ . Sei  $f$  ein normiertes, über  $\mathbb{Z}_p$  irreduzibles Polynom in  $\mathbb{Z}_p[x]$  vom Grad  $m$ . Dann ist jeder Körper mit  $q$  Elementen zu  $\mathbb{Z}_p[x]/f$  isomorph.



## KAPITEL 9

### Lineare Abbildungen

#### 1. Beispiele

Wir betrachten einige Funktionen, die von einem Vektorraum in einen Vektorraum gehen.

AUFGABE 9.1. Sei  $s$  jene Funktion von  $\mathbb{R}^2$  nach  $\mathbb{R}^2$ , die jeden Punkt auf den Punkt abbildet, auf dem er nach der Spiegelung an der  $x$ -Achse landet. Dann lässt sich  $s$  so schreiben:

$$s : \mathbb{R}^2 \longrightarrow \mathbb{R}^2 \\ \begin{pmatrix} x \\ y \end{pmatrix} \longmapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} .$$

AUFGABE 9.2. Wir überlegen uns, wo der Punkt  $\begin{pmatrix} x \\ y \end{pmatrix}$  nach einer Drehung um den Nullpunkt um  $60^\circ$  gegen den Uhrzeigersinn landet. Sei  $d$  diese Drehung. Dann lässt sich  $d$  so schreiben:

$$d : \mathbb{R}^2 \longrightarrow \mathbb{R}^2 \\ \begin{pmatrix} x \\ y \end{pmatrix} \longmapsto \begin{pmatrix} \cos(\frac{\pi}{3}) & -\sin(\frac{\pi}{3}) \\ \sin(\frac{\pi}{3}) & \cos(\frac{\pi}{3}) \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} .$$

AUFGABE 9.3. Wir bestimmen die Projektion des Punktes  $(x, y, z) \in \mathbb{R}^3$  auf  $U = L((0, 1, 2), (3, 0, 4))$ . Sei  $p_U$  diese Projektionsabbildung. Wir berechnen die Projektionsmatrix  $P_U$  in folgender Rechnung:

```
In[115]:= B = Transpose [{{0, 1, 2}, {3, 0, 4}}]
```

```
Out[115]= {{0, 3}, {1, 0}, {2, 4}}
```

```
In[116]:= PU = B . Inverse [Transpose [B] . B] . Transpose [B];
```

```
MatrixForm [PU]
```

$$Out[116]= \begin{pmatrix} \frac{45}{61} & -\frac{24}{61} & \frac{12}{61} \\ \frac{61}{24} & \frac{61}{25} & \frac{61}{18} \\ -\frac{61}{12} & \frac{61}{18} & \frac{61}{52} \\ \frac{61}{61} & \frac{61}{61} & \frac{61}{61} \end{pmatrix}$$

Somit haben wir eine Matrix  $P_U$  gefunden, sodass  $P_U \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix}$  die Projektion von  $(x, y, z)$  auf  $U$  ist.

Solche Abbildungen, die man durch Matrizen beschreiben kann, werden der Inhalt dieses Kapitels sein.

## 2. Die Definition linearer Abbildungen

DEFINITION 9.4. Seien  $U$  und  $V$  Vektorräume über dem Körper  $K$ . Eine Abbildung  $h : U \rightarrow V$  ist eine *lineare Abbildung*, wenn:

- (1) für alle  $u_1, u_2 \in U : h(u_1 + u_2) = h(u_1) + h(u_2)$
- (2) für alle  $u \in U$  und für alle  $\lambda \in K : h(\lambda u) = \lambda h(u)$

BEISPIEL 9.5. Sei  $K$  ein Körper, und sei  $A \in K^{n \times m}$ . Dann ist die Abbildung  $h$ , die durch

$$\begin{aligned} h : K^m &\longrightarrow K^n \\ x &\longmapsto A \cdot x \end{aligned}$$

definiert ist, eine lineare Abbildung vom  $K$ -Vektorraum  $K^m$  in den  $K$ -Vektorraum  $K^n$ .

AUFGABE 9.6. Welche der folgenden Abbildungen von  $\mathbb{R}^2$  nach  $\mathbb{R}$  sind linear?

- (1)  $h_1((x, y)) = 3x - 2y$  für  $x, y \in \mathbb{R}$ .
- (2)  $h_2((x, y)) = 3x + 1$  für  $x, y \in \mathbb{R}$ .
- (3)  $h_3((x, y)) = 0$  für  $x, y \in \mathbb{R}$ .

*Lösung.*

- (1) Wir zeigen, dass die Abbildung  $h_1$  linear ist. Seien dazu  $u, v \in \mathbb{R}^2$ . Es gibt dann  $x_1, y_1, x_2, y_2 \in \mathbb{R}$ , sodass  $u = (x_1, y_1)$  und  $v = (x_2, y_2)$ . Es gilt dann  $h_1(u + v) = 3(x_1 + x_2) - 2(y_1 + y_2) = (3x_1 - 2y_1) + (3x_2 - 2y_2) = h_1(u) + h_1(v)$  und  $h_1(\lambda u) = 3(\lambda x_1) - 2(\lambda y_1) = \lambda(3x_1 - 2y_1) = \lambda h_1(u)$ .
- (2)  $h_2$  ist keine lineare Abbildung, da  $h_2((1, 1) + (1, 1)) = h_2((2, 2)) = 7$  und  $h_2((1, 1)) + h_2((1, 1)) = 4 + 4 = 8$ .
- (3)  $h_3$  ist linear.

SATZ 9.7. Sei  $K$  ein Körper, seien  $U, V, W$  Vektorräume über  $K$ , und seien  $f : U \rightarrow V$  und  $g : V \rightarrow W$  lineare Abbildungen. Dann ist die Hintereinanderausführung  $g \circ f$  ebenfalls linear.

SATZ 9.8. Sei  $K$  ein Körper, sei  $m \in \mathbb{N}$ , und sei  $V$  ein Vektorraum über  $K$  mit Basis  $B = (b_1, \dots, b_m)$ . Dann ist die Abbildung  $c$ , die durch

$$\begin{aligned} c : V &\longrightarrow K^m \\ v &\longmapsto (v)_B \end{aligned}$$

definiert ist, eine lineare Abbildung.

*Beweis.* Wir geben hier nur den Beweis dafür, dass  $c(u+v) = c(u)+c(v)$  für alle  $u, v \in V$ . Seien  $u, v \in V$ . Zu zeigen ist, dass  $(u+v)_B = (u)_B + (v)_B$ . Seien  $\lambda_1, \dots, \lambda_m \in K$  und  $\mu_1, \dots, \mu_m \in K$  so, dass

$$\sum_{i=1}^m \lambda_i b_i = u$$

und

$$\sum_{i=1}^m \mu_i b_i = v.$$

Dann gilt also  $(u)_B = (\lambda_1, \dots, \lambda_m)$  und  $(v)_B = (\mu_1, \dots, \mu_m)$ . Wir berechnen nun

$$\sum_{i=1}^m (\lambda_i + \mu_i) b_i.$$

Es gilt  $\sum_{i=1}^m (\lambda_i + \mu_i) b_i = \sum_{i=1}^m \lambda_i b_i + \sum_{i=1}^m \mu_i b_i = u + v$ . Da also  $\sum_{i=1}^m (\lambda_i + \mu_i) b_i = u + v$ , gilt  $(u+v)_B = (\lambda_1 + \mu_1, \dots, \lambda_m + \mu_m) = (\lambda_1, \dots, \lambda_m) + (\mu_1, \dots, \mu_m) = (u)_B + (v)_B$ . ■

Auch die inverse Abbildung dieser Abbildung ist linear:

**SATZ 9.9.** Sei  $K$  ein Körper, sei  $m \in \mathbb{N}$ , und sei  $V$  ein Vektorraum über  $K$  mit Basis  $B = (b_1, \dots, b_m)$ . Dann ist die Abbildung  $d$ , die durch

$$d : \quad K^m \longrightarrow V \\ (\lambda_1, \dots, \lambda_m) \longmapsto \sum_{i=1}^m \lambda_i b_i$$

definiert ist, eine lineare Abbildung.

**SATZ 9.10.** Seien  $U$  und  $V$  Vektorräume über  $K$  mit den Basen  $B = (b_1, \dots, b_m)$  und  $C = (c_1, \dots, c_n)$ . Sei  $A$  eine  $m \times n$ -Matrix. Die Funktion  $f : U \rightarrow V$  bilde  $x$  auf jenes  $y$ , das durch

$$(y)_C = A \cdot (x)_B$$

gegeben ist, ab. Dann ist  $f$  eine lineare Abbildung.

*Beweisskizze.* Es gilt  $f = g \circ h \circ i$ , wobei  $i : U \rightarrow K^m$ ,  $u \mapsto (u)_B$ ,  $h : K^m \rightarrow K^n$ ,  $x \mapsto A \cdot x$ ,  $g : K^n \rightarrow V$ ,  $(\lambda_1, \dots, \lambda_n) \mapsto \sum_{i=1}^n \lambda_i c_i$ . Alle drei Abbildungen  $g, h, i$  sind linear, also auch ihre Hintereinanderausführung. ■

**AUFGABE 9.11.** Sei  $U$  der Unterraum des  $\mathbb{R}^3$  mit Basis  $B = ((1, 1, 1), (1, 0, 0))$ , und sei  $h : \mathbb{R}^3 \rightarrow \mathbb{R}^2$ ,  $v \mapsto (v)_B$ . Dann ist etwa

$$h((4, 1, 1)) = \begin{pmatrix} 1 \\ 3 \end{pmatrix}, \\ h((-1, -1, -1)) = \begin{pmatrix} -1 \\ 0 \end{pmatrix}.$$

**ÜBUNGSAUFGABEN 9.12.**

- (1) Eine lineare Abbildung von  $h$  von  $\mathbb{R}^2$  nach  $\mathbb{R}^2$  bildet den Punkt  $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$  auf  $\begin{pmatrix} 2 \\ 0 \end{pmatrix}$  und den Punkt  $\begin{pmatrix} 1 \\ -1 \end{pmatrix}$  auf  $\begin{pmatrix} 0 \\ -2 \end{pmatrix}$  ab. Auf welchen Punkt wird  $\begin{pmatrix} 1 \\ 2 \end{pmatrix}$  abgebildet?
- (2) Zeigen oder widerlegen Sie: Wenn  $h$  eine lineare Abbildung von  $\mathbb{R}^3$  nach  $\mathbb{R}^2$  ist und  $h \neq 0$ , dann gilt für alle  $v_1, v_2 \in \mathbb{R}^3$ :

$$(v_1, v_2) \text{ linear unabhängig} \Rightarrow (h(v_1), h(v_2)) \text{ linear unabhängig.}$$

### 3. Abbildungsmatrizen linearer Abbildungen

Sei  $h : U \rightarrow V$  eine lineare Abbildung,  $B = (b_1, \dots, b_m)$  eine Basis von  $U$ . Sei  $x \in U$  mit  $x = \sum_{i=1}^m \lambda_i \cdot b_i$ . Dann gilt wegen der Linearität von  $h$ :

$$h(x) = h\left(\sum_{i=1}^m \lambda_i \cdot b_i\right) = \sum_{i=1}^m \lambda_i \cdot h(b_i).$$

Eine lineare Abbildung ist also durch die Bilder der Basisvektoren bereits vollständig bestimmt.

Wir werden jetzt sehen, dass sich jede lineare Abbildung, deren Definitions- und Bildbereich endlichdimensionale Vektorräume sind, durch eine Matrix darstellen lässt.

