Lineare Algebra I

Lösungen zu diversen Aufgaben im Kurs

Raj Dahya
Fakultät für Mathematik und Informatik/Institut für Philosophie
Universität Leipzig.
Wintersemester 2020/2021

Vorwort

Dieses Dokument enthält Lösungsansätze zu den Übungsserien, Selbstkontrollenaufgaben, und Quizzes. Diese werden natürlich *nach* Abgabefristen hochgeladen und dienen *nicht* als Musterlösungen! Der Zweck dieser Lösungen ist es vielmehr, Ansätze zu präsentieren, mit denen man seine *eigenen* Versuche vergleichen kann.

Inhaltsverzeichnis

TEIL I
Übungsserien

Übungsserie 1

Woche 1

ACHTUNG. Diese Lösungen dienen *nicht* als Musterlösungen sondern eher als Referenz. Hier wird eingehender gearbeitet, als generell verlangt wird. Das Hauptziel hier ist, eine Variant anzubieten, gegen die man seine Versuche vergleichen kann.

Aufgabe 1·1

Zu bestimmen ist die Lösungsmenge

$$L_{\alpha,\beta} \quad := \quad \{\mathbf{x} \in \mathbb{R}^n \mid A_\alpha \mathbf{x} = \mathbf{b}_\beta\}$$

für $\alpha, \beta \in \mathbb{R}$, wobei $m = 3$ und $n = 4$, und $A_\alpha \in \mathbb{R}^{m \times n}$ und $\mathbf{b}_\beta \in \mathbb{R}^m$ durch

$$A_\alpha \quad := \quad \begin{pmatrix} 1 & 7 & 2 & -1 \\ 1 & 8 & 6 & -3 \\ 2 & 14 & \alpha & -2 \end{pmatrix} \quad \mathbf{b}_\beta \quad := \quad \begin{pmatrix} 4 \\ 0 \\ \beta \end{pmatrix}$$

gegeben sind. Um die Lösungsmenge zu bestimmen führen wir das Gaußverfahren aus:

Ursprüngliches LGS $(A_\alpha | b_\beta)$:

$$\left(\begin{array}{cccc|c} 1 & 7 & 2 & -1 & 4 \\ 1 & 8 & 6 & -3 & 0 \\ 2 & 14 & \alpha & -2 & \beta \end{array}\right)$$

Wende die Zeilentransformationen

$$\begin{array}{rcl} Z_2 & \rightsquigarrow & Z_2 - Z_1 \\ Z_3 & \rightsquigarrow & Z_3 - 2 \cdot Z_1 \end{array}$$

an:

$$\left(\begin{array}{cccc|c} \boxed{1} & 7 & 2 & -1 & 4 \\ 0 & \boxed{1} & 4 & -2 & -4 \\ 0 & 0 & \boxed{\alpha - 4} & 0 & \beta - 8 \end{array}\right)$$

Die eingezeichneten Einträge markieren die ersten Einträge der Stufen. Es gibt also 2 oder 3 Stufen, je nachdem, ob $\alpha - 4 = 0$. Dies führt zu einem Fallunterschied:

Fall 1. $\alpha - 4 = 0$. Das heißt, $\alpha = 4$. In diesem Falle hat das augmentierte System genau 2 Stufen und sieht wie folgt aus:

$$\left(\begin{array}{cccc|c} \boxed{1} & 7 & 2 & -1 & 4 \\ 0 & \boxed{1} & 4 & -2 & -4 \\ 0 & 0 & 0 & 0 & \beta - 8 \end{array}\right)$$

Dies führt zu zwei weiteren Fällen, denn die 3. Gleichung ist jetzt genau dann lösbar, wenn $\beta - 8 = 0$.

Fall 1a. $\beta - 8 \neq 0$. Das heißt, $\beta \neq 8$. Dann ist die 3. Gleichung und damit das LGS nicht lösbar. Darum erhalten wir $\boxed{L_{\alpha,\beta} = \emptyset}$.

Fall 1b. $\beta-8=0$. Das heißt, $\beta=8$. Dann ist die 3. Gleichung trivialerweise erfüllt. Das augmentierte System sieht wird zum

$$\left(\begin{array}{cccc|c} \boxed{1} & 7 & 2 & -1 & 4 \\ 0 & \boxed{1} & 4 & -2 & -4 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

und kann jetzt aufgelöst werden. Wir arbeiten von unten nach oben:

Aus der ganzen Zeilenstufenform erschließt sich

$$x_3,\ x_4 \text{ sind frei}$$

Aus der Stufenform von Gleichungen 2 und 1 erschließt sich

$$\begin{array}{rcl} x_2 & = & -4-4x_3+2x_4 \\ x_1 & = & 4-7x_2-2x_3+x_4 \\ & = & 4-7(-4-4x_3+2x_4)-2x_3+x_4 \\ & = & 32+26x_3+-13x_4 \end{array}$$

Zusammengefasst erhalten wir die allgemeine Form der Lösung:

$$\begin{array}{rcl} \mathbf{x} & = & \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} \\ & = & \begin{pmatrix} 32+26x_3+-13x_4 \\ -4-4x_3+2x_4 \\ x_3 \\ x_4 \end{pmatrix} \\ & = & \begin{pmatrix} 32+26x_3+-13x_4 \\ -4-4x_3+2x_4 \\ 0+1x_3+0x_4 \\ 0+0x_3+1x_4 \end{pmatrix} \\ & = & \begin{pmatrix} 32 \\ -4 \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 26x_3 \\ -4x_3 \\ 1x_3 \\ 0x_3 \end{pmatrix} + \begin{pmatrix} -13x_4 \\ 2x_4 \\ 1x_4 \\ 1x_4 \end{pmatrix} \\ & = & \begin{pmatrix} 32 \\ -4 \\ 0 \\ 0 \end{pmatrix} + x_3 \cdot \begin{pmatrix} 26 \\ -4 \\ 1 \\ 0 \end{pmatrix} + x_4 \cdot \begin{pmatrix} -13 \\ 2 \\ 1 \\ 1 \end{pmatrix} \end{array}$$

mit x_3, x_4 frei wählbar.

Also erhalten wird in diesem Falle $\boxed{L_{\alpha,\beta} = \left\{ \begin{pmatrix} 32 \\ -4 \\ 0 \\ 0 \end{pmatrix} + t_1 \cdot \begin{pmatrix} 26 \\ -4 \\ 1 \\ 0 \end{pmatrix} + t_2 \cdot \begin{pmatrix} -13 \\ 2 \\ 1 \\ 1 \end{pmatrix} \mid t_1, t_2 \in \mathbb{R} \right\}}$,
oder etwas kompakter formuliert, $L_{\alpha,\beta} = \begin{pmatrix} 32 \\ -4 \\ 0 \\ 0 \end{pmatrix} + \mathsf{Lin}\left\{ \begin{pmatrix} 26 \\ -4 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -13 \\ 2 \\ 1 \\ 1 \end{pmatrix} \right\}$.

Fall 2. $\alpha-4 \neq 0$. Das heißt, $\alpha \neq 4$. In diesem Falle hat das augmentierte System genau 3 Stufen und diesmal ist nur x_4 frei. Man beachte, dass dies im Grunde genau wie Fall 1b ist, nur dass wir zusätzlich Gleichung 3 beachten und x_3 bestimmen müssen.

Aus der Stufenform von Gleichungen 3 ergibt sich

$$x_3 \quad = \quad \frac{\beta-8}{\alpha-4}$$

Der Rest der Lösung des Gleichungssystems verhält sich genau wie im Fall 3b, das heißt

$$\begin{array}{rcl} \mathbf{x} & = & \begin{pmatrix} 32 \\ -4 \\ 0 \\ 0 \end{pmatrix} + x_3 \cdot \begin{pmatrix} 26 \\ -4 \\ 1 \\ 0 \end{pmatrix} + x_4 \cdot \begin{pmatrix} -13 \\ 2 \\ 1 \\ 1 \end{pmatrix} \\ & = & \begin{pmatrix} 32 \\ -4 \\ 0 \\ 0 \end{pmatrix} + \frac{\beta-8}{\alpha-4} \cdot \begin{pmatrix} 26 \\ -4 \\ 1 \\ 0 \end{pmatrix} + x_4 \cdot \begin{pmatrix} -13 \\ 2 \\ 1 \\ 1 \end{pmatrix}, \end{array}$$

wobei x_4 frei wählbar ist.

Also erhalten wird in diesem Falle $\boxed{L_{\alpha,\beta} = \left\{ \begin{pmatrix} 32 \\ -4 \\ 0 \\ 0 \end{pmatrix} + \frac{\beta-8}{\alpha-4} \cdot \begin{pmatrix} 26 \\ -4 \\ 1 \\ 0 \end{pmatrix} + t \cdot \begin{pmatrix} -13 \\ 2 \\ 1 \\ 1 \end{pmatrix} \mid t \in \mathbb{R} \right\}}$, oder etwas kompakter formuliert, $L_{\alpha,\beta} = \begin{pmatrix} 32 \\ -4 \\ 0 \\ 0 \end{pmatrix} + \frac{\beta-8}{\alpha-4} \cdot \begin{pmatrix} 26 \\ -4 \\ 1 \\ 0 \end{pmatrix} + \mathsf{Lin}\left\{ \begin{pmatrix} -13 \\ 2 \\ 1 \\ 1 \end{pmatrix} \right\}$.

Wir fassen die Lösung für alle Fälle zusammen:

$$L_{\alpha,\beta} \quad = \quad \begin{cases} \emptyset & : \quad \alpha = 4,\ \beta \neq 8 \\ \mathbf{u} + \mathsf{Lin}\{\mathbf{v}, \mathbf{w}\} & : \quad \alpha = 4,\ \beta = 8 \\ \mathbf{u} + \frac{\alpha-4}{\beta-8}\mathbf{v} + \mathsf{Lin}\{\mathbf{w}\} & : \quad \alpha \neq 4 \end{cases}$$

für alle $\alpha, \beta \in \mathbb{R}$, wobei $\mathbf{u} = \begin{pmatrix} 32 \\ -4 \\ 0 \\ 0 \end{pmatrix}$, $\mathbf{v} = \begin{pmatrix} 26 \\ -4 \\ 1 \\ 0 \end{pmatrix}$, $\mathbf{w} = \begin{pmatrix} -13 \\ 2 \\ 1 \\ 1 \end{pmatrix}$.

Aufgabe 1·2

Satz 1·1 *Angewandt auf die erweiterte Koeffizientenmatrix eines linearen Gleichungssystems verändern die elementaren Zeilenumformungen vom Typ (I), (II) und (III) die Menge der Lösungen nicht.* ◊

Wir beweisen Satz 1·1 mithilfe der folgenden Teilergebnisse.

Lemma 1·2 *Seien $m, n \in \mathbb{N}$ und $A \in \mathbb{R}^{m\times n}$ und $\mathbf{b} \in \mathbb{R}^m$. Für $i, j \in \{1, 2, \ldots, m\}$ mit $i \neq j$ bezeichne mit*

$$(A|\mathbf{b}) \quad \overset{I;i,j}{\rightsquigarrow} \quad (A'|\mathbf{b}')$$

die Anwendung von Zeilentransformation (I) auf $(A|\mathbf{b})$, wobei Zeile$_i$ und Zeile$_j$ umgetauscht werden, was in $(A'|\mathbf{b}')$ resultiert. Dann für alle $\mathbf{x} \in \mathbb{R}^n$, falls $\mathbf{x}$ eine Lösung für $(A|\mathbf{b})$ ist, dann ist $\mathbf{x}$ eine Lösung für $(A'|\mathbf{b}')$. ◊

Beweis. Betrachte den Fall $i < j$. Es gilt

$\mathbf{x}$ eine Lösung für $(A|\mathbf{b})$

$$\Longrightarrow \quad \begin{cases} & (a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n = b_1) \\ \text{und} & (a_{2,1}x_1 + a_{2,2}x_2 + \cdots + a_{2,n}x_n = b_2) \\ & \cdots \\ \text{und} & (a_{i,1}x_1 + a_{i,2}x_2 + \cdots + a_{i,n}x_n = b_i) \\ & \cdots \\ \text{und} & (a_{j,1}x_1 + a_{j,2}x_2 + \cdots + a_{j,n}x_n = b_j) \\ & \cdots \\ \text{und} & (a_{m,1}x_1 + a_{m,2}x_2 + \cdots + a_{m,n}x_n = b_m) \end{cases}$$

$$\Longrightarrow \quad \begin{cases} & (a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n = b_1) \\ \text{und} & (a_{2,1}x_1 + a_{2,2}x_2 + \cdots + a_{2,n}x_n = b_2) \\ & \cdots \\ \text{und} & (a_{j,1}x_1 + a_{j,2}x_2 + \cdots + a_{j,n}x_n = b_j) \\ & \cdots \\ \text{und} & (a_{i,1}x_1 + a_{i,2}x_2 + \cdots + a_{i,n}x_n = b_i) \\ & \cdots \\ \text{und} & (a_{m,1}x_1 + a_{m,2}x_2 + \cdots + a_{m,n}x_n = b_m) \end{cases}$$

da lediglich zwei Aussagen in einer Konjunktion umgetauscht werden

$\Longrightarrow$ $\mathbf{x}$ eine Lösung für $(A'|\mathbf{b})'$, da $(A|\mathbf{b}) \overset{I;i,j}{\rightsquigarrow} (A'|\mathbf{b}')$.

Der Fall $i > j$ lässt sich analog zeigen. Falls $i = j$ bleibt das System unverändert, sodass die Behauptung trivialerweise gilt. ■

Lemma 1·3 *Seien $m, n \in \mathbb{N}$ und $A \in \mathbb{R}^{m\times n}$ und $\mathbf{b} \in \mathbb{R}^m$. Für $i \in \{1, 2, \ldots, m\}$ und $\alpha \in \mathbb{R} \setminus \{0\}$ bezeichne mit*

$$(A|\mathbf{b}) \quad \overset{II;i,\alpha}{\rightsquigarrow} \quad (A'|\mathbf{b}')$$

die Anwendung von Zeilentransformation (II) auf $(A|\mathbf{b})$, wobei Zeile$_i$ durch α·Zeile$_i$ ersetzt wird, was in $(A'|\mathbf{b}')$ resultiert. Dann für alle $\mathbf{x} \in \mathbb{R}^n$, falls $\mathbf{x}$ eine Lösung für $(A|\mathbf{b})$ ist, dann ist $\mathbf{x}$ eine Lösung für $(A'|\mathbf{b}')$. ◊

Beweis. Es gilt

$\mathbf{x}$ eine Lösung für $(A|\mathbf{b})$

$$\Longrightarrow \quad \left\{ \begin{array}{lrcl} & (a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n &=& b_1) \\ \text{und} & (a_{2,1}x_1 + a_{2,2}x_2 + \cdots + a_{2,n}x_n &=& b_2) \\ \cdots & & & \\ \text{und} & (a_{i,1}x_1 + a_{i,2}x_2 + \cdots + a_{i,n}x_n &=& b_i) \\ \cdots & & & \\ \text{und} & (a_{m,1}x_1 + a_{m,2}x_2 + \cdots + a_{m,n}x_n &=& b_m) \end{array} \right.$$

$$\Longrightarrow \quad \left\{ \begin{array}{lrcl} & (a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n &=& b_1) \\ \text{und} & (a_{2,1}x_1 + a_{2,2}x_2 + \cdots + a_{2,n}x_n &=& b_2) \\ \cdots & & & \\ \text{und} & (\alpha \cdot (a_{i,1}x_1 + a_{i,2}x_2 + \cdots + a_{i,n}x_n) &=& \alpha \cdot b_i) \\ \cdots & & & \\ \text{und} & (a_{m,1}x_1 + a_{m,2}x_2 + \cdots + a_{m,n}x_n &=& b_m) \end{array} \right.$$

$$\Longrightarrow \quad \left\{ \begin{array}{lrcl} & (a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n &=& b_1) \\ \text{und} & (a_{2,1}x_1 + a_{2,2}x_2 + \cdots + a_{2,n}x_n &=& b_2) \\ \cdots & & & \\ \text{und} & (\alpha \cdot a_{i,1}x_1 + \alpha \cdot a_{i,2}x_2 + \cdots + \alpha \cdot a_{i,n}x_n &=& \alpha \cdot b_i) \\ \cdots & & & \\ \text{und} & (a_{m,1}x_1 + a_{m,2}x_2 + \cdots + a_{m,n}x_n &=& b_m) \end{array} \right.$$

$\mathbf{x}$ eine Lösung für $(A'|\mathbf{b})'$, da $(A|\mathbf{b}) \overset{III;i,\alpha}{\rightsquigarrow} (A'|\mathbf{b}')$.

Also gilt die Behauptung. ■

Lemma 1·4 *Seien $m, n \in \mathbb{N}$ und $A \in \mathbb{R}^{m\times n}$ und $\mathbf{b} \in \mathbb{R}^m$. Für $i, j \in \{1, 2, \ldots, m\}$ mit $i \neq j$ und $\alpha \in \mathbb{R}$ bezeichne mit*

$$(A|\mathbf{b}) \quad \overset{III;i,j,\alpha}{\rightsquigarrow} \quad (A'|\mathbf{b}')$$

die Anwendung von Zeilentransformation (III) auf $(A|\mathbf{b})$, wobei Zeile$_i$ durch die Addition von Zeile$_i$ mit α·Zeile$_j$ ersetzt wird, was in $(A'|\mathbf{b}')$ resultiert. Dann für alle $\mathbf{x} \in \mathbb{R}^n$, falls $\mathbf{x}$ eine Lösung für $(A|\mathbf{b})$ ist, dann ist $\mathbf{x}$ eine Lösung für $(A'|\mathbf{b}')$. ◊

Beweis. Es gilt

$\mathbf{x}$ eine Lösung für $(A|\mathbf{b})$

$$\Longrightarrow \quad \left\{ \begin{array}{lrcl} & (a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n &=& b_1) \\ \text{und} & (a_{2,1}x_1 + a_{2,2}x_2 + \cdots + a_{2,n}x_n &=& b_2) \\ \cdots & & & \\ \text{und} & (a_{i,1}x_1 + a_{i,2}x_2 + \cdots + a_{i,n}x_n &=& b_i) \\ \cdots & & & \\ \text{und} & (a_{m,1}x_1 + a_{m,2}x_2 + \cdots + a_{m,n}x_n &=& b_m) \end{array} \right.$$

$$\Longrightarrow \quad \left\{ \begin{array}{lrcl} & (a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n &=& b_1) \\ \text{und} & (a_{2,1}x_1 + a_{2,2}x_2 + \cdots + a_{2,n}x_n &=& b_2) \\ \cdots & & & \\ \text{und} & (a_{i,1}x_1 + a_{i,2}x_2 + \cdots + a_{i,n}x_n + \alpha \cdot b_j &=& b_i + \alpha \cdot b_j) \\ \cdots & & & \\ \text{und} & (a_{m,1}x_1 + a_{m,2}x_2 + \cdots + a_{m,n}x_n &=& b_m) \end{array} \right.$$

$$\Longrightarrow \quad \left\{ \begin{array}{lrcl} & (a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n &=& b_1) \\ \text{und} & (a_{2,1}x_1 + a_{2,2}x_2 + \cdots + a_{2,n}x_n &=& b_2) \\ \cdots & & & \\ \text{und} & (a_{i,1}x_1 + a_{i,2}x_2 + \cdots + a_{i,n}x_n & & \\ & +\alpha \cdot a_{j,1}x_1 + \alpha \cdot a_{j,2}x_2 + \cdots + \alpha \cdot a_{j,n}x_n &=& b_i + \alpha \cdot b_j) \\ \cdots & & & \\ \text{und} & (a_{m,1}x_1 + a_{m,2}x_2 + \cdots + a_{m,n}x_n &=& b_m) \end{array} \right.$$

da laut der j-ten Gleichung gilt $b_j = \sum_{k=1}^{m} a_{j,k}x_k$

$$\Longrightarrow \quad \left\{ \begin{array}{lrcl} & (a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n &=& b_1) \\ \text{und} & (a_{2,1}x_1 + a_{2,2}x_2 + \cdots + a_{2,n}x_n &=& b_2) \\ \cdots & & & \\ \text{und} & (a'_{i,1}x_1 + a'_{i,2}x_2 + \cdots + a'_{i,n}x_n &=& b'_i) \\ \cdots & & & \\ \text{und} & (a_{m,1}x_1 + a_{m,2}x_2 + \cdots + a_{m,n}x_n &=& b_m), \end{array} \right.$$

wobei $a'_{i,k} = a_{i,k} + \alpha \cdot a_{j,k}$ für alle k und $b'_i = b_i + \alpha \cdot b_j$

$\Longrightarrow$ $\mathbf{x}$ eine Lösung für $(A'|\mathbf{b})'$, da $(A|\mathbf{b}) \overset{III;i,j,\alpha}{\rightsquigarrow} (A'|\mathbf{b}')$.

Also gilt die Behauptung. ■

Endlich können wir Satz 1·1 beweisen:

Beweis (von Satz 1·1). Seien $m, n \in \mathbb{N}$ und $A \in \mathbb{R}^{m\times n}$ und $\mathbf{b} \in \mathbb{R}^m$. Seien $A' \in \mathbb{R}^{m\times n}$ und $\mathbf{b}' \in \mathbb{R}^m$, so dass $(A|\mathbf{b})$ durch eine Transformation der Art (I), (II) oder (III) aus $(A|\mathbf{b})$ entsteht. Das heißt, entweder

$$\begin{array}{rll} & (A|\mathbf{b}) & \overset{I;i,j}{\rightsquigarrow} \quad (A'|\mathbf{b}') \\ \text{oder} & (A|\mathbf{b}) & \overset{I;i,\alpha}{\rightsquigarrow} \quad (A'|\mathbf{b}') \\ \text{oder} & (A|\mathbf{b}) & \overset{III;i,j,\alpha}{\rightsquigarrow} \quad (A'|\mathbf{b}') \end{array} \tag{1·1}$$

gilt, für ein $i, j \in \{1, 2, \ldots, m\}$ mit $i \neq j$ und $\alpha \in \mathbb{R} \setminus \{0\}$.
Zu zeigen:

$$\{\mathbf{x} \in \mathbb{R}^n \mid \mathbf{x} \text{ eine Lösung für } (A|\mathbf{b})\} \quad = \quad \{\mathbf{x} \in \mathbb{R}^n \mid \mathbf{x} \text{ eine Lösung für } (A|\mathbf{b})\}. \tag{1·2}$$

Wir zeigen dies in zwei Teile:

(⊆.)
Sei $\mathbf{x} \in \mathbb{R}^n$ ein beliebiges Element aus der linken Menge, d. h. $\mathbf{x}$ ist eine Lösung zu $(A|\mathbf{b})$. Laut Lemma 1·2 + Lemma 1·3 + Lemma 1·4 und wegen (1·1) erhalten wir, dass $\mathbf{x}$ eine Lösung zu $(A'|\mathbf{b}')$ ist, d. h. $\mathbf{x}$ liegt in der rechten Menge. Also ist die linke Menge in der rechten enthalten.

(⊇.)
Man beachte zuerst, dass sich die Transformation in (1·1) umkehren lässt— und zwar durch Elementartransformationen. Es ist einfach zu sehen, dass entweder

$$\begin{array}{rll} & (A'|\mathbf{b}') & \overset{I;i,j}{\rightsquigarrow} \quad (A|\mathbf{b}) \\ \text{oder} & (A'|\mathbf{b}') & \overset{I;i,\alpha^{-1}}{\rightsquigarrow} \quad (A|\mathbf{b}) \\ \text{oder} & (A'|\mathbf{b}') & \overset{III;i,j,-\alpha}{\rightsquigarrow} \quad (A|\mathbf{b}). \end{array}$$

Die Situation ist also analog zum ⊆-Teil. Darum gilt die ⊇-Inklusion in (1·2). ■

Aufgabe 1·3

Für diese Aufgabe wird das Konzept der *linearen Unabhängigkeit* aus Kapitel 5 angewandt.