**DEFINITION 9.13.** Seien  $U, V$  Vektorräume über  $K$ , seien  $m, n \in \mathbb{N}$ , sei  $B = (b_1, \dots, b_m)$  eine Basis von  $U$  und  $C = (c_1, \dots, c_n)$  eine Basis von  $V$ . Sei  $h$  eine lineare Abbildung von  $U$  nach  $V$ . Wir definieren nun die  $n \times m$ -Matrix  $S_h(B, C)$ . Dazu legen wir fest, dass für  $i \in \{1, \dots, m\}$  in der  $i$ -ten Spalte von  $S_h(B, C)$  der Vektor  $(h(b_i))_C$  steht. Es gilt also

$$S_h(B, C) = \left( \begin{array}{c|c|c|c} | & | & & | \\ (h(b_1))_C & (h(b_2))_C & \cdots & (h(b_m))_C \\ | & | & & | \end{array} \right).$$

Die Matrix  $S_h(B, C) \in K^{n \times m}$  heißt *Abbildungsmatrix* oder *Darstellungsmatrix* von  $h$  bezüglich der Basen  $B$  und  $C$ .

**SATZ 9.14.** Seien  $U, V$  Vektorräume über  $K$ , seien  $m, n \in \mathbb{N}$ , sei  $B = (b_1, \dots, b_m)$  eine Basis von  $U$  und  $C = (c_1, \dots, c_n)$  eine Basis von  $V$ . Sei  $h$  eine lineare Abbildung von  $U$  nach  $V$ . Dann gilt

$$(9.1) \quad (h(u))_C = S_h(B, C) \cdot (u)_B \text{ für alle } u \in U.$$

*Beweis.* Sei  $u \in U$  mit  $u = \sum_{i=1}^m \lambda_i b_i$ . Dann gilt

$$\begin{aligned} (h(u))_C &= \left( h \left( \sum_{i=1}^m \lambda_i b_i \right) \right)_C \\ &= \left( \sum_{i=1}^m \lambda_i h(b_i) \right)_C \\ &= \sum_{i=1}^m \lambda_i (h(b_i))_C \\ &= \begin{pmatrix} | & | & \cdots & | \\ (h(b_1))_C & (h(b_2))_C & \cdots & (h(b_m))_C \\ | & | & & | \end{pmatrix} \cdot \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_m \end{pmatrix} \\ &= S_h(B, C) \cdot (u)_B. \end{aligned}$$

■

Wir zeigen nun, dass die Abbildungsmatrix durch die Gleichung (9.1) eindeutig bestimmt ist.

**SATZ 9.15.** Seien  $U, V$  Vektorräume über  $K$ , seien  $m, n \in \mathbb{N}$ , sei  $B = (b_1, \dots, b_m)$  eine Basis von  $U$  und  $C = (c_1, \dots, c_n)$  eine Basis von  $V$ . Sei  $h$  eine lineare Abbildung von  $U$  nach  $V$ , und sei  $A$  eine  $n \times m$ -Matrix, sodass für alle  $u \in U$ :

$$(9.2) \quad (h(u))_C = A \cdot (u)_B.$$

Dann gilt  $A = S_h(B, C)$ .

*Beweis.* Sei  $i \in \{1, \dots, m\}$ . Wegen (9.2) gilt  $(h(b_i))_C = A \cdot (b_i)_B$ , also

$$(h(b_i))_C = A \cdot \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix},$$

wobei der Einser an der  $i$ ten Stelle steht. Die rechte Seite dieser Gleichung ergibt die  $i$ -te Spalte von  $A$ . Also ist die  $i$ -te Spalte von  $A$  gleich  $(h(b_i))_C$ . Daher  $A = S_h(B, C)$ . ■

**AUFGABE 9.16.** Sei  $h : \mathbb{R}^2 \rightarrow \mathbb{R}^3$  die folgende lineare Abbildung.

$$\begin{aligned} h : \mathbb{R}^2 &\longrightarrow \mathbb{R}^3 \\ \begin{pmatrix} x \\ y \end{pmatrix} &\longmapsto \begin{pmatrix} 3x-2y \\ 2x+y \\ -x+4y \end{pmatrix}. \end{aligned}$$

Sei  $B$  die Basis  $\left( \begin{pmatrix} -1 \\ 2 \end{pmatrix}, \begin{pmatrix} 4 \\ 5 \end{pmatrix} \right)$  des  $\mathbb{R}^2$ , und sei  $C$  die Basis  $\left( \begin{pmatrix} -9 \\ -13 \\ -7 \end{pmatrix}, \begin{pmatrix} 20 \\ 39 \\ 30 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right)$  des  $\mathbb{R}^3$ . Bestimmen Sie  $S_h(B, C)$ .

*Lösung:* Es gilt

$$h(b_1) = \begin{pmatrix} -7 \\ 0 \\ 9 \end{pmatrix}, \quad h(b_2) = \begin{pmatrix} 2 \\ 13 \\ 16 \end{pmatrix}.$$

Aus dem Gleichungssystem

$$\begin{pmatrix} -9 & 20 & 0 \\ -13 & 39 & 1 \\ -7 & 30 & 0 \end{pmatrix} \cdot x = \begin{pmatrix} -7 \\ 0 \\ 9 \end{pmatrix}$$

erhalten wir  $(h(b_1))_C = \begin{pmatrix} 3 \\ 1 \\ 0 \end{pmatrix}$  und ebenso  $(h(b_2))_C = \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix}$ . Insgesamt erhalten wir

$$S_h(B, C) = \begin{pmatrix} 3 & 2 \\ 1 & 1 \\ 0 & 0 \end{pmatrix}.$$

In Mathematica kann man die notwendigen Rechnungen so durchführen:

```
In[117]:= h[x_, y_] = {{3, -2}, {2, 1}, {-1, 4}} . {x, y}
```

```
Out[117]= {3 x - 2 y, 2 x + y, -x + 4 y}
```

```
In[118]:= hb1 = h[-1, 2]
```

```
Out[118]= {-7, 0, 9}
```

```
In[119]:= hb2 = h[4, 5]
```

```
Out[119]= {2, 13, 16}
```

```
In[120]:= CC = {{-9, 20, 0}, {-13, 39, 1}, {-7, 30, 0}}
```

```
Out[120]= {{-9, 20, 0}, {-13, 39, 1}, {-7, 30, 0}}
```

```
In[121]:= MatrixForm[CC]
```

```
Out[121]=  $\begin{pmatrix} -9 & 20 & 0 \\ -13 & 39 & 1 \\ -7 & 30 & 0 \end{pmatrix}$ 
```

```
In[122]:= LinearSolve[CC, hb1]
```

```
Out[122]= {3, 1, 0}
```

```
In[123]:= LinearSolve[CC, hb2]
```

```
Out[123]= {2, 1, 0}
```

AUFGABE 9.17. Sei  $U = \mathbb{R}^2$ ,  $V = \mathbb{R}^1$  mit den kanonischen Basen  $B = ((1, 0), (0, 1))$  und  $C = ((1))$ . Die lineare Abbildung  $h : U \rightarrow V$  sei definiert durch

$$h((x, y)) = (3x - 2y)$$

für alle  $x, y \in \mathbb{R}$ . In diesem Fall ist  $(h(b_1))_C = (3)$  und  $(h(b_2))_C = (-2)$ . Somit gilt

$$S_h(B, C) = \begin{pmatrix} 3 & -2 \end{pmatrix}.$$

AUFGABE 9.18. Sei  $U = \mathbb{R}^2$ ,  $V = \mathbb{R}^1$  mit den Basen  $B = ((2, 3), (3, -2))$ ,  $C = ((2))$ . Die lineare Abbildung  $h : U \rightarrow V$  sei definiert durch

$$h((x, y)) = (3x - 2y)$$

für alle  $x, y \in \mathbb{R}$ . Dann ist  $h(b_1) = 0$ , also  $(h(b_1))_B = (0)$  und  $h(b_2) = (13)$ , also  $(h(b_2))_B = 6.5$ , und folglich  $S_h(B, C) = \begin{pmatrix} 0 & 6.5 \end{pmatrix}$ .



## ÜBUNGSAUFGABEN 9.19.

- (1) Eine lineare Abbildung  $h : \mathbb{R}^2 \rightarrow \mathbb{R}^2$  sei gegeben durch  $h\left(\begin{pmatrix} 1 \\ -1 \end{pmatrix}\right) = \begin{pmatrix} 0 \\ 2 \end{pmatrix}$  und  $h\left(\begin{pmatrix} -2 \\ 1 \end{pmatrix}\right) = \begin{pmatrix} 1 \\ 7 \end{pmatrix}$ . Bestimmen Sie die Abbildungsmatrix  $S_h(E, E)$ , wobei  $E = \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right)$ .
- (2) Seien  $E_2, E_3$  die kanonischen Basen von  $\mathbb{R}^2$  und  $\mathbb{R}^3$ , und sei

$$\sigma((x, y, z)) := (3x - 2y, 2z).$$

Geben Sie die Abbildungsmatrix  $S_\sigma(E_3, E_2)$  an.

#### 4. Abbildungsmatrizen für Spiegelungen und Drehungen

Wir wollen nun die Abbildungsmatrizen für bestimmte Drehungen und Spiegelungen bestimmen. Wir betrachten folgende Beispiele:

AUFGABE 9.20. Sei  $e$  die Ebene  $L\left(\begin{pmatrix} 1 \\ 2 \\ -1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix}\right)$ , und sei  $\sigma$  jene Abbildung, die jeden Punkt im  $\mathbb{R}^3$  auf den Punkt abbildet, auf dem er nach der Spiegelung an der Ebene  $e$  landet.

Gesucht ist die Abbildungsmatrix  $S_\sigma(E, E)$  dieser Spiegelung bezüglich der kanonischen Basis  $E$  des  $\mathbb{R}^3$ .

AUFGABE 9.21. Sei  $g$  die Gerade mit der Gleichung  $5x - 2y = 0$  im  $\mathbb{R}^2$ . Sei  $\sigma$  jene Abbildung, die jeden Punkt im  $\mathbb{R}^2$  auf den Punkt abbildet, auf dem er nach der Spiegelung an  $g$  landet.

Gesucht ist die Abbildungsmatrix  $S_\sigma(E, E)$  dieser Spiegelung bezüglich der kanonischen Basis  $E$  des  $\mathbb{R}^2$ .

AUFGABE 9.22. Sei  $g$  die Gerade  $L\left(\begin{pmatrix} 1 \\ 2 \\ -2 \end{pmatrix}\right)$ , und sei  $\delta : \mathbb{R}^3 \rightarrow \mathbb{R}^3$  jene Abbildung, die jeden Punkt auf den Punkt abbildet, auf dem er nach der Drehung um  $60^\circ$  um die Gerade  $g$  landet. Wir müssen noch die Richtung der Drehung festlegen: Wenn wir vom Punkt  $\begin{pmatrix} 1 \\ 2 \\ -2 \end{pmatrix}$  auf die Ebene  $x + 2y - 2z = 0$  hinunterschauen, dann sollen sich die Punkte dieser Ebene gegen den Uhrzeigersinn drehen.

Alle drei Beispiele kann man mit dem gleichen "Programm" lösen. Sei  $h$  die angegebene lineare Abbildung. Dann gehen wir so vor:

- (1) Bestimme eine Basis  $B$ , sodass  $S_h(B, B)$  leicht zu bestimmen ist.
- (2) Bestimme  $S_h(B, B)$ .
- (3) Bestimme  $S_h(E, E)$  aus  $S_h(B, B)$ .

Die Schritte (1) und (2) können wir bereits jetzt durchführen; für den Schritt (3) müssen wir uns noch überlegen, wie man aus den Koordinaten eines Vektors bezüglich einer Basis die Koordinaten bezüglich einer anderen Basis ausrechnet.

Wir starten mit Beispiel 9.20. Wir wählen eine Basis  $(b_1, b_2, b_3)$  des  $\mathbb{R}^3$ , sodass  $b_1, b_2$  in der Ebene  $e$  liegen, und  $b_3$  auf  $b_1$  und  $b_2$  normal steht. Es gilt dann  $\sigma(b_1) = b_1$ ,

$\sigma(b_2) = b_2$  und  $\sigma(b_3) = -b_3$ . Also gilt  $(\sigma(b_1))_B = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ ,  $(\sigma(b_2))_B = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$  und  $(\sigma(b_3))_B = (-b_3)_B = \begin{pmatrix} 0 \\ 0 \\ -1 \end{pmatrix}$ . Dann gilt

$$S_\sigma(B, B) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

Wir bestimmen nun eine Basis  $B$  mit den gewünschten Eigenschaften. Dazu wählen wir  $b_1 = \begin{pmatrix} 1 \\ 2 \\ -1 \end{pmatrix}$  und  $b_2 = \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix}$ . Wir bestimmen einen Vektor, der auf beiden normal steht:

`In[124]:= Nullspace [ {{1, 2, -1}, {0, 1, -1}} ]`

`Out[124]= {{-1, 1, 1}}`

Also wählen wir  $b_3 = \begin{pmatrix} -1 \\ 1 \\ 1 \end{pmatrix}$ , und somit

$$B = \left( \begin{pmatrix} 1 \\ 2 \\ -1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \\ 1 \end{pmatrix} \right).$$

Wir bestimmen nun  $B$  und  $S_\sigma(B, B)$  für Beispiel 9.21. Wir wählen eine Basis  $(b_1, b_2)$  des  $\mathbb{R}^2$ , sodass  $b_1$  auf der Gerade  $g$  liegt, und  $b_2$  auf  $b_1$  normal steht. Es gilt dann  $\sigma(b_1) = b_1$  und  $\sigma(b_2) = -b_2$ , und somit  $(\sigma(b_1))_B = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$  und  $(\sigma(b_2))_B = (-b_2)_B = \begin{pmatrix} 0 \\ -1 \end{pmatrix}$ . Dann gilt

$$S_\sigma(B, B) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Wir bestimmen nun eine Basis  $B$  mit den gewünschten Eigenschaften. Dazu wählen wir  $b_2 = \begin{pmatrix} 5 \\ -2 \end{pmatrix}$  und  $b_1 = \begin{pmatrix} 2 \\ 5 \end{pmatrix}$ . Wir erhalten

$$B = \left( \begin{pmatrix} 2 \\ 5 \end{pmatrix}, \begin{pmatrix} 5 \\ -2 \end{pmatrix} \right).$$

Nun bestimmen wir  $B$  und  $S_\delta(B, B)$  für Beispiel 9.22. Dazu bestimmen wir eine Orthonormalbasis  $B$  von  $\mathbb{R}^3$ , sodass  $b_3 = \frac{1}{\left\| \begin{pmatrix} 1 \\ 2 \\ -2 \end{pmatrix} \right\|} \begin{pmatrix} 1 \\ 2 \\ -2 \end{pmatrix}$ . Außerdem soll  $(b_1, b_2, b_3)$  *positiv orientiert* sein. Das heißt: "Wenn man  $b_1$  in  $b_2$  hineinschraubt, dann soll sich eine Schraube mit Rechtsgewinde in Richtung  $b_3$  bewegen." Eine ONB  $(b_1, b_2, b_3)$  ist dann positiv orientiert, wenn  $b_1 \times b_2 = b_3$ . Zu dieser Basis  $B$  bestimmen wir jetzt die Matrix  $S_\delta(B, B)$ . Es gilt  $h(b_3) = b_3$ ,  $h(b_1) = \cos(60^\circ)b_1 + \sin(60^\circ)b_2$ , und  $h(b_2) = -\sin(60^\circ)b_1 + \cos(60^\circ)b_2$ . Mit  $c := \cos(60^\circ)$  und  $s := \sin(60^\circ)$  lässt sich  $S_\delta(B, B)$  also durch

$$S_\delta(B, B) = \begin{pmatrix} c & -s & 0 \\ s & c & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

angeben. Jetzt bestimmen eine Basis  $B$  des  $\mathbb{R}^3$  mit den gewünschten Eigenschaften. Dazu bestimmen wir zunächst eine ONB der Ebene  $e = (L(\begin{pmatrix} 1 \\ 2 \\ -2 \end{pmatrix}))^\perp$ . Wir bestimmen eine Basis für diese Ebene:

`In[125]:= NullSpace[{{1, 2, -2}}]`

`Out[125]= {{2, 0, 1}, {-2, 1, 0}}`

Daher ist  $((2, 0, 1), (-2, 1, 0))$  eine Basis von  $e$ . Wir bestimmen nun eine ONB von  $e$ .

`In[126]:= e1 = {2, 0, 1};`

`e2 = {-2, 1, 0};`

`d1 = e1 / Sqrt[e1.e1]`

`Out[126]= { $-\frac{2}{\sqrt{5}}, 0, \frac{1}{\sqrt{5}}$ }`

`In[127]:= c2 = e2 - (e2.d1) * d1`

`Out[127]= { $-\frac{2}{5}, 1, \frac{4}{5}$ }`

`In[128]:= d2 = c2 / Sqrt[c2.c2]`

`Out[128]= { $-\frac{2}{3\sqrt{5}}, \frac{\sqrt{5}}{3}, \frac{4}{3\sqrt{5}}$ }`

Daher ist die Basis  $F$ , die durch

$$F = \left( \frac{1}{\sqrt{5}} \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{45}} \begin{pmatrix} -2 \\ 5 \\ 4 \end{pmatrix}, \frac{1}{3} \begin{pmatrix} 1 \\ 2 \\ -2 \end{pmatrix} \right)$$

gegeben ist, eine ONB des  $\mathbb{R}^3$ . Wir bestimmen, ob  $F$  positive Orientierung hat:

`In[129]:= Cross[d1, d2]`

`Out[129]= { $-\frac{1}{3}, -\frac{2}{3}, \frac{2}{3}$ }`

Die Orientierung ist also noch falsch. Wenn wir das Vorzeichen von  $f_1$  umdrehen, erhalten wir eine Basis mit positiver Orientierung. (Man kann genausogut das Vorzeichen von  $f_2$  umdrehen. Man darf aber nicht das Vorzeichen von  $f_3$  umdrehen; die Basis, die man durch Umdrehen des Vorzeichens von  $f_3$  erhält, ist zwar positiv orientiert, aber ihr dritter Basisvektor ist nicht mehr der gewünschte.) Wir schreiben die Basisvektoren von  $B$  in die Spalten der Matrix  $\bar{B}$ .

`In[130]:= d3 = Cross[-d1, d2]`

`Out[130]= { $\frac{1}{3}, \frac{2}{3}, -\frac{2}{3}$ }`

`In[131]:= B = Transpose[{-d1, d2, d3}]`

`Out[131]= {{ $-\frac{2}{\sqrt{5}}, -\frac{2}{3\sqrt{5}}, \frac{1}{3}$ }, { $0, \frac{\sqrt{5}}{3}, \frac{2}{3}$ }, { $-\frac{1}{\sqrt{5}}, \frac{4}{3\sqrt{5}}, -\frac{2}{3}$ }}`

`In[132]:= MatrixForm[B]`

`Out[132]= 
$$\begin{pmatrix} -\frac{2}{\sqrt{5}} & -\frac{2}{3\sqrt{5}} & \frac{1}{3} \\ 0 & \frac{\sqrt{5}}{3} & \frac{2}{3} \\ -\frac{1}{\sqrt{5}} & \frac{4}{3\sqrt{5}} & -\frac{2}{3} \end{pmatrix}$$`

Somit haben wir auch für Beispiel 9.22 eine Basis  $B$  und die Matrix  $S_\delta(B, B)$  gefunden.

## 5. Basistransformationen

Wir lösen folgendes Problem: Gegeben sind zwei Basen  $B, C$  des gleichen Unterraums  $U$  des  $\mathbb{R}^n$ , und die Koordinaten  $(v)_B$  eines Vektors  $v \in U$ . Gesucht sind die Koordinaten von  $v$  bezüglich  $C$ , also  $(v)_C$ .

AUFGABE 9.23. Sei  $B = ((1, 0, 1), (1, -1, 0))$  und  $C = ((3, -2, 1), (1, 1, 2))$ , und sei  $(x)_B = (1, -1)$ . Gesucht ist  $(x)_C$ .

*Lösung:* Aus  $B$  und  $(x)_B$  können wir

$$x = B \cdot (x)_B = \begin{pmatrix} 1 & 1 \\ 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$$

berechnen. Wegen  $C \cdot (x)_C = x$  gilt:

$$\begin{pmatrix} 3 & 1 \\ -2 & 1 \\ 1 & 2 \end{pmatrix} \cdot (x)_C = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$$

Als Lösung dieses Gleichungssystems erhalten wir  $(x)_C = (-0.2, 0.6)$ .

Allgemein gehen wir also so vor: Wenn  $\bar{B}$  und  $\bar{C}$  die Matrizen sind, in deren Spalten die Vektoren von  $B$  beziehungsweise  $C$  stehen. Dann lässt sich  $(x)_C$  aus der Gleichung

$$\bar{C} \cdot (x)_C = \bar{B} \cdot (x)_B$$

berechnen. Wenn  $\bar{C}$  gleich viele Spalten wie Zeilen hat, dann ist  $\bar{C}$  invertierbar, und wir erhalten

$$(x)_C = \bar{C}^{-1} \cdot \bar{B} \cdot (x)_B.$$

Wenn  $\bar{C}$  weniger Spalten als Zeilen hat, dann wissen wir, dass die Spaltenvektoren von  $\bar{C}$  linear unabhängig sind. Da  $\bar{C}$  eine Matrix über den reellen Zahlen ist, ist  $\bar{C}^T \cdot \bar{C}$  invertierbar. Dann gilt:  $\bar{C}^T \cdot \bar{C} \cdot (x)_C = \bar{C}^T \cdot \bar{B} \cdot (x)_B$ , und somit

$$(x)_C = (\bar{C}^T \cdot \bar{C})^{-1} \cdot \bar{C}^T \cdot \bar{B} \cdot (x)_B.$$

DEFINITION 9.24. Sei  $K$  ein Körper, sei  $U$  ein Unterraum von  $K^n$ , und seien  $B$  und  $C$  Basen von  $U$ . Eine Matrix  $T$  ist eine *Basistransformationsmatrix* von  $B$  nach  $C$ , wenn für alle  $u \in U$  gilt

$$(u)_C = T \cdot (u)_B.$$

Es gibt genau eine solche Matrix. Wir kürzen sie mit  ${}_C T_B$  ab. Es gilt also

$$(u)_C = {}_C T_B \cdot (u)_B \text{ für alle } u \in U.$$

Die Basistransformationsmatrix ist genau die Abbildungsmatrix  $S_{\text{id}}(B, C)$ , wobei  $\text{id} : U \rightarrow U, u \mapsto u$  die identische Abbildung ist.

Seien  $\bar{B}$  und  $\bar{C}$  die Matrizen, in deren Spalten die Vektoren der Basen  $B$  bzw.  $C$  stehen. Dann kann die Basistransformationsmatrizen so berechnen:

- (1) Falls  $\bar{B}$  und  $\bar{C}$  quadratische Matrizen sind, so gilt  ${}_C T_B := \bar{C}^{-1} \cdot \bar{B}$ .
- (2) Falls  $\bar{C}^T \cdot \bar{C}$  invertierbar ist (das ist immer der Fall, wenn  $K$  der Körper der reellen Zahlen ist), so gilt  ${}_C T_B := (\bar{C}^T \cdot \bar{C})^{-1} \cdot \bar{C}^T \cdot \bar{B}$ .
- (3) In jedem Fall kann man  ${}_C T_B$  als Abbildungsmatrix  $S_{\text{id}}(B, C)$  berechnen. In der  $i$ -ten Spalte von  ${}_C T_B$  steht also  $(b_i)_C$ , also die Lösung des Gleichungssystems  $\bar{C} \cdot x = b_i$ .