Definition 1·5 Seien $m, n \in \mathbb{N}$ mit $m > n$ und seien $A \in \mathbb{R}^{m\times n}$, $\mathbf{b} \in \mathbb{R}^m$, und $I \subseteq \{1, 2, \ldots, m\}$. Bezeichne mit $(A|\mathbf{b})_I$ die erweiterte Koeffizientenmatrix $(A|\mathbf{b})$, die auf die Zeilen mit Indexes aus I (in bspw. aufsteigender Reihenfolge) reduziert ist. ◊

Beipsiel 1·6 Für $(A|\mathbf{b})$ gleich

$$\left(\begin{array}{ccc|c} -5 & 0 & 0 & -7 \\ 4 & -6 & -10 & 6 \\ -2 & -6 & -6 & 9 \\ -7 & 4 & -1 & -5 \\ 4 & -5 & 2 & -9 \\ -5 & 8 & -7 & -5 \end{array}\right)$$

und $I = \{2, 5, 6\}$ ist $(A|\mathbf{b})_I$ gleich

$$\left(\begin{array}{ccc|c} 4 & -6 & -10 & 6 \\ 4 & -5 & 2 & -9 \\ -5 & 8 & -7 & -5 \end{array}\right).$$

◊

Mit diesem Mittel können wir nun die Hauptaussage in der Aufgabe formulieren:

Satz 1·7 *Seien $m, n \in \mathbb{N}$ mit $m > n$ und seien $A \in \mathbb{R}^{m\times n}$ und $\mathbf{b} \in \mathbb{R}^m$. Falls $(A|\mathbf{b})$ unlösbar ist, dann existiert $I \subseteq \{1, 2, \ldots, m\}$ mit $|I| = n + 1$, so dass $(A|\mathbf{b})_I$ unlösbar ist.* ◊

Beweis. Es stehen nun die *Zeilen* der Matrix A im Fokus. Wir verwandeln diese in Vektoren, d. h. setze

$$\mathbf{z}^{(i)} \in \mathbb{R}^n \text{ die } i\text{-te Zeile von } A \text{ als Vektor geschrieben}$$

für $i \in \{1, 2, \ldots, m\}$. Da $\mathbf{z}^{(1)}, \mathbf{z}^{(2)}, \ldots, \mathbf{z}^{(m)} \in \mathbb{R}^n$, können wir eine *maximale Menge* $I_0 \subseteq \{1, 2, \ldots, m\}$ finden, so dass $(\mathbf{z}^{(i)})_{i\in I_0}$ aus linear unabhängigen Vektoren besteht. Wegen der Dimension von $\mathbb{R}^n$ gilt $|I| \leqslant \min\{m, n\} = n$. Sei $k \in \{1, 2, \ldots, m\} \setminus I_0$ beliebig. Wegen Maximalität muss $(\mathbf{z}^{(i)})_{i\in I_0\cup\{k\}}$ *linear abhängig* sein. Und wegen der linearen Unabhängigkeit von $(\mathbf{z}^{(i)})_{i\in I_0}$ existieren (eindeutige) Koeffizienten $c_{k,i} \in \mathbb{R}$ für $i \in I_0$ so dass

$$\mathbf{z}^{(k)} \quad = \quad \textstyle\sum_{i\in I_0:}\ c_{k,i}\mathbf{z}^{(i)} \tag{1·3}$$

gilt.

Um nun die Hauptaussage zu zeigen, nehmen wir an, dass $(A|\mathbf{b})$ unlösbar ist. **Zu zeigen:** Es gibt eine Teilmenge $I \subseteq \{1, 2, \ldots, m\}$ mit $|I| = n + 1$, so dass $(A|\mathbf{b})_I$ unlösbar ist. Angenommen, dies sei nicht der Fall. Aus dieser Annahme leiten wir folgende Behauptungen ab:

Behauptung 1. Die Verhältnisse zwischen den Zeilenvektoren in (1·3) gelten auch für die Einträge aus $\mathbf{b}$. Das heißt

$$b_k \quad = \quad \textstyle\sum_{i\in I_0:}\ c_{k,i}b_i \tag{1·4}$$

für alle $k \in \{1, 2, \ldots, m + 1\} \setminus I_0$.

Bew. Sei $k \in \{1, 2, \ldots, m + 1\} \setminus I_0$ beliebig. Da $|I_0| \leqslant n < n + 1$ lässt sich eine Teilmenge $I \subseteq \{1, 2, \ldots, m\}$ wählen, mit $I \supseteq I_0 \cup \{k\}$ und $|I| = n + 1$. Dann per *Annahme* ist $(A|\mathbf{b})_I$ lösbar. Das heißt, $\mathbf{x} \in \mathbb{R}^n$ existiert, so dass

$$b_i \quad = \quad \textstyle\sum_{j=1}^{n} a_{i,j}x_j \tag{1·5}$$

für alle $i \in I$ gilt. Da $k \in I$ und $I_0 \subseteq I$ und wegen (1·3) erhalten wir nun das Verhältnis

$$\begin{array}{rcl} b_k & = & \sum_{j=1}^{n} a_{k,j}x_j \\ & = & \sum_{j=1}^{n} (\mathbf{z}^{(k)})_j x_j \\ & & \quad \text{da die Einträge der } k\text{-ten Zeile den Einträgen von } \mathbf{z}^{(k)} \text{ entsprechen} \\ & \overset{(1·3)}{=} & \sum_{j=1}^{n} (\sum_{i\in I_0} c_{k,i}\mathbf{z}^{(i)})_j x_j \\ & = & \sum_{j=1}^{n} \sum_{i\in I_0} c_{k,i} z_j^{(i)} x_j \end{array}$$

$$
\begin{array}{rl}
= & \sum_{i\in I_0} c_{k,i} \sum_{j=1}^{n} z_j^{(i)} x_j \\
= & \sum_{i\in I_0} c_{k,i} \sum_{j=1}^{n} a_{i,j} x_j \\
& \quad \text{da die Einträge der } i\text{-ten Zeile den Einträgen von } \mathbf{z}^{(i)} \text{ entsprechen} \\
\overset{(1\cdot5)}{=} & \sum_{i\in I_0} c_{k,i} b_i .
\end{array}
$$

Darum gilt die Behauptung. ⊣ **(Beh. 1)**

Behauptung 2. Es gibt eine Lösung zu $(A|\mathbf{b})$.

Bew. Da $|I_0| \leqslant n < n+1$ lässt sich eine Teilmenge $I \subseteq \{1, 2, \ldots, m\}$ wählen, so dass $I \supseteq I_0$ und $|I| = n+1$. Dann per *Annahme* ist $(A|\mathbf{b})_I$ lösbar. Das heißt, ein $\mathbf{x} \in \mathbb{R}^n$ existiert, so dass

$$b_i \quad = \quad \sum_{j=1}^{n} a_{i,j} x_j \tag{1·6}$$

für alle $i \in I$ gilt. Da $I \supseteq I_0$ können wir **Behauptung 1** und die Verhältnisse in (1·3) anwenden. Für jedes $k \in \{1, 2, \ldots, m\} \setminus I$ gilt

$$
\begin{array}{rl}
\sum_{j=1}^{n} a_{k,j} x_j \quad = & \sum_{j=1}^{n} (\mathbf{z}^{(k)})_j x_j \\
& \quad \text{da die Einträge der } k\text{-ten Zeile den Einträgen von } \mathbf{z}^{(k)} \text{ entsprechen} \\
\overset{(1\cdot3)}{=} & \sum_{j=1}^{n} (\sum_{i\in I_0} c_{k,i} \mathbf{z}^{(i)})_j x_j \\
= & \sum_{j=1}^{n} \sum_{i\in I_0} c_{k,i} z_j^{(i)} x_j \\
= & \sum_{i\in I_0} c_{k,i} \sum_{j=1}^{n} z_j^{(i)} x_j \\
= & \sum_{i\in I_0} c_{k,i} \sum_{j=1}^{n} a_{i,j} x_j \\
& \quad \text{da die Einträge der } i\text{-ten Zeile den Einträgen von } \mathbf{z}^{(i)} \text{ entsprechen} \\
\overset{(1\cdot6)}{=} & \sum_{i\in I_0} c_{k,i} b_i \\
\overset{\text{Beh. 1}}{=} & b_k
\end{array}
$$

Also ist $\mathbf{x} \in \mathbb{R}^n$ nicht nur eine Lösung zu Zeile i des LGS, $(A|\mathbf{b})$, für jedes $i \in I$, sondern auch für jedes $i \in \{1, 2, \ldots, m\} \setminus I$. Das heißt, $\mathbf{x}$ ist eine Lösung des LGS $(A|\mathbf{b})$. Also ist $(A|\mathbf{b})$ lösbar. ⊣ **(Beh. 2)**

Laut **Behauptung 2** ist also $(A|\mathbf{b})$ lösbar. Dies ist aber ein Widerspruch! Darum stimmt die *Annahme* oben nicht. Also gibt es *doch* eine Teilmenge $I \subseteq \{1, 2, \ldots, m\}$ mit $|I| = n+1$, so dass $(A|\mathbf{b})_I$ unlösbar ist. Damit wurde die zu zeigende Implikation bewiesen. ■ **(Satz 1·7)**

Bemerkung 1·8 Falls man sich aber auf rudimentäre Mitteln beschränken will, kann man alternativ wie folgt vorgehen. Man wende zuerst das Gaußverfahren an und erhalte somit eine Folge

$$(A^{(0)}|\mathbf{b}^{(0)}) \quad \rightsquigarrow \quad (A^{(1)}|\mathbf{b}^{(1)}) \quad \rightsquigarrow \quad (A^{(2)}|\mathbf{b}^{(2)}) \quad \rightsquigarrow \quad \cdots \quad \rightsquigarrow \quad (A^{(N)}|\mathbf{b}^{(N)})$$

wobei $N \in \mathbb{N}$, $A^{(0)} = A$, $\mathbf{b}^{(0)} = \mathbf{b}$, $(A^{(N)}|\mathbf{b}^{(N)})$ eine erweiterte Koeffizientenmatrix in Zeilenstufenform ist, und jede der »$\rightsquigarrow$« Übergänge jeweils eine Transformation der Art (I), (II), oder (III) bezeichnet. Da $m > n$ sieht nun die Zeilenstufenform, also $(A^{(N)}|\mathbf{b}^{(N)})$, folgendermaßen aus:

$$
\left(\begin{array}{ccccccccc|c}
\underbrace{0\,0\,\ldots\,0}_{\ell_1} & \gamma_1 & \cdots\cdots & * & \cdots\cdots & \cdots\cdots & * & \cdots\cdots & b_1^{(N)} \\
0\,0\,\ldots\,0 & 0 & \underbrace{0\,0\,\ldots\,0}_{\ell_2} & \gamma_2 & \cdots\cdots & \cdots\cdots & * & \cdots\cdots & b_2^{(N)} \\
\vdots & & & & & & & \vdots & \\
0\,0\,\ldots\,0 & 0 & 0\,0\,\ldots\,0 & 0 & \cdots\cdots & \underbrace{0\,0\,\ldots\,0}_{\ell_r} & \gamma_r & \cdots\cdots & b_r^{(N)} \\
0\,0\,\ldots\,0 & 0 & 0\,0\,\ldots\,0 & 0 & \cdots\cdots & 0\,0\,\ldots\,0 & 0 & \cdots\cdots & b_{r+1}^{(N)} \\
\vdots & & & & & & & \vdots & \\
0\,0\,\ldots\,0 & 0 & 0\,0\,\ldots\,0 & 0 & \cdots\cdots & 0\,0\,\ldots\,0 & 0 & \cdots\cdots & b_m^{(N)}
\end{array}\right)
$$

wobei $r \in \mathbb{N}_0$ die Anzahl der Stufen ist, $\ell_1, \ell_2, \ldots, \ell_r \in \mathbb{N}_0$, und $\gamma_1, \gamma_2, \ldots, \gamma_r \in \mathbb{R} \setminus \{0\}$ die Hauptkoeffizienten der Stufen sind. Es muss nun $0 \leqslant r \leqslant \min\{m, n\} = n$ gelten.

Jetzt kann man leicht dafür argumentiere, dass (1) die Zeilenstufenform, $(A^{(N)}|\mathbf{b}^{(N)})$, die Implikation erfüllt. Dann aufgrund der Umkehrbarkeit der Elementartransformationen, reicht es aus zu zeigen, dass (2): wenn $(A', \mathbf{b}') \rightsquigarrow (A'', \mathbf{b}'')$ und wenn $(A', \mathbf{b}')$ die Implikation erfüllt, dann erfüllt $(A'', \mathbf{b}'')$ die Implikation. Dies ist nur etwas mühseliger und die Argumentation von (2) führt letzten Endes zu ähnlichen Ideen, die im Beweis oben vorkommen. ◊

Übungsserie 2

Woche 2

ACHTUNG. Diese Lösungen dienen *nicht* als Musterlösungen sondern eher als Referenz. Hier wird eingehender gearbeitet, als generell verlangt wird. Das Hauptziel hier ist, eine Variant anzubieten, gegen die man seine Versuche vergleichen kann.

Aufgabe 2·1

Satz 2·1 (vgl. [Sin20, Korollar 1.3.3]). *Sei V ein Vektorraum über $\mathbb{R}$ wie $\mathbb{R}^n$ für ein $n \in \mathbb{N}$. Seien $\mathbf{v}, \mathbf{w} \in V$ mit $\mathbf{v} \neq \mathbf{w}$ und $\mathbf{w} \neq \mathbf{0}$ und sei*

$$L \quad := \quad \{s\mathbf{v} + (1-s)\mathbf{w} \mid s \in \mathbb{R}\}$$

die Verbindungsgerade zw. $\mathbf{v}$ und $\mathbf{w}$. Dann gilt $\mathbf{0} \in L \Leftrightarrow \exists c \in \mathbb{R} : \mathbf{v} = c\mathbf{w}$. ◊

Beweis. Der Beweis wird in zwei Teilen gezeigt.

($\Longrightarrow$). Angenommen, $\mathbf{0} \in L$. **Zu zeigen:** $\exists c \in \mathbb{R} : \mathbf{v} = c\mathbf{w}$.
Per Definition von L existiert ein $s \in \mathbb{R}$, so dass sich $\mathbf{0}$ als $\mathbf{0} = s\mathbf{v} + (1-s)\mathbf{w}$ darstellen lässt. Daraus lässt sich ableiten:

$$\begin{aligned}
\mathbf{0} = s\mathbf{v} + (1-s)\mathbf{w} \quad &\Longleftrightarrow \quad s\mathbf{v} = (s-1)\mathbf{w} \\
&\Longleftrightarrow \quad \underbrace{(s = 0 \text{ und } \mathbf{w} = s(\mathbf{w}-\mathbf{v}) = \mathbf{0})}_{\text{unmöglich, da } \mathbf{w} \neq \mathbf{0} \text{ per Voraussetzung}} \text{ oder } (s \neq 0 \text{ und } \mathbf{v} = ((s-1)/s)\mathbf{w}) \\
&\Longleftrightarrow \quad s \neq 0 \text{ und } \mathbf{v} = ((s-1)/s)\mathbf{w} \\
&\Longrightarrow \quad \exists c \in \mathbb{R} : \mathbf{v} = c\mathbf{w}.
\end{aligned}$$

($\Longleftarrow$). Angenommen, $\mathbf{v} = c\mathbf{w}$ für ein $c \in \mathbb{R}$. **Zu zeigen:** $\mathbf{0} \in L$.
Per Voraussetzung gilt nun $\mathbf{v} \neq \mathbf{w}$, sodass $c = 1$ direkt ausgeschlossen ist.
Setze nun $\boxed{s := \frac{1}{1-c} \in \mathbb{R}}$, was wohldefiniert ist, da $c \neq 1$.
Man berechnet nun

$$\overbrace{s\mathbf{v} + (1-s)\mathbf{w}}^{\in L, \text{ per Definition}} \quad = \quad \tfrac{1}{1-c}c\mathbf{w} + (1 - \tfrac{1}{1-c})\mathbf{w} \quad = \quad (\underbrace{\frac{c}{1-c} + 1 - \frac{1}{1-c}}_{= \frac{c-1}{1-c} + 1 = 0})\mathbf{w} \quad = \quad 0\mathbf{w} \quad = \quad \mathbf{0}.$$

Darum gilt $\mathbf{0} \in L$. ■

Aufgabe 2·2

(a) **Satz 2·2** *Seien* $\mathbf{v}, \mathbf{v}', \mathbf{w}, \mathbf{w}' \in \mathbb{R}^2$ *mit* $\mathbf{w}, \mathbf{w}' \neq \mathbf{0}$. *Seien* $L := \{\mathbf{v} + t\mathbf{w} \mid t \in \mathbb{R}\}$ *und* $L' := \{\mathbf{v}' + s\mathbf{w}' \mid s \in \mathbb{R}\}$. *Angenommen,* $L \neq L'$. *Dann sind folgende Aussagen äquivalent:*

(i) $L \cap L' = \emptyset$;

(ii) $\mathbf{w}, \mathbf{w}'$ *sind kolinear, d. h.* $\exists c \in \mathbb{R} : \mathbf{w} = c\mathbf{w}'$.

$\Diamond$

Beweis. Der Beweis wird in zwei Teilen gezeigt.

((ai)⟹(aii)). Angenommen, $L \cap L' = \emptyset$. **Zu zeigen:** $\exists c \in \mathbb{R} : \mathbf{w} = c\mathbf{w}'$.
Angenommen, dies sei nicht der Fall.
Da $\mathbf{w}, \mathbf{w}' \neq \mathbf{0}$ bedeutet dies, dass $\mathbf{w}, \mathbf{w}'$ *linear unabhängig* sind. (→ Warum??)
Also gilt für den Untervektorraum $U := \mathrm{Lin}\{\mathbf{w}, \mathbf{w}'\}$, dass $\dim(U) = 2$.
Da $U \subseteq \mathbb{R}^2$ Vektorräume sind und $\dim(U) = 2 = \dim(\mathbb{R}^2)$, folgt hieraus, dass $U = \mathbb{R}^2$. (→ Warum??)
Betrachte bspw. den Vektor

$$\xi \quad := \quad \mathbf{v}' - \mathbf{v} \in \mathbb{R}^2. \tag{2·1}$$

Dann $\xi \in U = \mathrm{Lin}\{\mathbf{w}, \mathbf{w}'\}$. Folglich existieren Skalare $\alpha, \beta \in \mathbb{R}$, so dass $\alpha\mathbf{w} + \beta\mathbf{w}' = \xi$ gilt.
Setze nun $t := \alpha$ und $s := -\beta$. Dann gilt

$$\begin{aligned}
\overbrace{\mathbf{v} + t\mathbf{w}}^{\in L} &= (\mathbf{v} + t\mathbf{w}) - (\mathbf{v}' + s\mathbf{w}') + \mathbf{v}' + s\mathbf{w}' \\
&= (\mathbf{v} - \mathbf{v}') + (t\mathbf{w} - s\mathbf{w}') + \mathbf{v}' + s\mathbf{w}' \\
&= (\mathbf{v} - \mathbf{v}') + (\alpha\mathbf{w} + \beta\mathbf{w}') + \mathbf{v}' + s\mathbf{w}' \\
&\overset{(2·1)}{=} -\xi + \xi + \mathbf{v}' + s\mathbf{w}' \qquad = \quad \underbrace{\mathbf{v}' + s\mathbf{w}'}_{\in L'}.
\end{aligned}$$

Darum gilt $L \cap L' \neq \emptyset$, was ein Widerspruch ist.
Darum stimmt die o. s. Annahme nicht. Also sind $\mathbf{w}, \mathbf{w}'$ kolinear.

((aii)⟹(ai)). Angenommen, $\mathbf{w} = c\mathbf{w}'$ für ein $c \in \mathbb{R}$. **Zu zeigen:** $L \cap L' = \emptyset$.
Angenommen, dies sei nicht der Fall. Dann existiert ein Vektor, $\mathbf{u} \in L \cap L'$.
Per Konstruktion existieren dann $s_0, t_0 \in \mathbb{R}$, so dass

$$\mathbf{v} + t_0\mathbf{w} \quad = \quad \mathbf{u} \quad = \quad \mathbf{v}' + s_0\mathbf{w}'.$$

Aus der Voraussetzung für diese Richtung folgt

$$\mathbf{v}' \quad = \quad \mathbf{v} + (t_0 - s_0 c)\mathbf{w} \tag{2·2}$$

Beachte, dass $c \neq 0$, denn sonst würde $\mathbf{w} = c\mathbf{w}' = \mathbf{0}$ gelten, was ein Widerspruch ist. Wir berechnen

$$\begin{aligned}
L' &= \{\mathbf{v}' + s\mathbf{w}' \mid s \in \mathbb{R}\} \\
&\overset{(2·2)}{=} \{\mathbf{v} + (t_0 - s_0 c)\mathbf{w} + sc\mathbf{w} \mid s \in \mathbb{R}\} \\
&= \{\mathbf{v} + (t_0 + (s - s_0)c)\mathbf{w} \mid s \in \mathbb{R}\} \\
&= \{\mathbf{v} + t\mathbf{w} \mid t \in R\},
\end{aligned} \tag{2·3}$$

wobei $R = \{t_0 + (s - s_0)c \mid s \in \mathbb{R}\} = f(\mathbb{R})$. Also $R = f(\mathbb{R})$, wobei $f : \mathbb{R} \to \mathbb{R}$ eine durch $f(s) = t_0 + (s - s_0)c$ definierte Funktion ist. Da $c \neq 0$, ist es einfach zu sehen, dass f surjektiv ist (in der Tat bijektiv). Darum gilt $R = f(\mathbb{R}) = \mathbb{R}$.
Aus (2·3) folgt also $L' = \{\mathbf{v} + t\mathbf{w} \mid t \in \mathbb{R}\} = L$, was ein Widerspruch ist.
Darum stimmt die o. s. Annahme nicht. Also gilt $L \cap L' = \emptyset$. ■

(b) Wir zeigen nun ein minimales Beispiel dafür, dass Satz 2·2 im allgemeinen für andere Vektorräume nicht gilt. Betrachte den Vektorraum $\mathbb{R}^3$. Betrachte die folgenden Vektoren in $\mathbb{R}^3$:

$$\mathbf{v} \quad = \quad \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \quad \mathbf{v}' \quad = \quad \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad \mathbf{w} \quad = \quad \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \quad \mathbf{w}' \quad = \quad \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}.$$

Bis auf 2-Dimensionalität erfüllen diese die Voraussetzungen in Satz 2·2. Einerseits wurden $\mathbf{w}$, $\mathbf{w}'$ so gewählt, dass sie *nicht* kolinear sind. Dennoch schneiden sich die beiden Geraden, L, L', nicht, da $L \subseteq \{\mathbf{x} \in \mathbb{R}^3 \mid x_1 = 0\} =: E$ und $L' \subseteq \{\mathbf{x} \in \mathbb{R}^3 \mid x_1 = 1\} =: E'$ und offensichtlich $E \cap E' = \emptyset$.

Aufgabe 2·3

(a) Für jedes $\gamma \in \mathbb{R}$ sei die Gerade $L_\gamma \subseteq \mathbb{R}^2$ gegeben durch

$$L_\gamma \quad = \quad \{(x,y) \in \mathbb{R}^2 \mid 2x + y = \gamma \cdot (x - 3y - 7)\}.$$

Satz 2·3 *Es gibt exakt einen Punkt in dem Schnitt aus den Geraden, L_γ, $\gamma \in \mathbb{R}$. Es gilt nämlich $\bigcap_{\gamma\in\mathbb{R}} L_\gamma = \{\xi\}$, wobei $\xi = (1,-2)$.* ◊

Beweis. Wir teilen diesen Beweis in zwei Teilen auf:

(⊇). Es reicht aus, für alle $\gamma \in \mathbb{R}$ **zu zeigen**, dass $\xi \in L_\gamma$.
Fixiere also ein beliebiges $\gamma \in \mathbb{R}$. Dann

$$\begin{array}{rcl} 2\xi_1 + \xi_2 & = & 2 \cdot 1 + (-2) \quad = \quad 0, \qquad \text{und} \\ \gamma \cdot (\xi_1 - 3\xi_2 - 7) & = & \gamma \cdot (1 - 3(-2) - 7) \quad = \quad \gamma \cdot 0 \quad = \quad 0. \end{array}$$

Also $2\xi_1 + \xi_2 = \gamma \cdot (\xi_1 - 3\xi_2 - 7)$. Folglich gilt $\xi \in L_\gamma$ per Konstruktion.

(⊆). Sei $\eta := (x,y) \in \bigcap_{\gamma\in\mathbb{R}} L_\gamma$ beliebig. **Zu zeigen:** $\eta = \xi$.
Zu diesem Zwecke seien $\gamma_1, \gamma_2 \in \mathbb{R}$ irgendwelche Werte mit $\gamma_1 \neq \gamma_2$. Per Wahl gilt $\eta \in L_{\gamma_1} \cap L_{\gamma_2}$. Also

$$\begin{array}{rcl} 2x + y & = & \gamma_1 \cdot (x - 3x - 7), \text{ und} \\ 2x + y & = & \gamma_2 \cdot (x - 3x - 7). \end{array}$$

Wir können ganz naiv arbeiten und die Gleichungen subtrahieren. Dies liefert $(\gamma_1 - \gamma_2) \cdot (x - 3x - 7) = 0$, woraus sich ergibt, dass $x - 3y - 7 = 0$ gelten muss, da $\gamma_1 \neq \gamma_2$. Eingesetzt in die erste Gleichung oben liefert $2x + y = \gamma \cdot 0 = 0$. Darum muss $\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right)$ das LGS $(A|\mathbf{b})$ lösen, wobei

$$A \quad = \quad \left(\begin{smallmatrix} 1 & -3 \\ 2 & 1 \end{smallmatrix}\right), \quad \mathbf{b} \quad = \quad \left(\begin{smallmatrix} 7 \\ 0 \end{smallmatrix}\right)$$

Gaußverfahren angewandt auf $(A|\mathbf{b})$:

$$\left(\begin{array}{cc|c} 1 & -3 & 7 \\ 2 & 1 & 0 \end{array}\right)$$

Wende die Zeilentransformation $Z_2 \rightsquigarrow Z_2 - 2 \cdot Z_1$ an:

$$\left(\begin{array}{cc|c} 1 & -3 & 7 \\ 0 & 7 & -14 \end{array}\right)$$

Aus der Stufenform erschließt sich

$$\begin{array}{rcl} y & = & \frac{-14}{7} \quad = \quad -2 \\ x & = & 7 + 3 \cdot y \quad = \quad 1. \end{array}$$

Also $\eta = (x,y) = (1,-2) = \xi$ für alle $\eta \in \bigcap_{\gamma\in\mathbb{R}} L_\gamma$. Das heißt $\bigcap_{\gamma\in\mathbb{R}} L_\gamma \subseteq \{\xi\}$. ■

(b) **(i)** Sei $\gamma \in \mathbb{R}$. Dann gilt

$$\begin{array}{rcl}(-3,2) \in L_\gamma & \iff & 2(-3)+(2) = \gamma \cdot ((-3)-3(2)-7) \\ & \iff & \gamma = \frac{-4}{-16} = \frac{1}{4}.\end{array}$$

Also ist $\boxed{\gamma = \frac{1}{4}}$ der eindeutige Parameter, für den $(-3,2) \in L_\gamma$ gilt.