ÜBUNGSAUFGABEN 9.25.

- (1) (Koordinaten) Die Ebene  $\varepsilon$  hat die Basen

$$A = \left( \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ 0 \end{pmatrix} \right)$$

und

$$B = \left( \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ 2 \end{pmatrix} \right).$$

- (a) Der Vektor  $v$  hat bezüglich  $B$  die Koordinaten  $(v)_B = \begin{pmatrix} 7 \\ -3 \end{pmatrix}$ . Berechnen Sie seine Koordinaten bezüglich  $A$ !
- (b) Bestimmen Sie eine Matrix  $T$ , sodass für alle  $v \in \varepsilon$  gilt:

$$(v)_A = T \cdot (v)_B.$$

(Diese Matrix heißt *Basistransformationsmatrix*).

**6. Die Hintereinanderausführung und die Matrizenmultiplikation**

SATZ 9.26. Seien  $U, V, W$  Vektorräume über dem Körper  $K$  mit den Basen  $A, B, C$ , und seien  $f : U \rightarrow V$  und  $g : V \rightarrow W$  lineare Abbildungen. Dann gilt

$$(9.3) \quad S_{g \circ f}(A, C) = S_g(B, C) \cdot S_f(A, B).$$

*Beweis.* Wir zeigen, dass für alle  $u \in U$  gilt:

$$(S_g(B, C) \cdot S_f(A, B)) \cdot (u)_A = ((g \circ f)(u))_C.$$

Dann folgt aus Satz 9.15 die Gleichung 9.3. Sei  $u \in U$ . Dann gilt  $(S_g(B, C) \cdot S_f(A, B)) \cdot (u)_A = S_g(B, C) \cdot (S_f(A, B) \cdot (u)_A) = S_g(B, C) \cdot (f(u))_B = (g(f(u)))_C = (g \circ f(u))_C$ . ■

AUFGABE 9.27. Man spiegle den Punkt  $(2, 3)$  an der  $x$ -Achse, und drehe anschließend den gespiegelten Punkt um  $90^\circ$  gegen den Uhrzeigersinn um den Nullpunkt:

*Lösung:* Die Spiegelung  $\sigma$  an der  $x$ -Achse hat bzgl. der kanonischen Basis  $E$  des  $\mathbb{R}^2$  die Darstellungsmatrix  $S_\sigma(E, E) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ . Die Drehung  $\delta$  um  $90^\circ$  hat die Darstellungsmatrix  $S_\delta(E, E) = \begin{pmatrix} \cos(90^\circ) & -\sin(90^\circ) \\ \sin(90^\circ) & \cos(90^\circ) \end{pmatrix}$ . Die Darstellungsmatrix der Spiegelung mit

anschließender Drehung ist also

$$S_{\delta \circ \sigma}(E, E) = S_{\delta}(E, E) \cdot S_{\sigma}(E, E) = \begin{pmatrix} \cos(90^\circ) & \sin(90^\circ) \\ \sin(90^\circ) & -\cos(90^\circ) \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Wir erhalten  $\delta(\sigma((2, 3))) = (3, 2)$ .

**SATZ 9.28.** Seien  $U, V$  Vektorräume über dem Körper  $K$ , und seien  $A, B$  Basen von  $U$  und  $C, D$  Basen von  $V$ . Sei  $h$  eine lineare Abbildung von  $U$  nach  $V$ . Dann gilt

$$S_h(A, D) = {}_D T_C \cdot S_h(B, C) \cdot {}_B T_A.$$

*Beweisskizze.* Für alle  $u \in U$  gilt  ${}_D T_C \cdot S_h(B, C) \cdot {}_B T_A \cdot (u)_A = (h(u))_D$ . Also gilt nach Satz 9.15  ${}_D T_C \cdot S_h(B, C) \cdot {}_B T_A = S_h(A, D)$ . ■

Das folgende Korollar wird uns helfen, die Beispiele 9.20, 9.21 und 9.22 zu lösen.

**KOROLLAR 9.29.** Sei  $K$  ein Körper, sei  $B$  eine Basis des  $K$ -Vektorraums  $K^n$ , und sei  $E$  die kanonische Basis von  $K^n$ . Sei  $h$  eine lineare Abbildung von  $K^n$  nach  $K^n$ . Dann gilt

$$S_h(E, E) = {}_E T_B \cdot S_h(B, B) \cdot {}_B T_E.$$

Wenn  $\bar{B}$  die Matrix ist, in deren Spalten die Vektoren von  $B$  stehen, so gilt also

$$S_h(E, E) = \bar{B} \cdot S_h(B, B) \cdot \bar{B}^{-1}.$$

## 7. Abbildungsmatrizen für Spiegelungen und Drehungen bezüglich der kanonischen Basis

Wir lösen das Beispiel 9.20. Dazu müssen wir die Abbildungsmatrix  $S_h(E, E)$  aus der Abbildungsmatrix  $S_h(B, B)$  ausrechnen.

`In[133]:= B = Transpose [{{1, 2, -1}, {0, 1, -1}, {-1, 1, 1}}]`

`Out[133]= {{1, 0, -1}, {2, 1, 1}, {-1, -1, 1}}`

`In[134]:= ShBB = {{1, 0, 0}, {0, 1, 0}, {0, 0, -1}}`

`Out[134]= {{1, 0, 0}, {0, 1, 0}, {0, 0, -1}}`

`In[135]:= ETB = B`

`Out[135]= {{1, 0, -1}, {2, 1, 1}, {-1, -1, 1}}`

`In[136]:= BTE = Inverse [B]`

`Out[136]= {{2/3, 1/3, 1/3}, {-1, 0, -1}, {-1/3, 1/3, 1/3}}`

`In[137]:= ShEE = ETB . ShBB . BTE`

`Out[137]= {{1/3, 2/3, 2/3}, {2/3, 1/3, -2/3}, {2/3, -2/3, 1/3}}`

`In[138]:= MatrixForm [ShEE]`

$$\text{Out}[138]= \begin{pmatrix} \frac{1}{3} & \frac{2}{3} & \frac{2}{3} \\ \frac{2}{3} & \frac{1}{3} & -\frac{2}{3} \\ \frac{2}{3} & -\frac{2}{3} & \frac{1}{3} \end{pmatrix}$$

Nun lösen wir das Beispiel 9.21.

`In[139]:= B = Transpose[{2, 5}, {5, -2}]`

`Out[139]= {{2, 5}, {5, -2}}`

`In[140]:= ShBB = {{1, 0}, {0, -1}}`

`Out[140]= {{1, 0}, {0, -1}}`

`In[141]:= ETB = B`

`Out[141]= {{2, 5}, {5, -2}}`

`In[142]:= BTE = Inverse[B]`

`Out[142]= {{2/29, 5/29}, {5/29, -2/29}}`

`In[143]:= ShEE = ETB . ShBB . BTE`

`Out[143]= {{-21/29, 20/29}, {20/29, 21/29}}`

`In[144]:= MatrixForm[ShEE]`

`Out[144]=  $\begin{pmatrix} -\frac{21}{29} & \frac{20}{29} \\ \frac{20}{29} & \frac{21}{29} \end{pmatrix}$`

Schließlich lösen wir noch Beispiel 9.22

`In[145]:= B = Transpose[{-1/Sqrt[5] * {2, 0, 1},`

`1/Sqrt[45] * {-2, 5, 4}, 1/3 * {1, 2, -2}]`

`Out[145]= {{-2/√5, -2/(3√5), 1/3}, {0, √5/3, 2/3}, {-1/√5, 4/(3√5), -2/3}}`

`In[146]:= c = Cos[π/3];`

`s = Sin[π/3];`

`ShBB = {{c, -s, 0}, {s, c, 0}, {0, 0, 1}}`

`Out[146]= {{1/2, -√3/2, 0}, {√3/2, 1/2, 0}, {0, 0, 1}}`

`In[147]:= ETB = B`

`Out[147]= {{-2/√5, -2/(3√5), 1/3}, {0, √5/3, 2/3}, {-1/√5, 4/(3√5), -2/3}}`

`In[148]:= BTE = Inverse[B]`

`Out[148]= {{-2/√5, 0, -1/√5}, {-2/(3√5), √5/3, 4/(3√5)}, {1/3, 2/3, -2/3}}`

`In[149] := ShEE = Simplify [ETB.ShBB.BTE]`

$$\text{Out}[149] = \left\{ \left\{ \frac{5}{9}, \frac{1}{9} + \frac{1}{\sqrt{3}}, -\frac{1}{9} + \frac{1}{\sqrt{3}} \right\}, \left\{ \frac{1}{9} - \frac{1}{\sqrt{3}}, \frac{13}{18}, \frac{1}{18} (-4 - 3\sqrt{3}) \right\}, \right. \\ \left. \left\{ -\frac{1}{9} - \frac{1}{\sqrt{3}}, \frac{1}{18} (-4 + 3\sqrt{3}), \frac{13}{18} \right\} \right\}$$

`In[150] := MatrixForm [N[ShEE, 6]]`

$$\text{Out}[150] = \begin{pmatrix} 0.555556 & 0.688461 & 0.466239 \\ -0.466239 & 0.722222 & -0.510897 \\ -0.688461 & 0.0664529 & 0.722222 \end{pmatrix}$$

### ÜBUNGSAUFGABEN 9.30.

- (1) Finden Sie eine Basis  $B$ , bezüglich der die Spiegelung  $\delta$  an der Ebene  $x + y + z = 0$  die Abbildungsmatrix

$$S_{\delta}(B, B) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

hat.

- (2) Bestimmen Sie eine geeignete Basis  $B$  des  $\mathbb{R}^2$ , für die die Abbildungsmatrix der Spiegelung  $s$  an der Geraden  $g: 7x - 4y$  folgende Form besitzt:

$$S_s(B, B) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

- (3) (Spiegelung an einer Geraden in der Ebene) Wir bezeichnen mit  $\sigma$  jene Spiegelung, die jeden Punkt der Ebene  $\mathbb{R}^2$  an der Geraden  $-3x + 4y = 0$  spiegelt.

- (a) Bestimmen Sie eine Basis  $B$  des  $\mathbb{R}^2$ , sodass für die Abbildungsmatrix  $S_{\sigma}(B, B)$  der Spiegelung  $\sigma$  bezüglich der Basis  $B$  folgende Gleichung gilt.

$$S_{\sigma}(B, B) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

- (b) Berechnen Sie die Abbildungsmatrix  $S_{\sigma}(E, E)$  der Spiegelung  $\sigma$  bezüglich der kanonischen Basis  $E$ .

- (c) Wo landet der Punkt  $(a, b)$  nach dieser Spiegelung  $\sigma$ ?

- (4) Sei  $h$  die lineare Abbildung, die jeden Punkt an der Ebene  $e: x + 2y + 2z = 0$  spiegelt.

- (a) Berechnen Sie  $h(v)$  für  $v \in \left\{ \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} -2 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ -5 \\ 4 \end{pmatrix} \right\}$ .

- (b) Bestimmen Sie die Abbildungsmatrix  $S_h(B, B)$  für die Basis

$$B = \left( \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} -2 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ -5 \\ 4 \end{pmatrix} \right).$$

- (5) Wir betrachten die Abbildung  $\sigma: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ , die jeden Punkt an der  $y$ -Achse spiegelt. Bestimmen Sie die Abbildungsmatrix  $S_{\sigma}(E, E)$  dieser Abbildung bezüglich der kanonischen Basis  $E$ . Testen Sie Ihre Abbildungsmatrix, indem Sie damit das Spiegelbild von  $\begin{pmatrix} 4 \\ -3 \end{pmatrix}$  ausrechnen.