(ii) Sei $\gamma \in \mathbb{R}$. Man beobachte, dass

$$\begin{array}{rcl} L_\gamma & = & \{(x,y) \in \mathbb{R}^2 \mid (2-\gamma)x + (1+3\gamma)y = -7\gamma\} \\ & = & \begin{cases} \{(x,y) \in \mathbb{R}^2 \mid 0x + (1+3\cdot 2)y = -7\cdot 2\} & : \ \gamma = 2 \\ \{(x,y) \in \mathbb{R}^2 \mid (2-\frac{-1}{3})x + 0y = -7\cdot\frac{-1}{3}\} & : \ \gamma = -\frac{1}{3} \\ \{(x,y) \in \mathbb{R}^2 \mid (2-\gamma)x + (1+3\gamma)y = -7\gamma\} & : \ \text{sonst} \end{cases} \\ & = & \begin{cases} \{(x,y) \in \mathbb{R}^2 \mid y = -2\} & : \ \gamma = 2 \\ \{(x,y) \in \mathbb{R}^2 \mid x = 1\} & : \ \gamma = -\frac{1}{3} \\ \{(x,y) \in \mathbb{R}^2 \mid y = \frac{\gamma-2}{1+3\gamma}x - \frac{7\gamma}{1+3\gamma}\} & : \ \text{sonst} \end{cases} . \end{array}$$

Daraus folgt, dass L_γ

- parallel zur x-Achse für $\gamma = 2$ ist,
- parallel zur y-Achse für $\gamma = -\frac{1}{3}$ ist,
- und ansonsten weder zur x- noch y-Achse parallel ist, da in diesem Falle L_γ die Gerade »$y = ax + b$« ist, wobei $a \neq 0$.

Also ist der gesuchte Parameterwert eindeutig $\boxed{\gamma = -\frac{1}{3}}$.

(iii) Die Gerade »$x - 2y = -1$« lässt sich äquivalent als »$y = \frac{1}{2}x + 1$ darstellen. Darum wird ein Wert $\gamma \in \mathbb{R}$ gesucht, so dass die Gerade L_γ weder zur x- noch y-Achse parallel ist, und die die y-x-Steigung $\frac{1}{2}$ hat. Nach der o. s. Berechnung in (ii) kommt dies nur für den 3. Fall in Frage. Darum gilt

$$\begin{array}{rcl} L_\gamma \text{ parallel zur Gerade } \text{»}x - 2y = -1\text{«} & \iff & \gamma \notin \{2, -\frac{1}{3}\} \text{ und } \frac{\gamma-2}{1+3\gamma} = \frac{1}{2} \\ & \iff & \gamma \notin \{2, -\frac{1}{3}\} \text{ und } (\gamma-2) = \frac{1}{2}(1+3\gamma) \\ & \iff & \gamma \notin \{2, -\frac{1}{3}\} \text{ und } \gamma = -5 \\ & \iff & \gamma = -5. \end{array}$$

Also ist der gesuchte Parameterwert eindeutig $\boxed{\gamma = -5}$.

Übungsserie 3

Woche 3

ACHTUNG. Diese Lösungen dienen *nicht* als Musterlösungen sondern eher als Referenz. Hier wird eingehender gearbeitet, als generell verlangt wird. Das Hauptziel hier ist, eine Variant anzubieten, gegen die man seine Versuche vergleichen kann.

Aufgabe 3·1

Wir arbeiten im Vektorraum $\mathbb{R}^3$ und betrachten die Vektoren

$$\mathbf{v}_1 = \begin{pmatrix}1\\3\\1\end{pmatrix} \quad \mathbf{v}_2 = \begin{pmatrix}-2\\5\\-2\end{pmatrix} \quad \mathbf{w}_1 = \begin{pmatrix}4\\-3\\-3\end{pmatrix} \quad \mathbf{w}_2 = \begin{pmatrix}0\\1\\1\end{pmatrix}$$

Zu berechnen: $U := \mathrm{Lin}\{\mathbf{v}_1, \mathbf{v}_2\} \cap \mathrm{Lin}\{\mathbf{w}_1, \mathbf{w}_2\}$ als Untervektorraum von $\mathbb{R}^3$.
Zu diesem Zwecke betrachte einen beliebigen Vektor, $\xi \in \mathbb{R}^3$. Es gilt

$$\begin{aligned}
\xi \in U &\iff \exists t_1, t_2, t_3, t_4 \in \mathbb{R} : \xi = t_1\mathbf{v}_1 + t_2\mathbf{v}_2 \text{ und } \xi = t_3\mathbf{w}_1 + t_4\mathbf{w}_2 \\
&\iff \exists \mathbf{t} \in \mathbb{R}^4 : \xi = t_1\mathbf{v}_1 + t_2\mathbf{v}_2 \text{ und } t_1\mathbf{v}_1 + t_2\mathbf{v}_2 = t_3\mathbf{w}_1 + t_4\mathbf{w}_2 \\
&\iff \exists \mathbf{t} \in \mathbb{R}^4 : \xi = t_1\mathbf{v}_1 + t_2\mathbf{v}_2 \text{ und } t_1\mathbf{v}_1 + t_2\mathbf{v}_2 - t_3\mathbf{w}_1 - t_4\mathbf{w}_2 = \mathbf{0} \qquad (3\text{·}1) \\
&\iff \exists \mathbf{t} \in \mathbb{R}^4 : \xi = t_1\mathbf{v}_1 + t_2\mathbf{v}_2 \text{ und } t_1\mathbf{v}_1 + t_2\mathbf{v}_2 + t_3\mathbf{w}_1 + t_4\mathbf{w}_2 = \mathbf{0} \\
&\iff \exists \mathbf{t} \in \mathbb{R}^4 : \xi = t_1\mathbf{v}_1 + t_2\mathbf{v}_2 \text{ und } A\mathbf{t} = \mathbf{0},
\end{aligned}$$

wobei

$$A := (\mathbf{v}_1\ \mathbf{v}_2\ \mathbf{w}_1\ \mathbf{w}_2) = \begin{pmatrix}1&-2&4&0\\3&5&-3&1\\1&-2&-3&1\end{pmatrix}$$

Darum ist es notwendig und hinreichend, die *homogenen Lösungen* für A zu finden, und daraus die Parameter abzulesen.

Homogenes Problem für A:
Zeilentransformationen $Z_2 \rightsquigarrow Z_2 - 3 \cdot Z_1$, $Z_3 \rightsquigarrow Z_3 - Z_1$ anwenden:

$$\begin{pmatrix}1&-2&4&0\\0&11&-15&1\\0&0&-7&1\end{pmatrix}$$

Wende die Zeilentransformation $Z_2 \rightsquigarrow Z_2 - Z_3$ an:

$$\begin{pmatrix}1&-2&4&0\\0&11&-8&0\\0&0&-7&1\end{pmatrix}$$

Aus der Zeilenstufenform erschließt sich, dass t_4 frei ist. Also $t_4 = \alpha$ für ein frei wählbares $\alpha \in \mathbb{R}$.
Aus der Stufenform von Gleichungen $3, 2, 1$ erschließt sich

$$\begin{aligned}
t_3 &= \tfrac{1}{7}t_4 = \tfrac{1}{7}\alpha \\
t_2 &= \tfrac{8}{11}t_3 = \tfrac{8}{77}\alpha \\
t_1 &= 2t_2 - 4t_3 = \tfrac{16}{77}\alpha - \tfrac{4}{7}\alpha = -\tfrac{28}{77}\alpha
\end{aligned}$$

Man kann o. E. α durch $\beta := -77\alpha$ ersetzen. Also ist die homogene Lösung gegeben durch

$$\mathbf{t} = \beta\begin{pmatrix}28\\-8\\-11\\-77\end{pmatrix}, \quad \text{mit } \beta \in \mathbb{R} \text{ frei wählbar.}$$

Wir können nun (3·1) fortsetzen und erhalten

$$\begin{aligned}
\xi \in U &\iff \exists \mathbf{t} \in \mathbb{R}^4 : \xi = t_1\mathbf{v}_1 + t_2\mathbf{v}_2 \text{ und } A\mathbf{t} = \mathbf{0} \\
&\iff \exists \mathbf{t} \in \mathbb{R}^4 : \xi = t_1\mathbf{v}_1 + t_2\mathbf{v}_2 \text{ und } \exists \beta \in \mathbb{R} : \mathbf{t} = \beta \begin{pmatrix} 28 \\ -8 \\ -11 \\ -77 \end{pmatrix} \\
&\iff \exists \beta \in \mathbb{R} : \xi = \beta \cdot (\underbrace{28\mathbf{v}_1 + -8\mathbf{v}_2}_{=:\mathbf{u}}) \\
&\iff \xi \in \mathsf{Lin}\{\mathbf{u}\}
\end{aligned} \tag{3·2}$$

für alle $\xi \in \mathbb{R}^3$.
Es gilt

$$\mathbf{u} \;=\; 28\begin{pmatrix} 1 \\ 3 \\ 1 \end{pmatrix} - 8\begin{pmatrix} -2 \\ 5 \\ -2 \end{pmatrix} \;=\; \begin{pmatrix} 44 \\ 44 \\ 44 \end{pmatrix} \;=\; 44\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}.$$

Aus (3·2) ergibt sich der zu berechnende Untervektorraum als

$$\mathsf{Lin}\{\mathbf{v}_1, \mathbf{v}_2\} \cap \mathsf{Lin}\{\mathbf{w}_1, \mathbf{w}_2\} \;=\; U \;=\; \mathsf{Lin}\{\mathbf{u}\} \;=\; \mathsf{Lin}\{44\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}\} \;=\; \mathsf{Lin}\{\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}\}.$$

Aufgabe 3·2

Seien X, Y nicht leere Mengen und $f : X \to Y$ eine Funktion.

(a) Behauptung. *Die Aussage* $\forall A, B \subseteq X : f(A \cap B) = f(A) \cap f(B)$ *ist* *nicht allgemein gültig*. ◊

Beweis. Betrachte das Beispiel $X = \{0, 1\}$, $Y = \{2\}$, und $f : X \to Y$ mit $f(x) = 2$ für alle $x \in X$. Für $A = \{0\}$ und $B = \{1\}$ gilt $f(A \cap B) = f(\emptyset) = \emptyset$, während $f(A) \cap f(B) = \{2\} \cap \{2\} = \{2\}$. Also $f(A \cap B) \neq f(A) \cap f(B)$. Darum ist dies ein Gegenbeispiel zur Aussage. ■

Bemerkung. Die Aussage ist eigentlich genau dann wahr, wenn f injektiv ist.

(b) Behauptung. *Die Aussage* $\forall A, B \subseteq X : f(A \cup B) = f(A) \cup f(B)$ *ist* *allgemein gültig*. ◊

Für manche (doppelte) Implikationen hier, nämlich für den Umgang mit Existenzquantoren, braucht man Grundkenntnisse in Prädikatenlogik 1. Stufe. Hierfüg gibt es zahlreiche Einführungswerke in die mathematische Logik, bspw. [EFT18].