- (6) Geben Sie die Darstellungsmatrix für die Spiegelung an der Ebene  $2x - y + z = 0$  bezüglich der kanonischen Basis  $E$  an. (Sie brauchen die auftretenden inversen Matrizen nicht zu berechnen.)

- (7) (Spiegelung an einer Geraden in der Ebene)

- (a) Wir bezeichnen mit  $\sigma$  jene Spiegelung, die jeden Punkt an der Geraden

$$x + y = 0$$

spiegelt. Wo landet der Punkt  $(a, b)$  nach dieser Spiegelung  $\sigma$ ? Bestimmen Sie die Abbildungsmatrix dieser Spiegelung bezüglich der kanonischen Basis.

- (b) Finden Sie mithilfe einer Skizze, wo der Punkt  $\begin{pmatrix} 1 \\ 4 \end{pmatrix}$  landet, und überprüfen Sie das Ergebnis Ihrer Rechnung anhand der Skizze.

- (8) Sei  $h$  die lineare Abbildung, die jeden Punkt an der Ebene  $e: x + 2y + 2z = 0$  spiegelt. Wir suchen in diesem Beispiel  $S_h(E, E)$ , wobei  $E$  die kanonische Basis des  $\mathbb{R}^3$  ist. Gehen Sie dazu so vor:

- (a) Bestimmen Sie  $S_{\text{id}}(E, B)$ . Dabei ist  $\text{id}$  die identische Abbildung.  $S_{\text{id}}(E, B)$  ist also eine Basistransformationsmatrix, und erfüllt die Eigenschaft  $(v)_B = S_{\text{id}}(E, B) \cdot (v)_E$  für alle  $v \in \mathbb{R}^3$ .

- (b) Bestimmen Sie  $S_{\text{id}}(B, E)$ .

- (c) Bauen Sie aus diesen beiden Matrizen und  $S_h(B, B)$  die Matrix  $S_h(E, E)$  zusammen.



- (9) (Spiegelung an einer Ebene im Raum) Wo landet der Punkt  $\begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathbb{R}^3$  nach der Spiegelung  $\sigma$  an der Ebene  $-2x - y + z = 0$ ?

Bestimmen Sie die Abbildungsmatrix dieser Spiegelung!

- (10) (Spiegelung an einer Geraden in der Ebene) Wir bezeichnen mit  $\sigma$  jene Spiegelung, die jeden Punkt an der Geraden  $12x + 5y = 0$  spiegelt. Wo landet der Punkt  $(a, b)$  nach dieser Spiegelung  $\sigma$ ? Bestimmen Sie die Abbildungsmatrix dieser Spiegelung bezüglich der kanonischen Basis.
- (11) Wir bezeichnen mit  $\sigma$  jene Spiegelung, die jeden Punkt an der Geraden  $15x - 8y = 0$  spiegelt. Wo landet der Punkt  $(a, b)$  nach dieser Spiegelung  $\sigma$ ? Bestimmen Sie die Abbildungsmatrix dieser Spiegelung bezüglich der kanonischen Basis.
- (12) Geben Sie die Darstellungsmatrix für die Spiegelung an der Geraden  $x - 2y = 0$  bezüglich der kanonischen Basis  $E$  an.
- (13) Wo landet der Punkt  $\begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathbb{R}^3$  nach der Drehung  $\delta$  um  $90^\circ$  um die Gerade

$$X = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} + \lambda \cdot \begin{pmatrix} 4 \\ 0 \\ -3 \end{pmatrix}.$$

Bestimmen Sie die Abbildungsmatrix dieser Drehung bezüglich der kanonischen Basis! Wir drehen dabei *gegen den Uhrzeigersinn*, wenn man von  $\begin{pmatrix} 4 \\ 0 \\ -3 \end{pmatrix}$  nach  $\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$  schaut.

- (14) (Drehung um eine Gerade im Raum) Wo landet der Punkt  $\begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathbb{R}^3$  nach der Drehung  $\delta$  um  $90^\circ$  um die Gerade  $g$ , die durch

$$g : X = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} + \lambda \cdot \begin{pmatrix} 12 \\ 0 \\ 5 \end{pmatrix}$$

gegeben ist? Dabei drehen wir *gegen den Uhrzeigersinn*, wenn man von  $\begin{pmatrix} 12 \\ 0 \\ 5 \end{pmatrix}$  in Richtung  $\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$  schaut. Bestimmen Sie die Abbildungsmatrix dieser Drehung bezüglich der kanonischen Basis!



## Der Zusammenhang zwischen linearen Abbildungen und Matrizen

### 1. Faktorräume

DEFINITION 10.1. Sei  $V$  ein Vektorraum über dem Körper  $K$ , und sei  $U$  ein Unterraum von  $V$ , und sei  $w \in V$ . Dann definieren wir

$$w + U := \{w + u \mid u \in U\}$$

und

$$V/U := \{v + U \mid v \in V\}.$$

DEFINITION 10.2. Sei  $V$  ein Vektorraum über dem Körper  $K$ , und sei  $U$  ein Unterraum von  $V$ . Dann definieren wir  $\oplus$  und  $*$  durch

$$(v + U) \oplus (w + U) := (v + w) + U$$

und

$$\alpha * (v + U) := (\alpha v) + U$$

für alle  $v, w \in V$  und  $\alpha \in K$ .

Wir überlegen uns, dass  $\oplus$  und  $*$  wohldefiniert sind, das heißt, dass die Relation  $\{(v + U, w + U), (v + w) + U \mid v, w \in V\}$ , die ja eine Teilmenge von  $(V/U \times V/U) \times V/U$  ist, eine Funktion von  $V/U \times V/U$  nach  $V/U$  ist.

DEFINITION 10.3. Sei  $V$  ein Vektorraum über dem Körper  $K$ , und sei  $U$  ein Unterraum von  $V$ . Dann ist  $\langle V/U, \oplus, \ominus, 0 + U, * \rangle$  ein Vektorraum über  $K$ .

SATZ 10.4. Sei  $V$  ein Vektorraum über dem Körper  $K$ . Seien  $v_1, \dots, v_m \in V$  und  $u_1, \dots, u_n$  in  $U$  so, dass  $(v_1 + U, v_2 + U, \dots, v_m + U)$  eine Basis von  $V/U$  ist und  $(u_1, \dots, u_n)$  eine Basis von  $U$  ist. Dann ist  $B = (v_1, \dots, v_m, u_1, \dots, u_n)$  eine Basis von  $V$ .

*Beweis.* Wir zeigen zunächst, dass  $V \subseteq L(B)$ . Sei dazu  $w \in V$ . Wegen  $w + U \in V/U$  gibt es  $\alpha_1, \dots, \alpha_m \in K$ , sodass

$$\sum_{i=1}^m \alpha_i * (v_i + U) = w + U.$$

Also gilt

$$\left( \sum_{i=1}^m \alpha_i v_i \right) + U = w + U.$$

Es gibt also ein  $u \in U$ , sodass

$$\left(\sum_{i=1}^m \alpha_i v_i\right) + u = w + 0.$$

Da  $u \in U$ , gibt es  $\beta_1, \dots, \beta_n \in K$ , sodass  $u = \sum_{i=1}^n \beta_i u_i$ . Also gilt

$$w = \sum_{i=1}^m \alpha_i v_i + \sum_{i=1}^n \beta_i u_i,$$

und daher  $w \in L(B)$ .

Um zu zeigen, dass  $B$  linear unabhängig ist, wählen wir  $\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_n \in K$  so, dass

$$\sum_{i=1}^m \alpha_i v_i + \sum_{i=1}^n \beta_i u_i = 0.$$

Dann gilt

$$\sum_{i=1}^m \alpha_i v_i \in U,$$

also

$$\sum_{i=1}^m \alpha_i * (v_i + U) = 0 + U.$$

Da  $(v_1 + U, \dots, v_m + U)$  eine Basis von  $V/U$  sind, gilt  $\alpha_1 = \dots = \alpha_m = 0$ . Also gilt  $\sum_{i=1}^n \beta_i u_i = 0$ , und daher sind wegen der linearen Unabhängigkeit von  $(u_1, \dots, u_n)$  auch alle  $\beta_i$  gleich 0. ■

**KOROLLAR 10.5.** Sei  $V$  ein Vektorraum über  $K$ , und sei  $U$  ein endlichdimensionaler Unterraum von  $V$ , sodass  $V/U$  ebenfalls wieder endlichdimensional ist. Dann gilt

$$\dim(V) = \dim(V/U) + \dim U.$$

## 2. Der Homomorphiesatz

**DEFINITION 10.6.** Seien  $U$  und  $V$  Vektorräume über  $K$ . Eine lineare Abbildung  $h : V \rightarrow U$  heißt *Isomorphismus*, wenn  $h$  bijektiv ist. Der Vektorraum  $U$  heißt *isomorph* zu  $V$ , wenn es einen Isomorphismus von  $U$  nach  $V$  gibt.

**SATZ 10.7.** Seien  $U, V$  Vektorräume über  $K$ , und sei  $U$  endlichdimensional. Wenn  $U$  isomorph zu  $V$  ist, dann ist  $V$  endlichdimensional, und es gilt  $\dim(U) = \dim(V)$ .

**SATZ 10.8.** Seien  $V$  und  $W$  Vektorräume, und sei  $h$  eine lineare Abbildung von  $V$  nach  $W$ . Dann ist

$$h(V) = \{h(v) \mid v \in V\}$$

ein Unterraum von  $W$ , und

$$\ker(h) := \{v \in V \mid h(v) = 0\}$$

ein Unterraum von  $V$ .

Diese beiden Unterräume heißen auch *Image* und *Kern* von  $h$ .

**SATZ 10.9 (Homomorphiesatz).** *Seien  $V$  und  $W$  Vektorräume, und sei  $h$  eine lineare Abbildung von  $V$  nach  $W$ . Sei  $U := \ker(h)$ . Dann ist die Abbildung*

$$\begin{aligned} H &: V/U \longrightarrow h(V) \\ v + U &\longmapsto h(v) \end{aligned}$$

*wohldefiniert. Die Abbildung  $H$  ist außerdem ein Isomorphismus von  $V/U$  nach  $h(V)$ .*

Anstelle “Dann ist die Abbildung [...] wohldefiniert” kann man sagen: “Dann ist die Relation  $H = \{(v + U, h(v)) \mid v \in V\}$  eine Funktion von  $V/U$  von  $h(V)$ .”