Beweis. Seien $A, B \subseteq X$ beliebige Teilmengen. Es reicht aus **zu zeigen**, dass $y \in f(A \cup B) \Leftrightarrow y \in f(A) \cup f(B)$ für alle $y \in Y$ gilt.
Sei also $y \in Y$ beliebig. Es gilt

$$\begin{aligned}
y \in f(A \cup B) &\iff \exists x \in A \cup B : y = f(x) \\
&\iff \exists x \in X : x \in A \cup B \text{ und } y = f(x) \\
&\iff \exists x \in X : (x \in A \text{ oder } x \in B) \text{ und } y = f(x) \\
&\iff \exists x \in X : \big((x \in A \text{ und } y = f(x)) \text{ oder } (x \in B \text{ und } y = f(x))\big) \\
&\iff \exists x \in X : (x \in A \text{ und } y = f(x)) \text{ oder } \exists x \in X : (x \in B \text{ und } y = f(x)) \\
&\iff \exists x \in A : y = f(x) \text{ oder } \exists x \in B : y = f(x) \\
&\iff y \in f(A) \text{ oder } y \in f(B) \\
&\iff y \in f(A) \cup f(B).
\end{aligned}$$

Darum gilt $f(A \cup B) = f(A) \cup f(B)$ für alle $A, B \subseteq X$. ■

(c) Behauptung. *Die Aussage* $\forall A \subseteq X : f(X \setminus A) = Y \setminus f(A)$ *ist* *nicht allgemein gültig*. ◊

Beweis. Betrachte das Beispiel $X = \{0, 1\}$, $Y = \{2\}$, und $f : X \to Y$ mit $f(x) = 2$ für alle $x \in X$. Für $A = \{0\}$ gilt $f(X \setminus A) = f(\{1\}) = \{2\}$, während $Y \cap f(A) = \{2\} \setminus \{2\} = \emptyset$. Also $f(X \setminus A) \neq Y \cap f(A)$. Darum ist dies ein Gegenbeispiel zur Aussage. ■

Bemerkung. Die Aussage ist eigentlich genau dann wahr, wenn f bijektiv ist. Und eine leicht modifizierte Aussage, $\forall A \subseteq X : f(X \setminus A) = f(X) \cap f(A)$, ist genau dann wahr, wenn f injektiv ist.

(d) Behauptung. *Die Aussage* $\forall A, B \subseteq Y : f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$ *ist* *allgemein gültig*. ◊

Beweis. Seien $A, B \subseteq Y$ beliebige Teilmengen. Es reicht aus **zu zeigen**, dass $x \in f^{-1}(A \cap B) \Leftrightarrow x \in f^{-1}(A) \cap f^{-1}(B)$ für alle $x \in X$ gilt.
Sei also $x \in X$ beliebig. Es gilt

$$\begin{aligned}
x \in f^{-1}(A \cap B) &\iff f(x) \in A \cap B \\
&\iff f(x) \in A \text{ und } f(x) \in B \\
&\iff x \in f^{-1}(A) \text{ und } x \in f^{-1}(B) \\
&\iff x \in f^{-1}(A) \cap f^{-1}(B).
\end{aligned}$$

Darum gilt $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$ für alle $A, B \subseteq Y$. ■

(e) Behauptung. *Die Aussage* $\forall A, B \subseteq Y : f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$ *ist* *allgemein gültig*. ◊

Beweis. Seien $A, B \subseteq Y$ beliebige Teilmengen. Es reicht aus **zu zeigen**, dass $x \in f^{-1}(A \cup B) \Leftrightarrow x \in f^{-1}(A) \cup f^{-1}(B)$ für alle $x \in X$ gilt.

Sei also $x \in X$ beliebig. Es gilt

$$\begin{aligned} x \in f^{-1}(A \cup B) &\iff f(x) \in A \cup B \\ &\iff f(x) \in A \text{ oder } f(x) \in B \\ &\iff x \in f^{-1}(A) \text{ oder } x \in f^{-1}(B) \\ &\iff x \in f^{-1}(A) \cup f^{-1}(B). \end{aligned}$$

Darum gilt $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$ für alle $A, B \subseteq Y$. ■

Aufgabe 3·3

(a) Seien $n \in \mathbb{N}$ und $v \in \mathbb{R}^n$. Sei $f : \mathbb{R}^n \to \mathbb{R}^n$ durch $f(x) = x + v$ definiert.

Behauptung. *f ist* *bijektiv*. ◊

Beweis. Sei $g : \mathbb{R}^n \to \mathbb{R}^n$ durch $g(x) = x - v$ definiert. Es ist einfach zu sehen, dass $f \circ g = \mathrm{id}_{\mathbb{R}^n}$ und $g \circ f = \mathrm{id}_{\mathbb{R}^n}$. Per Definition ist als f eine Bijektion mit Inversem g. ■

(b) Seien $n \in \mathbb{N}$ und $X = \mathbb{R}^n \times (\mathbb{R}^n \setminus \{\mathbf{0}\})$. Sei Y die Menge aller Geraden im $\mathbb{R}^n$. Sei $f : X \to Y$ durch $f(v, w) = \{v + t \cdot w \mid t \in \mathbb{R}\}$ definiert.

Behauptung. *f ist* *surjektiv* *aber* *nicht injektiv*. ◊

Beweis. **Surjektivität**
Idee: Folgt aus der Definition von Geraden durch Parameter.
Sei $L \subseteq \mathbb{R}^n$ eine beliebige Gerade. **Zu zeigen:** $L \in f(X)$.
Nun, *per Definition* einer Geraden existieren $u, v \in \mathbb{R}^n$ mit $w \neq \mathbf{0}$ und so dass $L = \{u + t \cdot w \mid t \in \mathbb{R}\}$.
Offensichtlicht gilt $(v, w) \in X$. Darum gilt $L = f((v, w)) \in f(X)$.

Nichtinjektivität
Idee: Wir wissen, dass verschiedene aber parallele Vektoren dieselbe Gerade definieren.
Fixiere beliebiges $v, w \in \mathbb{R}^n$ und wähle ein $c \in \mathbb{R} \setminus \{0, 1\}$.
Dann sind $w, cw \neq \mathbf{0}$ verschiedene aber parallele Vektoren.
Darum gilt $f((v, w)) = \{v + t \cdot w \mid t \in \mathbb{R}\} = \{v + tc \cdot w \mid t \in \mathbb{R}\} = f((v, cw))$.
Da $(v, w) \neq (v, cw)$, ist f somit nicht injektiv. ■

(c) Es sei X die Menge aller Bücher in einem fixierten Kontext. Sei Y die Menge alle Autor(inn)en von Büchern. Sei $f : X \to \mathcal{P}(Y)$ definiert durch $f(x) = \{y \mid y \text{ ein(e) Autor(in) vom Buch } x\}$ für alle $x \in X$.

Behauptung. *f ist* *nicht im Allgemeinen injektiv* *und* *niemals surjektiv*. ◊

Beweis. **Nichtsurjektivität**
Zu zeigen: Es gibt konstellationen von Autor(inn)en, die kein gemeinsames Buch verfasst haben.
Es gibt *immer* eine(n) Autor(in) eines Buchs, sodass $\emptyset \notin f(X)$ in allen Kontexten. Darum ist f niemals surjektiv.

Nichtinjektivität
Zu zeigen: Es gibt zwei verschiedene Bücher, die von der gleichen Konstellation an Autor(inn)en verfasst wurden. In unserem Kontext hat bspw. $a =$ *JK Rowling* alleine die Bücher $b_1 :=$ »*HP and the Philosopher's Stone*« und $b_2 :=$ »*HP and the Goblet of Fire*« geschrieben. Darum $b_1 \neq b_2$ und $f(b_1) = \{a\} = f(b_2)$. Also ist f in unserem Kontext nicht injektiv. ■

Anmerkung. Falls wir $\emptyset$ von der Bildmenge $\mathcal{P}(Y)$ exludieren, dann können wir mindestens dafür argumentieren, dass f nicht im Allgemeinen surjektiv ist: In unserem konkreten Kontext haben bspw. *JK Rowling* und *Oscar Wilde* nie am selben Buch gearbeitet, also gilt $\{\text{JK Rowling, Oscar Wilde}\} \notin f(X)$. In der Tat ist ein Kontext kaum vorstellbar, in dem sich *alle* Autor(inn)en an einem gemeinsamen Buch beteiligt haben, d. h. $Y \in f(X)$ sowie alle „große“ Teilmengen sind fast immer ausgeschlossen.

(d) Seien X die Menge aller in Deutschland zugelassener Kfz und Y die Menge aller amtlicher Kennzeichen. Sei $f : X \to Y$ die Abbildung, die jedem Kfz sein Kennzeichen zuordnet.

Behauptung. *f ist* *injektiv* *aber* *nicht im Allgemeinen surjektiv*. ◊

Beweis. **Injektivität:** Jedes Kennzeichen darf per Gesetz nur einem Kfz zugehören. **Nichtsurjektivität:** Es besteht zwar die Chance, dass irgendwann alle Kennzeichen aufgebraucht werden, aber in der Praxis ist die Menge Y sehr groß, dass dies aktuell und für eine lange Zeit nicht vorkommt. ■

Übungsserie 4

Woche 4

ACHTUNG. Diese Lösungen dienen *nicht* als Musterlösungen sondern eher als Referenz. Hier wird eingehender gearbeitet, als generell verlangt wird. Das Hauptziel hier ist, eine Variant anzubieten, gegen die man seine Versuche vergleichen kann.

Aufgabe 4·1

(a) Betrachte die Menge $X := \mathbb{Z} \times \mathbb{N}$ und die binäre Relation, $\sim \subseteq X \times X$, die durch

$$(a,b) \sim (a',b') \iff ab' = a'b$$

für $(a,b),(a',b') \in X$ definiert wird.

Behauptung. $(X,\sim)$ *ist eine Äquivalenzrelation.* ◊

Beweis. Wir gehen die Axiome durch:

Reflexivität: Sei $(a,b) \in X$ beliebig. **Zu zeigen:** $(a,b) \sim (a,b)$.
Offensichtlich gilt $ab = ab$.
Per Konstruktion gilt also $(a,b) \sim (a,b)$.

Symmetrie: Seien $(a,b),(a',b') \in X$ beliebig. **Zu zeigen:** $(a,b) \sim (a',b') \Rightarrow (a',b') \sim (a,b)$.
Es gilt

$$\begin{aligned} (a,b) \sim (a',b') &\iff ab' = a'b && \text{(per Konstruktion)} \\ &\implies a'b = ab' \\ &\iff (a',b') \sim (a,b) && \text{(per Konstruktion).} \end{aligned}$$

Transitivität: Seien $(a,b),(a',b'),(a'',b'') \in X$ beliebig.
Zu zeigen: $(a,b) \sim (a',b')$ und $(a',b') \sim (a'',b'') \Rightarrow (a,b) \sim (a'',b'')$.
Es gilt

$$\begin{aligned} &(a,b) \sim (a',b') \\ &\text{und } (a',b') \sim (a'',b'') \iff ab' = a'b \text{ und } a'b'' = a''b' \\ &\qquad \text{(per Konstruktion)} \\ &\implies (ab'')b' = (ab')b'' = (a'b)b'' = (a'b'')b = (a''b')b = (a''b)b' \\ &\implies ab'' = a''b, \\ &\qquad \text{da } b' \neq 0 \\ &\iff (a,b) \sim (a'',b'') \\ &\qquad \text{(per Konstruktion).} \end{aligned}$$

Darum erfüllt $(X,\sim)$ die Axiome einer Äquivalenzrelation. ■

Bemerkung. Man kann zeigen, dass $f : X/\sim \to \mathbb{Q}$ definiert durch $f([(a,b)]) = a/b$ wohldefiniert und bijektiv ist. In der Tat realisieren manche Werke die rationalen Zahlen, $\mathbb{Q}$, als genau diesen Quotientenraum, d. h. man kann die Äquivalenzklassen hier als rationale Zahlen deuten.

(b) Betrachte die Menge $X := \mathbb{Z} \times \mathbb{Z}$ und die binäre Relation, $\leqslant \subseteq X \times X$, die durch

$$(a,b) \leqslant (a',b') \iff a \leqslant a' \text{ und } b \leqslant b'$$

für $(a,b),(a',b') \in X$ definiert wird.

Behauptung. $(X, \leqslant)$ *ist ist eine Halbordnung aber* $\boxed{\textit{nicht total}}$. $\Diamond$

Beweis. Wir gehen die Axiome durch:

Reflexivität: Sei $(a, b) \in X$ beliebig. **Zu zeigen:** $(a, b) \leqslant (a, b)$.
Offensichtlich gilt $a \leqslant a$ und $b \leqslant b$.
Per Konstruktion gilt also $(a, b) \leqslant (a, b)$.