### 3. Der Rang einer Matrix und ihre Invertierbarkeit

**SATZ 10.10.** *Sei  $A$  eine  $m \times n$ -Matrix, und sei  $h_A : K^n \rightarrow K^m$ ,  $h_A(v) = A \cdot v$  für alle  $v \in K^n$ . Dann gilt:*

- (1) *Das Image von  $h$ , also  $h_A(K^n)$ , ist genau der Spaltenraum  $S(A)$  von  $A$ .*
- (2) *Der Nullraum  $N(A)$  ist genau der Kern  $\ker(h_A)$  von  $h_A$ .*

**SATZ 10.11.** *Sei  $A$  eine  $m \times n$ -Matrix. Dann haben Zeilenraum und Spaltenraum die gleiche Dimension.*

*Beweis.* Wir betrachten die Abbildung  $h_A$ . Wegen des Homomorphiesatzes sind  $K^n/\ker(h_A)$  und  $h_A(K^n)$  isomorph. Also sind  $K^n/N(A)$  und  $S(A)$  isomorph. Es gilt also  $\dim(S(A)) = \dim(K^n/N(A))$ . Da  $S(A)$  endlichdimensional ist, ist auch  $K^n/N(A)$  endlichdimensional. Nach Korollar 10.5 gilt also

$$\dim(K^n) = \dim(K^n/N(A)) + \dim(N(A)),$$

und daher

$$n = \dim(S(A)) + \dim(N(A)).$$

Nach Satz 4.56 gilt  $\dim(N(A)) = n - \dim(Z(A))$ , also

$$n = \dim(S(A)) + n - \dim(Z(A)),$$

und folglich  $\dim(S(A)) = \dim(Z(A))$ . ■

**SATZ 10.12.** *Sei  $m \in \mathbb{N}$ , sei  $K$  ein Körper, und seien  $A, B \in K^{m \times m}$  so, dass  $A \cdot B = E$ . Dann gilt  $B \cdot A = E$ .*

*Beweis.* Sei  $h_A : K^m \rightarrow K^m$ ,  $x \mapsto A \cdot x$  und  $h_B : K^m \rightarrow K^m$ ,  $x \mapsto B \cdot x$ . Dann gilt für alle  $x \in K^m$

$$x = A \cdot B \cdot x = h_A(h_B(x)).$$

Somit gilt  $K^m \subseteq h_A(K^m)$ . Daher hat  $h_A(K^m)$  Dimension  $m$ . Der Kern von  $h_A$  hat nach dem Homomorphiesatz daher Dimension 0. Also ist  $h_A$  injektiv. Für alle  $x \in K^m$  gilt  $h_A(h_B(x)) = x$ . Daher gilt für alle  $y \in K^m$

$$h_A(h_B(h_A(y))) = h_A(y).$$

Da  $h_A$  injektiv ist, gilt daher für alle  $y \in K^m$  auch  $h_B(h_A(y)) = y$ . Also gilt für alle  $y \in K^m$  auch  $B \cdot A \cdot y = y$ . Nach Satz 9.15 gilt also  $B \cdot A = E$ . ■

**SATZ 10.13.** *Sei  $A$  eine  $m \times m$ -Matrix über  $K$ . Äquivalent sind:*

- (1)  $A$  ist invertierbar.
- (2) Die Spaltenvektoren von  $A$  sind linear unabhängig.
- (3) Die Zeilenvektoren von  $A$  sind linear unabhängig.
- (4) Der Rang von  $A$  ist  $m$ .

*Beweis.* (1) $\Rightarrow$ (2): Sei  $B$  die inverse Matrix von  $A$ , und sei  $x$  so, dass  $A \cdot x = 0$ . Dann gilt  $B \cdot A \cdot x = 0$ , also  $x = 0$ . Also sind die Spaltenvektoren von  $A$  linear unabhängig. (2) $\Rightarrow$ (3): Da  $S(A)$  Dimension  $m$  hat, hat nach Satz 10.11 auch  $Z(A)$  die Dimension  $m$ . Wir nehmen an, dass die Zeilenvektoren von  $A$  linear abhängig sind. Dann gibt es eine Zeile, die in der linearen Hülle der anderen Zeilen liegt. Somit gilt wegen Korollar 4.53  $\dim(Z(A)) \leq m - 1$ , ein Widerspruch. (3) $\Rightarrow$ (4): Da die Zeilenvektoren linear unabhängig sind, sind sie eine  $m$ -elementige Basis für  $Z(A)$ . Also hat  $Z(A)$  Dimension  $m$ , und folglich ist der Rang von  $A$  gleich  $m$ . (4) $\Rightarrow$ (1): Da  $\dim(Z(A)) = m$ , gilt auch  $\dim(S(A)) = m$ , und folglich  $\dim(h_A(K^m)) = m$ . Also ist  $h_A$  surjektiv. Nach dem Homomorphiesatz gilt  $\dim(\ker(h_A)) = 0$ , also ist  $h_A$  injektiv. Somit ist  $h_A$  bijektiv. Sei  $f$  die inverse Abbildung, also  $f = \{(h_A(x), x) \mid x \in K^m\}$ . Diese Abbildung ist linear: seien  $u, v \in U$ , und  $\alpha \in K$ . Dann gibt es  $x, y$  mit  $h_A(x) = u$  und  $h_A(y) = v$ . Dann gilt  $h_A(x+y) = u+v$ , und folglich  $f(u+v) = x+y = f(u)+f(v)$ . Ebenso gilt  $h_A(\alpha * x) = \alpha * u$ , und daher  $f(\alpha * u) = \alpha * x = \alpha * f(u)$ . Sei  $B := S_f(E, E)$  die Darstellungsmatrix dieser Abbildung. Dann gilt  $B \cdot A \cdot x = f(h_A(x)) = x$  für alle  $x \in K^m$ . Also gilt  $B \cdot A = E$ . Daher gilt  $A \cdot B = B \cdot A = E$ . ■

## 4. Die Determinante einer quadratischen Matrix

**4.1. Definition der Determinante.** Sei  $A = \begin{pmatrix} -z_1- \\ -z_2- \\ \vdots \\ -z_m- \end{pmatrix}$  eine reelle  $m \times m$ -Matrix. Das von den Zeilen von  $A$  aufgespannte Parallelepiped ist die Teilmenge

$$\left\{ \sum_{i=1}^m \lambda_i \cdot z_i \mid \lambda_1, \dots, \lambda_m \in [0, 1] \right\}.$$

Wir versuchen jetzt das Volumen dieses Parallelepipeds zu messen, und schreiben  $D(z_1, z_2, \dots, z_m)$  für dieses Volumen.

Ohne den Begriff Volumen im  $\mathbb{R}^m$  definiert zu haben, könnte man vermuten, dass eine Funktion  $D : \mathbb{R}^m \times \mathbb{R}^m \times \cdots \times \mathbb{R}^m \rightarrow \mathbb{R}$ , die dieses Volumen misst, folgende Eigenschaften hat. Da wir die Eigenschaften auch für Matrizen über anderen Körpern als  $\mathbb{R}$  benötigen, formulieren wir diese Eigenschaften für einen Körper  $K$ .

(D1) Für alle  $z_1, \dots, z_m, y \in K^m$ ,  $\alpha, \beta \in K$  und  $i \in \{1, \dots, m\}$  gilt

$$\begin{aligned} D(z_1, \dots, z_{i-1}, \alpha * z_i + \beta * y, z_{i+1}, \dots, z_m) \\ = \alpha D(z_1, \dots, z_{i-1}, z_i, z_{i+1}, \dots, z_m) + \beta D(z_1, \dots, z_{i-1}, y, z_{i+1}, \dots, z_m). \end{aligned}$$

(D2) Für alle  $i, j \in \{1, \dots, m\}$  mit  $i \neq j$  gilt

$$\begin{aligned} D(z_1, \dots, z_{i-1}, z_i, z_{i+1}, \dots, z_{j-1}, z_j, z_{j+1}, \dots, z_m) \\ = D(z_1, \dots, z_{i-1}, z_i, z_{i+1}, \dots, z_{j-1}, z_i + z_j, z_{j+1}, \dots, z_m). \end{aligned}$$

(D3) Für die kanonische Basis  $(e_1, \dots, e_m)$  des  $K^n$  gilt

$$D(e_1, \dots, e_m) = 1.$$

#### ÜBUNGSAUFGABEN 10.14.

In den folgenden Übungsbeispielen nehmen wir an, dass  $D$  eine Funktion ist, die die Eigenschaften (D1), (D2) und (D3) erfüllt.

- (1) Zeigen Sie, dass für alle  $z_1, \dots, z_n \in K^m$  gilt:  $D(z_1, z_1, z_3, \dots, z_m) = 0$ .
- (2) Zeigen Sie, dass für alle  $z_1, \dots, z_n \in K^m$  gilt:  $D(z_1, \alpha \cdot z_1 + z_2, z_3, \dots, z_m) = D(z_1, z_2, \dots, z_m)$ .
- (3) Zeigen Sie, dass für alle  $z_1, \dots, z_n \in K^m$  gilt:  $D(z_1, z_2, \dots, z_m) = -D(z_2, z_1, \dots, z_m)$ .

Eine Funktion mit diesen Eigenschaften erhält man mithilfe der *Determinante*. Sei  $f : \{1, 2, \dots, m\} \rightarrow \{1, 2, \dots, m\}$  eine bijektive Abbildung. Wir definieren die *Signatur* von  $f$  durch

$$\text{sgn}(f) := \prod_{\{(i,j) \in \{1, \dots, m\} \times \{1, \dots, m\} \mid i < j\}} \frac{f(i) - f(j)}{i - j}.$$

Die Menge aller bijektiven Abbildungen von  $\{1, \dots, m\}$  nach  $\{1, \dots, m\}$  hat  $m!$  Elemente; wir kürzen sie mit  $S_m$  ab. Für alle  $f, g \in S_m$  gilt  $\text{sgn}(f) \in \{-1, 1\}$  und  $\text{sgn}(f \circ g) = \text{sgn}(f) \cdot \text{sgn}(g)$ , und folglich  $\text{sgn}(f^{-1}) = \text{sgn}(f)$ .

DEFINITION 10.15. Sei  $K$  ein Körper,  $m \in \mathbb{N}$ , und sei  $A \in K^{m \times m}$ . Dann definieren wir die *Determinante* von  $A$  durch

$$\det A := \sum_{f \in S_m} \text{sgn}(f) \prod_{i=1}^m A(i, f(i)).$$

SATZ 10.16. Sei  $K$  ein Körper, sei  $m \in \mathbb{N}$ , sei  $A$  eine  $m \times m$ -Matrix über  $K$ , und sei  $D : K^m \times K^m \times \cdots \times K^m \rightarrow K$  gegeben durch

$$\begin{aligned} D : \quad (K^m)^m &\longrightarrow K \\ (z_1, z_2, \dots, z_m) &\longmapsto \det \begin{pmatrix} -z_1- \\ -z_2- \\ \vdots \\ -z_m- \end{pmatrix}. \end{aligned}$$

Dann erfüllt  $D$  die Eigenschaften (D1), (D2), und (D3).

*Beweisskizze.* (D1) kann man nachrechnen. Für (D2) ist dann ausreichend zu zeigen, dass eine Matrix, in der zwei mal die gleiche Zeile  $z_j$  vorkommt, Determinante 0 hat. Auch (D3) kann man nachrechnen. ■

**SATZ 10.17.** *Sei  $K$  ein Körper, sei  $m \in \mathbb{N}$ , und seien  $A$  und  $B$   $m \times m$ -Matrizen über  $K$ . Dann gilt  $\det(A) = \det(A^T)$  und  $\det(A \cdot B) = \det(A) \cdot \det(B)$ .*

*Beweis.* Zuerst zeigen wir  $\det(A) = \det(A^T)$ . Es gilt

$$\begin{aligned} \det(A^T) &= \sum_{f \in \mathcal{S}_m} \operatorname{sgn}(f) \prod_{i=1}^m A^T(i, f(i)) \\ &= \sum_{f \in \mathcal{S}_m} \operatorname{sgn}(f) \prod_{i=1}^m A(f(i), i) \\ &= \sum_{f \in \mathcal{S}_m} \operatorname{sgn}(f) \prod_{j=1}^m A(j, f^{-1}(j)) \\ &= \sum_{f \in \mathcal{S}_m} \operatorname{sgn}(f^{-1}) \prod_{j=1}^m A(j, f^{-1}(j)) \\ &= \sum_{g \in \mathcal{S}_m} \operatorname{sgn}(g) \prod_{j=1}^m A(j, g(j)). \end{aligned}$$

Nun beweisen wir die zweite Eigenschaft: Seien  $b_1, \dots, b_m$  die Zeilen der Matrix  $B$ . Dann steht in der ersten Zeile des Produkts  $A \cdot B$  der Vektor

$$A(1, 1)b_1 + A(1, 2)b_2 + \dots + A(1, n)b_n.$$

Wenn wir alle  $m$  Zeilen des Produkts ausrechnen, dann sehen wir

$$\begin{aligned} (10.1) \quad \det(A \cdot B) &= \mathbf{D}(A(1, 1)b_1 + A(1, 2)b_2 + \dots + A(1, n)b_n, \\ &\quad A(2, 1)b_1 + A(2, 2)b_2 + \dots + A(2, n)b_n, \\ &\quad \dots \\ &\quad A(m, 1)b_1 + A(m, 2)b_2 + \dots + A(m, n)b_n). \end{aligned}$$