Antisymmetrie: Seien $(a, b), (a', b') \in X$ beliebig.
Zu zeigen: $(a, b) \leqslant (a', b')$ und $(a', b') \leqslant (a, b) \Rightarrow (a, b) = (a', b')$.
Es gilt

$$\begin{aligned} &(a, b) \leqslant (a', b') \\ &\text{und } (a', b') \leqslant (a, b) \quad &\iff\quad & a \leqslant a' \text{ und } b \leqslant b' \text{und } a' \leqslant a \text{ und } b' \leqslant b \\ & &&\text{(per Konstruktion)} \\ & &\implies\quad & a = a \text{ und } b = b', \\ & &&\text{da } (\mathbb{Z}, \leqslant) \text{ antisymmetrisch ist} \\ & &\iff\quad & (a, b) = (a', b'). \end{aligned}$$

Transitivität: Seien $(a, b), (a', b'), (a'', b'') \in X$ beliebig.
Zu zeigen: $(a, b) \leqslant (a', b')$ und $(a', b') \leqslant (a'', b'') \Rightarrow (a, b) \leqslant (a'', b'')$.
Es gilt

$$\begin{aligned} &(a, b) \leqslant (a', b') \\ &\text{und } (a', b') \leqslant (a'', b'') \quad &\iff\quad & a \leqslant a' \text{ und } b \leqslant b' \text{und } a' \leqslant a'' \text{ und } b' \leqslant b'' \\ & &&\text{(per Konstruktion)} \\ & &\implies\quad & a \leqslant a'' \text{ und } b \leqslant b'', \\ & &&\text{da } (\mathbb{Z}, \leqslant) \text{ transitiv ist} \\ & &\iff\quad & (a, b) \leqslant (a'', b'') \\ & &&\text{(per Konstruktion).} \end{aligned}$$

Darum erfüllt $(X, \leqslant)$ die Axiome einer Halbordnung.
Zum Schluss, beachte, dass $(0, 1)$ und $(1, 0)$ bzgl. $\leqslant$ unvergleichbar sind. Darum ist $(X, \leqslant)$ nicht total. ■

Aufgabe 4·2

Fixiere $n \in \mathbb{N}$. Wir definieren die binäre Relation $\sim \subseteq \mathbb{Z} \times \mathbb{Z}$ mittels

$$a \sim b \quad :\Longleftrightarrow \quad \mathsf{mod}(a,n) = \mathsf{mod}(b,n)$$

für $a, b \in \mathbb{Z}$.

(a) Behauptung. $(\mathbb{Z}, \sim)$ *ist eine Äquivalenzrelation.* ◊

Beweis. Wir gehen die Axiome durch:

Reflexivität: Sei $a \in \mathbb{Z}$ beliebig. **Zu zeigen:** $a \sim a$.
Offensichtlich gilt $\mathsf{mod}(a,n) = \mathsf{mod}(a,n)$.
Per Konstruktion gilt also $(a,b) \sim (a,b)$.

Symmetrie: Seien $a, a' \in \mathbb{Z}$ beliebig. **Zu zeigen:** $a \sim a' \Rightarrow a' \sim a$.
Es gilt

$$\begin{array}{rcll} a \sim a' & \Longleftrightarrow & \mathsf{mod}(a,n) = \mathsf{mod}(a',n) & \text{(per Konstruktion)} \\ & \Longrightarrow & \mathsf{mod}(a',n) = \mathsf{mod}(a,n) & \\ & \Longleftrightarrow & a' \sim a & \text{(per Konstruktion).} \end{array}$$

Transitivität: Seien $a, a', a'' \in \mathbb{Z}$ beliebig. **Zu zeigen:** $a \sim a'$ und $a' \sim a'' \Rightarrow a \sim a''$.
Es gilt

$$\begin{array}{rcl} a \sim a' \,\text{und}\, a' \sim a'' & \Longleftrightarrow & \mathsf{mod}(a,n) = \mathsf{mod}(a',n) \,\text{und}\, \mathsf{mod}(a',n) = \mathsf{mod}(a'',n) \\ & & \text{(per Konstruktion)} \\ & \Longrightarrow & \mathsf{mod}(a,n) = \mathsf{mod}(a'',n) \\ & \Longleftrightarrow & a \sim a'' \quad \text{(per Konstruktion).} \end{array}$$

Darum erfüllt $(\mathbb{Z}, \sim)$ die Axiome einer Äquivalenzrelation. ■

Bemerkung. Es gibt einen einfacheren Ansatz. Zunächst beweist man das allgemeine Lemma: Für jede Äquivalenzrelation $(Y, \approx)$ und jede Relation (X, R), falls eine Funktion $f : X \to Y$ existiert, so dass $\forall x, x' \in X : (x, x') \in R \Leftrightarrow f(x) \approx f(x')$, so gilt dass (X, R) eine Äquivalenzrelation ist. Und jetzt wendet man dies auf unseren Kontext an: Wir die Äquivalenzrelation $(\{0, 1, 2 \ldots, n-1\}, =)$ und die Relation $(\mathbb{Z}, \sim)$ und eine Abbildung $f : a \in \mathbb{Z} \mapsto \mathsf{mod}(a,n)$, für die $\forall a, a' \in \mathbb{Z} : (a, a') \in \sim \Leftrightarrow f(a) \approx f(a')$ *per Konstruktion* gilt. Darum ist $(\mathbb{Z}, \sim)$ eine Äquivalenzrelation.

(b) Behauptung. *Es gibt n Äquivalenzklassen.* ◊

Beweis. Betrachte die Abbildung

$$\begin{array}{rcccl} \rho & : & \mathbb{Z}/\sim & \to & \{0, 1, \ldots, n-1\} \\ & : & [a] & \mapsto & \mathsf{mod}(a,n) \end{array}$$

Es reicht aus **zu zeigen**, dass ρ eine wohldefinierte Bijektion ist.

Wohldefiniertheit: Sei $C \in \mathbb{Z}/\sim$ beliebig. Seien $a, a' \in \mathbb{Z}$ mit $[a] = C$ und $[a'] = C$.
Zu zeigen: $\mathsf{mod}(a,n) = \mathsf{mod}(a',n)$.
Aus $[a] = C = [a']$ folgt $a \sim a'$ und damit per Konstruktion $\mathsf{mod}(a,n) = \mathsf{mod}(a',n)$. Darum ordnet ρ einen eindeutig Wert $[a]$ zu.

Injektivität: Seien $C, C' \in \mathbb{Z}/\sim$ beliebig. **Zu zeigen:** $\rho(C) = \rho(C') \Rightarrow C = C'$.
Wähle zunächst $a, a' \in \mathbb{Z}$, so dass $C = [a]$ und $C = [a']$. Dann gilt

$$\begin{array}{rcl} \rho(C) = \rho(C') & \Longrightarrow & \mathsf{mod}(a,n) = \mathsf{mod}(a',n) \\ & \Longrightarrow & a \sim a' \\ & \Longrightarrow & C = [a] = [a'] = C'. \end{array}$$

Surjektivität: Sei $k \in \{0, 1, \ldots, n-1\}$ beliebig. **Zu zeigen:** $k \in \rho(\mathbb{Z}/\sim)$.
Setze $C = [k] \in \mathbb{Z}/\sim$. Dann $\rho(C) = \mathsf{mod}(k,n) = k$.[a] Also gilt $k \in \rho(\mathbb{Z}/\sim)$.

Darum ist ρ eine Bijektion. Also gilt $|\mathbb{Z}/\sim| = |\{0, 1, \ldots, n-1\}| = n$. ■

(c) Laut der Berechnung in Aufgabe 2(b) gilt $\mathbb{Z}/\sim = \{[0], [1], \ldots, [n-1]\}$. Für jedes $k \in \{0, 1, \ldots, n-1\}$

[a] Seien $q \in \mathbb{Z}$ und $r \in \{0, 1, \ldots, n-1\}$ mit $qn + r = k$. Da $k, r \in \{0, 1, \ldots, n-1\}$, gilt $qn = k - r \in \mathbb{Z} \cap (-n, n)$. Also muss $q = 0$ gelten. Also $r = k$. Also $\mathsf{mod}(k,n) = r = k$.

lässt sich die Äquivalenzklasse $[k]$ wie folgt als Teilmenge beschreiben

$$\begin{aligned}
[k] &= \{a \in \mathbb{Z} \mid a \sim k\} \text{ per Definition} \\
&= \{a \in \mathbb{Z} \mid \mathsf{mod}(a,n) = \mathsf{mod}(k,n)\} \\
&= \{a \in \mathbb{Z} \mid \mathsf{mod}(a,n) = k\} \\
&= \{a \in \mathbb{Z} \mid \exists q \in \mathbb{Z} : a = qn + r\} \\
&= \{qn + r \mid q \in \mathbb{Z}\} \\
&= \mathbb{Z} \cdot n + r.
\end{aligned}$$

Also lassen sich die Äquivalenzklassen durch die Teilmengen $\{\mathbb{Z} \cdot n + r \mid r \in \{0, 1, \ldots, n-1\}\}$ darstellen.

Aufgabe 4·3

Behauptung. *Für $n \in \mathbb{N}$ bezeichne mit $\Phi(n)$ die Aussage, dass für alle Mengen X, Y mit $|X| = |Y| = n$*

$$|\{f \mid f \text{ eine Bijektion zw. } X \text{ und } Y\}| \quad = \quad n!. \tag{4·1}$$

Dann gilt $\forall n \in \mathbb{N} : \Phi(n)$. ◊

Beweis (Ansatz I). Sei $n \in \mathbb{N}$ und seien X, Y n-elementige Mengen. Sei $(x_1, x_2, \ldots, x_n)$ eine Auflistung der Elemente in X. Um eine Injektion zw. X und Y zu definieren, wählt man zuerst ein Element $y_1 \in Y$ für x_1 (dafür gibt es n Möglichkeiten), dann ein Element $y_2 \in Y$ for x_2 (dafür bleiben $n-1$ Möglichkeiten übrig), usw. Darum gibt es insgesamt $n \cdot (n-1) \cdot \cdots \cdot 1 = n!$ Injektionen zwischen X und Y. Da X und Y endlich und gleichmächtig sind, ist jede Injektion zwischen diesen Mengen automatisch surjektiv und damit bijektiv. Darum gibt es $n!$ Bijektionen zwischen X und Y. ■ **(Ansatz I)**

Beweis (Ansatz II). Wir beweisen die Behauptung per Induktion über n.

Induktionsanfang: Sei $n = 1$. Für 1-elementigen Mengen X, Y, gibt es offensichtlich exakt eine Funktion zwischen X und Y, und dies ist eine Bijektion. Darum gilt (4·1).

Induktionsvoraussetzung: Sei $n > 1$. Angenommen, $\Phi(n-1)$ gilt.

Induktionsschritt: Seien X, Y beliebige n-elementige Mengen. **Zu zeigen:** (4·1) gilt.

Fixiere $x_0 \in X$. Beobachte, dass für alle $y_0 \in Y$ die Mengen $X' := X \setminus \{x_0\}$ und $Y' := Y \setminus \{y_0\}$ beide $n-1$-elementig sind. Betrachte nun die Abbildung

$$\begin{array}{rcccl}
F & : & \{g \mid g \text{ Bij. zw. } X \setminus \{x_0\} \text{ und } Y \setminus \{x_0\}\} & \to & \{f \mid f \text{ Bij. zw. } X \text{ und } Y,\ f(x_0) = y_0\} \\
 & : & g & \mapsto & g \cup \{(x_0, y_0)\}.
\end{array}$$

Das heißt, jede Bijektion $g : X \setminus \{x_0\} \to Y \setminus \{y_0\}$ wird durch F zu einer Funktion von X nach Y fortgesetzt, indem das zusätzliche Element, x_0, auf y_0 abgebildet wird. Es ist einfach zu sehen, dass F wohldefiniert ist, d. h. für jede Bijektion $g : X \setminus \{x_0\} \to Y \setminus \{y_0\}$, es gilt, dass $F(g)$ eine wohldefinierte Funktion zwischen X und Y ist und weiterhin ist dies eine Bijektion. Außerdem ist es klar, dass die Abbildung

$$\begin{array}{rcccl}
G & : & \{f \mid f \text{ Bij. zw. } X \text{ und } Y,\ f(x_0) = y_0\} & \to & \{g \mid g \text{ Bij. zw. } X \setminus \{x_0\} \text{ und } Y \setminus \{x_0\}\} \\
 & : & f & \mapsto & f|_{X \setminus \{x_0\} \times Y \setminus \{x_0\}}
\end{array}$$

die Abbildung F nach rechts und links invertiert. Also ist G eine Bijektion. Daraus folgt per Definition von Kardinalität

$$\begin{aligned}
|\{f \mid f \text{ Bij. zw. } X \text{ und } Y,\ f(x_0) = y_0\}| &= |\{g \mid g \text{ Bij. zw. } X \setminus \{x_0\} \text{ und } Y \setminus \{x_0\}\}| \\
&= (n-1)! \text{ laut IV.}
\end{aligned} \tag{4·2}$$

Anderseits ist $(\{f \mid f \text{ Bij. zw. } X \text{ und } Y,\ f(x_0) = y_0\})_{y_0 \in Y}$ eine Partition von $\{f \mid f \text{ Bij. zw. } X \text{ und } Y\}$. Darum gilt

$$\begin{aligned}
|\{f \mid f \text{ Bij. zw. } X \text{ und } Y\}| &= |\textstyle\bigcup_{y_0 \in Y} \{f \mid f \text{ Bij. zw. } X \text{ und } Y,\ f(x_0) = y_0\}| \\
&= \textstyle\sum_{y_0 \in Y} |\{f \mid f \text{ Bij. zw. } X \text{ und } Y,\ f(x_0) = y_0\}| \\
&\quad \text{wegen paarweise Disjunktheit} \\
&\overset{(4·2)}{=} \textstyle\sum_{y_0 \in Y} (n-1)! = |Y| \cdot (n-1)! = n \cdot (n-1)! = n!.
\end{aligned}$$

Also gilt (4·1).