Wir nutzen nun die Linearität der Funktion  $\mathbf{D}$  und erhalten

$$\det(A \cdot B) = \sum_{f: \{1, \dots, m\} \rightarrow \{1, \dots, m\}} \left( \prod_{i=1}^m A(i, f(i)) \right) \cdot \mathbf{D}(b_{f(1)}, b_{f(2)}, \dots, b_{f(m)}).$$

Die Determinante ist 0, wenn zwei Zeilen gleich sind. Daher brauchen wir nur über die bijektiven Funktionen zu summieren und erhalten:

$$\det(A \cdot B) = \sum_{f \in \mathcal{S}_m} \left( \prod_{i=1}^m A(i, f(i)) \right) \cdot \mathbf{D}(b_{f(1)}, b_{f(2)}, \dots, b_{f(m)}).$$



Man kann zeigen, dass für eine Bijektion  $f$  gilt:  $D(b_{f(1)}, b_{f(2)}, \dots, b_{f(m)}) = \text{sgn}(f) \cdot D(b_1, b_2, \dots, b_m)$ . Also erhalten wir

$$\det(A \cdot B) = \sum_{f \in S_m} \left( \prod_{i=1}^m A(i, f(i)) \right) \cdot \text{sgn}(f) \det(B) = \det(B) \cdot \det(A).$$

■

**SATZ 10.18.** Sei  $K$  ein Körper, sei  $m \in \mathbb{N}$ , und sei  $A$  eine  $m \times m$ -Matrix über  $K$ . Dann sind äquivalent:

- (1) Die Zeilen von  $A$  sind linear unabhängig.
- (2)  $\det(A) \neq 0$ .

*Beweis.* (1) $\Rightarrow$ (2): Wenn die Zeilenvektoren von  $A$  linear unabhängig sind, dann ist  $A$  invertierbar. Daher gilt  $\det(A) \det(A^{-1}) = \det(A \cdot A^{-1}) = \det(E) = 1$ . (2) $\Rightarrow$ (1): Wir gehen so vor: Wenn  $z_i$  in der linearen Hülle von  $z_1, \dots, z_{i-1}$  liegt, so kann man die Eigenschaften (D1) und (D2) verwenden, um eine Matrix mit gleicher Determinante und  $i$ -ter Zeile = 0 zu erzeugen. Wegen der Eigenschaft (D1) ist diese Determinante = 0. ■

**4.2. Berechnen der Determinante.** Es ist besonders leicht, die Determinante einer Matrix in Zeilenstaffelform zu berechnen:

**SATZ 10.19.** Sei  $K$  ein Körper, sei  $m \in \mathbb{N}$ , und sei  $A$  eine  $m \times m$ -Matrix über  $K$ , sodass für alle  $i, j$  mit  $i > j$  gilt:  $A(i, j) = 0$ . Dann gilt

$$\det(A) = \prod_{i=1}^m A(i, i).$$

Wir wissen, dass sich jede Matrix durch Zeilenumformungen in Zeilenstaffelnormalform bringen lässt. Dabei ändert sich die Determinante folgendermaßen:

- (1) Wenn wir ein Vielfaches einer Zeile zu einer anderen dazu addieren, bleibt die Determinante unverändert.
- (2) Wenn wir eine Zeile mit einem Körperelement vervielfachen, dann vervielfacht sich die Determinante um eben dieses Körperelement.
- (3) Beim Vertauschen von zwei Zeilen ändert sich das Vorzeichen der Determinante.

Aus diesen Überlegungen erhält man einen Algorithmus zum Berechnen der Determinante. Wir rechnen einige Beispiele.

`In[151] := << RowRed9.m`

`In[152] := DeterminantenDemo [B]`

$$\text{Det} \left[ \begin{pmatrix} 1 & 2 & -3 \\ 2 & 29 & -16 \\ -3 & -16 & 22 \end{pmatrix} \right]$$

Wir addieren das - 2 fache  
der 1. Zeile zum 1 fachen der 2. Zeile.

$$= 1 * 1 * \det \left[ \begin{pmatrix} 1 & 2 & -3 \\ 0 & 25 & -10 \\ -3 & -16 & 22 \end{pmatrix} \right]$$

Wir addieren das 3 fache  
der 1. Zeile zum 1 fachen der 3. Zeile.

$$= 1 * 1 * \det \left[ \begin{pmatrix} 1 & 2 & -3 \\ 0 & 25 & -10 \\ 0 & -10 & 13 \end{pmatrix} \right]$$

Wir addieren das 2 fache  
der 2. Zeile zum 5 fachen der 3. Zeile.

$$= 1 * \frac{1}{5} * \det \left[ \begin{pmatrix} 1 & 2 & -3 \\ 0 & 25 & -10 \\ 0 & 0 & 45 \end{pmatrix} \right]$$

$$= 225$$

$$\text{Out}[152]= 225$$

*In[153]:= DeterminantenDemo [A]*

$$\text{Det} \left[ \begin{pmatrix} 5 & 0 & 0 \\ 3 & 0 & -2 \\ 4 & 1 & 1 \end{pmatrix} \right]$$

Wir addieren das - 3 fache  
der 1. Zeile zum 5 fachen der 2. Zeile.

$$= 1 * \frac{1}{5} * \det \left[ \begin{pmatrix} 5 & 0 & 0 \\ 0 & 0 & -10 \\ 4 & 1 & 1 \end{pmatrix} \right]$$

Wir addieren das - 4 fache  
der 1. Zeile zum 5 fachen der 3. Zeile.

$$= \frac{1}{5} * \frac{1}{5} * \det \left[ \begin{pmatrix} 5 & 0 & 0 \\ 0 & 0 & -10 \\ 0 & 5 & 5 \end{pmatrix} \right]$$

$$= -\frac{1}{25} \det \left[ \begin{pmatrix} 5 & 0 & 0 \\ 0 & 5 & 5 \\ 0 & 0 & -10 \end{pmatrix} \right]$$

$$= 10$$

$$\text{Out}[153]= 10$$

In[154]:= **DeterminantenDemo[B2]**

$$\text{Det} \left[ \begin{pmatrix} 1 & 2 & -3 & 4 \\ 3 & 1 & 3 & 5 \\ 4 & 3 & 0 & 9 \\ 8 & 0 & 0 & 1 \end{pmatrix} \right]$$

Wir addieren das - 3 fache  
der 1. Zeile zum 1 fachen der 2. Zeile.

$$= 1 * 1 * \det \left[ \begin{pmatrix} 1 & 2 & -3 & 4 \\ 0 & -5 & 12 & -7 \\ 4 & 3 & 0 & 9 \\ 8 & 0 & 0 & 1 \end{pmatrix} \right]$$

Wir addieren das - 4 fache  
der 1. Zeile zum 1 fachen der 3. Zeile.

$$= 1 * 1 * \det \left[ \begin{pmatrix} 1 & 2 & -3 & 4 \\ 0 & -5 & 12 & -7 \\ 0 & -5 & 12 & -7 \\ 8 & 0 & 0 & 1 \end{pmatrix} \right]$$

Wir addieren das - 8 fache  
der 1. Zeile zum 1 fachen der 4. Zeile.

$$= 1 * 1 * \det \left[ \begin{pmatrix} 1 & 2 & -3 & 4 \\ 0 & -5 & 12 & -7 \\ 0 & -5 & 12 & -7 \\ 0 & -16 & 24 & -31 \end{pmatrix} \right]$$

Wir addieren das - 1 fache  
der 2. Zeile zum 1 fachen der 3. Zeile.

$$= 1 * 1 * \det \left[ \begin{pmatrix} 1 & 2 & -3 & 4 \\ 0 & -5 & 12 & -7 \\ 0 & 0 & 0 & 0 \\ 0 & -16 & 24 & -31 \end{pmatrix} \right]$$

Wir addieren das - 16 fache  
der 2. Zeile zum 5 fachen der 4. Zeile.

$$= 1 * \frac{1}{5} * \det \left[ \begin{pmatrix} 1 & 2 & -3 & 4 \\ 0 & -5 & 12 & -7 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & -72 & -43 \end{pmatrix} \right]$$

$$= -\frac{1}{5} \det \left[ \begin{pmatrix} 1 & 2 & -3 & 4 \\ 0 & -5 & 12 & -7 \\ 0 & 0 & -72 & -43 \\ 0 & 0 & 0 & 0 \end{pmatrix} \right]$$

= 0

Out[154]= 0

Schließlich berechnen wir noch die Determinante von  $\begin{pmatrix} 0 & 2 & 1 \\ 0 & 0 & 1 \\ 1 & 2 & 3 \end{pmatrix}$

*In[155]* := << **RowRed9.m**

*In[156]* := **M** = {{**0, 2, 1**}, {**0, 0, 1**}, {**1, 2, 3**}}

*Out[156]* = {{**0, 2, 1**}, {**0, 0, 1**}, {**1, 2, 3**}}

*In[157]* := **DeterminantenDemo [M]**

**Det**[  $\begin{pmatrix} 0 & 2 & 1 \\ 0 & 0 & 1 \\ 1 & 2 & 3 \end{pmatrix}$  ]

= -1 **det**[  $\begin{pmatrix} 1 & 2 & 3 \\ 0 & 0 & 1 \\ 0 & 2 & 1 \end{pmatrix}$  ]

= 1 **det**[  $\begin{pmatrix} 1 & 2 & 3 \\ 0 & 2 & 1 \\ 0 & 0 & 1 \end{pmatrix}$  ]

= 2

*Out[157]* = 2

*In[158]* := **Det [M]**

*Out[158]* = 2

## Homogene Koordinaten

### 1. Die projektive Ebene

Sei  $F$  ein Körper. Auf  $F^3 \setminus \left\{ \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \right\}$  definieren wir folgende Äquivalenzrelation  $\approx$ :

$$\begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \approx \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} \text{ genau dann wenn } \exists \lambda \in F : \begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} = \lambda \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix}.$$

Zwei Vektoren in  $F^3 \setminus \{0\}$  sind also äquivalent, wenn einer ein Vielfaches des anderen ist. Wir können auch ein Repräsentantensystem für diese Äquivalenzrelation angeben:

$$R := \left\{ \begin{pmatrix} x \\ y \\ 1 \end{pmatrix} \mid x, y \in F \right\} \cup \left\{ \begin{pmatrix} x \\ 1 \\ 0 \end{pmatrix} \mid x \in F \right\} \cup \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \right\}.$$

DEFINITION 11.1. Sei  $F$  ein Körper, sei  $\approx$  die oben definierte Äquivalenzrelation, und sei  $P := \{v/\approx \mid v \in F^3\}$ . Dann ist  $P$  die *Menge der Punkte der projektiven Ebene*.

Ein Punkt der projektiven Ebene ist also eine ganze Klasse von Vektoren. Die meisten Punkte der projektiven Ebene kann man aber gut veranschaulichen: Wenn  $z \neq 0$ , dann gilt  $\begin{pmatrix} x \\ y \\ z \end{pmatrix}/\approx = \begin{pmatrix} \frac{x}{z} \\ \frac{y}{z} \\ 1 \end{pmatrix}/\approx$ . Diesen Punkt kann man in  $F^2$  als  $\begin{pmatrix} \frac{x}{z} \\ \frac{y}{z} \end{pmatrix}$  zeichnen.

Wir kürzen jetzt den Punkt  $\begin{pmatrix} x \\ y \\ z \end{pmatrix}/\approx$  der projektiven Ebene durch  $(x : y : z)$  ab. Es gilt also, wenn  $z \neq 0$ ,  $(x : y : z) = \left(\frac{x}{z} : \frac{y}{z} : 1\right)$ . Die Punkte mit  $z \neq 0$  bezeichnet man als *affine Punkte* der projektiven Ebene, und den Punkt  $\begin{pmatrix} x \\ y \\ z \end{pmatrix}/\approx$  bezeichnet man als *affines Bild* von  $(x : y : z)$ . Zur Veranschaulichung von  $(x : y : z)$  zeichnet man also das dazugehörige affine Bild.

Seien nun  $a, b, c \in F$  (nicht alle = 0), und sei  $M$  die Menge, die durch

$$M = \{(x : y : z) \in F^3/\approx \mid ax + by + cz = 0\}$$

gegeben ist. Man sieht, dass die affinen Bilder von  $M$  genau die Gerade  $g : ax + by = -c$  sind.

Wir schneiden nun zwei Geraden:

$$\begin{aligned} g_1 &= \{(x : y : z) \in \mathbb{R}^3/\approx \mid 1x - 2y - 3z = 0\}, \\ g_2 &= \{(x : y : z) \in \mathbb{R}^3/\approx \mid 2x - 3y + 1z = 0\}. \end{aligned}$$

Wir erhalten

$$g_1 \cap g_2 = \{(-11 : -7 : 1)\}.$$

Tatsächlich haben auch im  $\mathbb{R}^2$  die Geraden  $x-2y=3$  und  $2x-3y=-1$  den Schnittpunkt  $\begin{pmatrix} -11 \\ -7 \end{pmatrix}$ .

Was passiert, wenn wir zwei parallele Geraden schneiden?

$$\begin{aligned} g_1 &= \{(x : y : z) \in \mathbb{R}^3/\approx \mid 1x - 2y - 3z = 0\}, \\ g_2 &= \{(x : y : z) \in \mathbb{R}^3/\approx \mid 1x - 2y - 4z = 0\}. \end{aligned}$$

Dann gilt

$$g_1 \cap g_2 = \{(2 : 1 : 0)\}.$$

Die beiden Geraden haben in der projektiven Ebene also genau einen Schnittpunkt. Dieser Schnittpunkt hat aber kein affines Bild. Wir stellen uns diesen Punkt als *Fernpunkt in Richtung*  $\begin{pmatrix} 2 \\ 1 \end{pmatrix}$  vor.

## 2. Lineare Abbildungen in der projektiven Ebene

Sei  $s_{(a,b)}$  die Schiebung, die jeden Punkt  $(x, y)$  des  $\mathbb{R}^2$  auf  $(x, y) + (a, b)$  abbildet. Rechnet man mit homogenen Koordinaten, dann sieht man, dass sich die entsprechende Abbildung der projektiven Ebene als

$$s'_{(a,b)}\left(\begin{pmatrix} x \\ y \\ z \end{pmatrix}\right) = \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

schreiben kann. Jetzt lassen sich also auch Schiebungen durch Matrizen ausdrücken. Die Drehung um  $60^\circ$  gegen den Uhrzeigersinn um den Punkt  $(0 : 0 : 0)$  kann man etwa durch

$$d_{60^\circ} = \left(\begin{pmatrix} x \\ y \\ z \end{pmatrix}\right) = \begin{pmatrix} \cos(60^\circ) & -\sin(60^\circ) & 0 \\ \sin(60^\circ) & \cos(60^\circ) & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

beschreiben.

Wir können jetzt auch eine Matrix bestimmen, die jeden affinen Punkt um den Winkel  $\alpha$  gegen den Uhrzeigersinn um den Punkt  $(a, b)$  dreht.

```
In[159]:= Schiebungsmatrix [a_, b_] := {{1, 0, a}, {0, 1, b}, {0, 0, 1}}
```

```
In[160]:= Drehungsmatrix [alpha_] :=
  {{Cos [alpha], - Sin [alpha], 0},
   {Sin [alpha], Cos [alpha], 0}, {0, 0, 1}}
```

```
In[161]:= MatrixForm [Schiebungsmatrix [-a, -b] .
  Drehungsmatrix [alpha] . Schiebungsmatrix [a, b]]
```

```
Out[161]=  $\begin{pmatrix} \cos[\alpha] & -\sin[\alpha] & -a + a \cos[\alpha] - b \sin[\alpha] \\ \sin[\alpha] & \cos[\alpha] & -b + b \cos[\alpha] + a \sin[\alpha] \\ 0 & 0 & 1 \end{pmatrix}$ 
```

Daher landet der Punkt  $(x : y : z)$  nach einer Drehung um  $\alpha$  gegen den Uhrzeigersinn um den Punkt  $(a : b : 1)$  auf dem Punkt

$$D\left(\begin{pmatrix} x \\ y \\ z \end{pmatrix}\right) = \begin{pmatrix} \cos(\alpha) & -\sin(\alpha) & -a + a\cos(\alpha) - b\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) & -b + b\cos(\alpha) + a\sin(\alpha) \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix}.$$

### 3. Der projektive Raum

Wir beschreiben jeden Punkt  $(x, y, z)$  im  $\mathbb{R}^3$  durch die Klasse  $(x : y : z : 1)$ . Der Ausdruck  $(x : y : z : 1)$  beschreibt dabei die Klasse von  $(x, y, z, 1)$  bezüglich der Äquivalenzrelation  $\approx$  auf  $\mathbb{R}^4 \setminus \{(0, 0, 0, 0)\}$ . Diese Äquivalenzrelation ist so gegeben:

$$v \approx w : \Leftrightarrow \exists \lambda \in \mathbb{R} : v = \lambda w$$

für alle  $v, w \in \mathbb{R}^4 \setminus \{(0, 0, 0, 0)\}$ .

Jetzt können wir folgendes Beispiel lösen:

AUFGABE 11.2. Wo landet ein Punkt in  $\mathbb{R}^3$  nach einer Drehung um  $120^\circ$  um die Gerade

$$\left\{ \begin{pmatrix} 2 \\ 3 \\ 4 \end{pmatrix} + t \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \mid t \in \mathbb{R} \right\}.$$

Dabei drehen wir gegen den Uhrzeigersinn, wenn wir vom Punkt  $\begin{pmatrix} 3 \\ 4 \\ 5 \end{pmatrix}$  auf die Ebene  $x + y + z = 2 + 3 + 4$  hinunterschauen.

Wir gehen so vor: Zuerst verschieben wir den Punkt  $(x, y, z)$  um  $(-2, -3, -4)$ , dann drehen wir ihn um die Gerade  $X = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} + t \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$ , dann verschieben wir den Ergebnispunkt um  $(2, 3, 4)$ . Um auch die Schiebung als Matrixmultiplikation schreiben zu können, rechnen wir mit  $(x : y : z : 1)$  anstelle von  $(x, y, z)$ .

`In[162] :=`

`(* Drehmatrix um die Gerade durch (0, 0, 0) und (1, 1, 1) *)`

`In[163] :=`

`n = NullSpace[{1, 1, 1}]`

`Out[163] = {{-1, 0, 1}, {-1, 1, 0}}`

`In[164] := a1 = n[[1]]`

`Out[164] = {-1, 0, 1}`

`In[165] := a3 = {1, 1, 1}`

`Out[165] = {1, 1, 1}`

`In[166] := b1 = a1/Sqrt[a1.a1]`

`Out[166] = {-1/Sqrt[2], 0, 1/Sqrt[2]}`

`In[167] := a2 = Cross[a1, a3]`

```

Out[167]= {-1, 2, -1}

In[168]:= b2 = a2 / Sqrt[a2.a2]
Out[168]= { -1/√6, √(2/3), -1/√6 }

In[169]:= b3 = Cross[b1, b2]
Out[169]= { -1/√3, -1/√3, -1/√3 }

In[170]:= B = Transpose[{b2, b1, b3}]
Out[170]= { { -1/√6, -1/√2, -1/√3 },
             { √(2/3), 0, -1/√3 }, { -1/√6, 1/√2, -1/√3 } }

In[171]:= grad = π / 180
Out[171]= π / 180

In[172]:= ShBB = {{c, -s, 0},
                  {s, c, 0},
                  {0, 0, 1}} /. {s → Sin[120 grad], c → Cos[120 grad]}
Out[172]= { { -1/2, -√3/2, 0 }, { √3/2, -1/2, 0 }, { 0, 0, 1 } }

In[173]:= ShEE = Simplify[B.ShBB.Inverse[B]]
Out[173]= { { 0, 0, 1 }, { 1, 0, 0 }, { 0, 1, 0 } }

In[174]:= MatrixForm[ShEE]
Out[174]= ( 0 0 1
            1 0 0
            0 1 0 )

In[175]:= (* Schiebungsmatrix *)
Schiebung = {{1, 0, 0, 2}, {0, 1, 0, 3}, {0, 0, 1, 4},
             {0, 0, 0, 1}}
Out[175]= {{1, 0, 0, 2}, {0, 1, 0, 3}, {0, 0, 1, 4}, {0, 0, 0, 1}}

In[176]:= (* Drehungsmatrix fuer Homogene Koordinaten *)
(* Initialisieren *)
Drehungsmatrix = ShEE
Out[176]= {{0, 0, 1}, {1, 0, 0}, {0, 1, 0}}

In[177]:= For[i = 1, i ≤ 3, i++,
              Drehungsmatrix[[i]] = Append[Drehungsmatrix[[i]], 0]]

In[178]:= Drehungsmatrix = Append[Drehungsmatrix, {0, 0, 0, 1}]
Out[178]= {{0, 0, 1, 0}, {1, 0, 0, 0}, {0, 1, 0, 0}, {0, 0, 0, 1}}

In[179]:= MatrixForm[Drehungsmatrix]

```



$$\text{Out}[179]= \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

`In[180]:= Drehungsmatrix2 =`

`Schiebung . Drehungsmatrix . Inverse [Schiebung]`

`Out[180]= {{0, 0, 1, -2}, {1, 0, 0, 1}, {0, 1, 0, 1}, {0, 0, 0, 1}}`

`In[181]:= MatrixForm [Drehungsmatrix2]`

$$\text{Out}[181]= \begin{pmatrix} 0 & 0 & 1 & -2 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Die Matrix `Drehungsmatrix2` dreht also den Punkt  $(x : y : z : 1)$ . Der Punkt  $(x, y, z)$  landet also nach dieser Drehung auf dem Punkt  $(-2 + z, 1 + x, 1 + y)$ .

`In[182]:= Drehungsmatrix2 . {x, y, z, 1}`

`Out[182]= {-2 + z, 1 + x, 1 + y, 1}`



## ANHANG A

### **Programme, die vorrechnen**

Die Mathematica-Files `GaussDemo6.m` und `RowRed9.m` enthalten Mathematica-Funktionen, die folgende Probleme mit Zwischenschritten vorrechnen:

- Lösen eines linearen Gleichungssystems (`Gauss[A, b]`).
- Bestimmen einer Matrix in Zeilenstaffelform, die den gleichen Zeilenraum wie die eingegebene Matrix hat (`RowEchelonForm[A]`).
- Bestimmen einer Matrix in Zeilenstaffelnormalform, die den gleichen Zeilenraum wie die eingegebene Matrix hat (`RowEchelonNormalForm[A]`).
- Bestimmen der Determinante einer Matrix (`DeterminantenDemo[A]`).

Die Programme können von Mathematica aus mit `<< GaussDemo6.m` und `<< RowRed9.m` geladen werden.

Sie sind auf <http://www.algebra.uni-linz.ac.at/Students/MathInf/vlws05/MathematicaProgramme/> erhältlich und werden den Studierenden ausschließlich für die Nutzung im Rahmen des Kurses Algebra zur Verfügung gestellt.