Darum gilt $\Phi(n)$ per Induktion für alle $n \in \mathbb{N}$. ■ **(Ansatz II)**

Übungsserie 5

Woche 5

ACHTUNG. Diese Lösungen dienen *nicht* als Musterlösungen sondern eher als Referenz. Hier wird eingehender gearbeitet, als generell verlangt wird. Das Hauptziel hier ist, eine Variant anzubieten, gegen die man seine Versuche vergleichen kann.

Aufgabe 5·1

Fixiere eine natürliche Zahl $n \in \mathbb{N}_0$. Sei $a_i \in \{0, 1, \ldots, 10-1\}$ die eindeutige Zahlen, so dass

$$n \quad = \quad \sum_{i\in\mathbb{N}_0} a_i 10^i$$

gilt.

(a) **Behauptung.** $3 \mid n \Leftrightarrow 3 \mid \sum_{i\in\mathbb{N}_0} a_i$. ◊

Beweis. Beachte zunächst, dass $10 \equiv 1 \mod 3$. Also gilt modulo 3

$$n \quad \equiv \quad \sum_{i\in\mathbb{N}_0} a_i 1^i \quad \equiv \quad \sum_{i\in\mathbb{N}_0} a_i.$$

Folglich gilt

$$3 \mid n \iff n \equiv 0 \mod 3 \iff \sum_{i\in\mathbb{N}_0} a_i \equiv 0 \mod 3 \iff 3 \mid \sum_{i\in\mathbb{N}_0} a_i$$

wie behauptet. ■

(b) **Behauptung.** $11 \mid n \Leftrightarrow 1 \mid \sum_{i\in\mathbb{N}_0} (-1)^i a_i$. ◊

Beweis. Beachte zunächst, dass $10 = -1 \mod 11$. Also gilt modulo 11

$$n \quad \equiv \quad \sum_{i\in\mathbb{N}_0} a_i (-1)^i.$$

Folglich gilt

$$11 \mid n \iff n \equiv 0 \mod 11 \iff \sum_{i\in\mathbb{N}_0} a_i \equiv 0 \mod 11 \iff 11 \mid \sum_{i\in\mathbb{N}_0} (-1)^i a_i$$

wie behauptet. ■

Aufgabe 5·2

(a) Seien $a = 142$ und $b = 84$. Wir berechnen $\mathsf{ggT}(a, b)$ mittels des Euklidischen Algorithmus (siehe [Sin20, Satz 3.4.7]).

Restberechnung (symbolisch)	Restberechnung (Werte)
$a = b \cdot q_1 + r_1$	$142 = 84 \cdot 1 + 58$
$b = r_1 \cdot q_2 + r_2$	$84 = 58 \cdot 1 + 26$
$r_1 = r_2 \cdot q_3 + r_3$	$58 = 26 \cdot 2 + 6$
$r_2 = r_3 \cdot q_4 + r_4$	$26 = 6 \cdot 4 + \boxed{\mathbf{2}}$
$r_3 = r_4 \cdot q_5 + r_5$	$6 = 2 \cdot 3 + 0$

Darum gilt $\mathsf{ggT}(a, b) = r_2 = 2$.

(b) Behauptung 5·3 *Seien $a, b, c \in \mathbb{Z}$ mit $a, b \neq 0$. Die folgenden Aussagen sind äquivalent:*

(i) $\exists x, y \in \mathbb{Z} : ax + by = c$

(ii) $\mathsf{ggT}(a, b) \mid c$

$\Diamond$

Beweis. Fixiere zunächst $d := \mathsf{ggT}(a, b)$. Da $a, b \in \mathbb{Z} \setminus \{0\}$, ist $d \in \mathbb{N}$ eine wohldefinierte positive Zahl.

((bi)⟹(bii)). Angenommen, $ax + by = c$ für ein $x, y \in \mathbb{Z}$.
Da $x, y \in \mathbb{Z}$, erhalten wir $c = ax + by \equiv 0x + 0z \equiv 0$ modulo d.
Also $\mathsf{ggT}(a, b) = d \mid c$.

((bii)⟹(bi)). Angenommen, $\mathsf{ggT}(a, b) \mid c$.
Dann existiert ein $k \in \mathbb{Z}$, so dass $c = k \cdot \mathsf{ggT}(a, b)$.
Laut des Lemmas von Bézout (siehe [Sin20, Lemma 3.4.8]) existiere nun $u, v \in \mathbb{Z}$, so dass $\mathsf{ggT}(a, b) = au + bv$.
Daraus folgt $c = k \cdot \mathsf{ggT}(a, b) = aku + bkv$.
Da $ku, kv \in \mathbb{Z}$, haben wir (bi) bewiesen. ■

Aufgabe 5·3

(a) Sei $H := \mathbb{Z}/2\mathbb{Z}$ die (abelsche) Gruppe von Restklassen modulo 2 unter Addition.
Sei $G := H \times H$ mit Neutralelement $e = ([0], [0])$ und versehen mit der Produktstruktur.
Als Produkt von (abelschen) Gruppen ist G automatisch eine (abelsche) Gruppe. Und offensichtlich hat G genau $|G| = |H \times H| = |H| \cdot |H| = 2 \cdot 2 = 4$ Elemente.
Es bleibt **zu zeigen**, dass $\forall a \in G : a * a = e$.
Sei also $a = ([k], [j]) \in H \times H = G$ ein beliebiges Element. Es gilt

$$\begin{aligned} a * a &= ([k], [j]) * ([k], [j]) \\ &= ([k] + [k], [j] + [j]) \\ &= ([k + k], [j + j]) \\ &= ([2k], [2j]) = ([0], [0]) = e, \end{aligned}$$

da $2 \equiv 0 \mod 2$.
Also ist unsere Konstruktion von G ein passendes Beispiel.

(b) Behauptung. *Sei $(G, *, e)$ eine Gruppe. Angenommen, $\forall a \in G : a * a = e$. Dann ist G kommutativ.* $\Diamond$

Beweis. Beachte zunächst, dass wegen Eindeutigkeit des Inverses die Annahme zu

$$\forall a \in G : a^{-1} = a \tag{5·1}$$

äquivalent ist.
Zu zeigen: Für alle $a, b \in G$ gilt $a * b = b * a$.
Seien also $a, b \in G$ beliebige Elemente. Es gilt

$$a * b \overset{(5·1)}{=} a^{-1} * b^{-1} = (b * a)^{-1} \overset{(5·1)}{=} b * a.$$

Also ist G eine kommutative Gruppe. ■

Übungsserie 6

Woche 6

ACHTUNG. Diese Lösungen dienen *nicht* als Musterlösungen sondern eher als Referenz. Hier wird eingehender gearbeitet, als generell verlangt wird. Das Hauptziel hier ist, eine Variant anzubieten, gegen die man seine Versuche vergleichen kann.

Aufgabe 6·1

Es sei X eine Menge und $R = \mathcal{P}(X)$. Auf R definiere man die folgenden Verknüpfungen:

$$\begin{aligned} A + B &= A \cup B \setminus (A \cap B) \\ A \cdot B &= A \cap B \end{aligned}$$

für alle $A, B \in R$.

(a) Die Additions und Multiplikationstabellen für eine 3-elementige Menge, $X = \{a, b, c\}$, sehen wie folgt aus:

$+$	$\emptyset$	$\{c\}$	$\{b\}$	$\{b,c\}$	$\{a\}$	$\{a,c\}$	$\{a,b\}$	$\{a,b,c\}$
$\emptyset$	$\emptyset$	$\{c\}$	$\{b\}$	$\{b,c\}$	$\{a\}$	$\{a,c\}$	$\{a,b\}$	$\{a,b,c\}$
$\{c\}$	$\{c\}$	$\emptyset$	$\{b,c\}$	$\{b\}$	$\{a,c\}$	$\{a\}$	$\{a,b,c\}$	$\{a,b\}$
$\{b\}$	$\{b\}$	$\{b,c\}$	$\emptyset$	$\{c\}$	$\{a,b\}$	$\{a,b,c\}$	$\{a\}$	$\{a,c\}$
$\{b,c\}$	$\{b,c\}$	$\{b\}$	$\{c\}$	$\emptyset$	$\{a,b,c\}$	$\{a,b\}$	$\{a,c\}$	$\{a\}$
$\{a\}$	$\{a\}$	$\{a,c\}$	$\{a,b\}$	$\{a,b,c\}$	$\emptyset$	$\{c\}$	$\{b\}$	$\{b,c\}$
$\{a,c\}$	$\{a,c\}$	$\{a\}$	$\{a,b,c\}$	$\{a,b\}$	$\{c\}$	$\emptyset$	$\{b,c\}$	$\{b\}$
$\{a,b\}$	$\{a,b\}$	$\{a,b,c\}$	$\{a\}$	$\{a,c\}$	$\{b\}$	$\{b,c\}$	$\emptyset$	$\{c\}$
$\{a,b,c\}$	$\{a,b,c\}$	$\{a,b\}$	$\{a,c\}$	$\{a\}$	$\{b,c\}$	$\{b\}$	$\{c\}$	$\emptyset$

$\cdot$	$\emptyset$	$\{c\}$	$\{b\}$	$\{b,c\}$	$\{a\}$	$\{a,c\}$	$\{a,b\}$	$\{a,b,c\}$
$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$
$\{c\}$	$\emptyset$	$\{c\}$	$\emptyset$	$\{c\}$	$\emptyset$	$\{c\}$	$\emptyset$	$\{c\}$
$\{b\}$	$\emptyset$	$\emptyset$	$\{b\}$	$\{b\}$	$\emptyset$	$\emptyset$	$\{b\}$	$\{b\}$
$\{b,c\}$	$\emptyset$	$\{c\}$	$\{b\}$	$\{b,c\}$	$\emptyset$	$\{c\}$	$\{b\}$	$\{b,c\}$
$\{a\}$	$\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	$\{a\}$	$\{a\}$	$\{a\}$	$\{a\}$
$\{a,c\}$	$\emptyset$	$\{c\}$	$\emptyset$	$\{c\}$	$\{a\}$	$\{a,c\}$	$\{a\}$	$\{a,c\}$
$\{a,b\}$	$\emptyset$	$\emptyset$	$\{b\}$	$\{b\}$	$\{a\}$	$\{a\}$	$\{a,b\}$	$\{a,b\}$
$\{a,b,c\}$	$\emptyset$	$\{c\}$	$\{b\}$	$\{b,c\}$	$\{a\}$	$\{a,c\}$	$\{a,b\}$	$\{a,b,c\}$

Der Additionstabelle ist zu entnehmen, dass $\boxed{\emptyset \text{ das Nullelement}}$ (d. h. additives Neutralelement) ist. Der Multiplikationstabelle ist zu entnehmen, dass $\boxed{\{a,b,c\} \text{ das Einselement}}$ (d. h. multiplikatives Neutralelement) ist.

(b) Sei nun X eine allgemeine Menge.

Behauptung 6·1 $(R, +, \cdot, \emptyset, X)$ *bildet einen kommutativen Ring, wobei* $R = \mathcal{P}(X)$. $\Diamond$

Es gibt hier zwei Ansätze.

Beweis (von Behauptung 6·1, Ansatz I). Wir gehen einfach alle Axiome durch. Zunächst aber beobachten wir für alle $A, B \in R$ und $x \in X$, dass

$$\begin{aligned} x \in A + B &\overset{\text{Defn}}{\iff} x \in (A \cup B) \setminus (A \cap B) \\ &\iff x \text{ in } A \text{ oder } B, \text{ aber nicht beides} \\ &\iff x \text{ in exakt einem von } A, B. \end{aligned} \tag{6·1}$$

Darauf werden wir uns in einigen Berechnungen berufen.

Addition/Assoziativität: Seien $A, B, C \in R$ beliebig. **Zu zeigen:** $(A + B) + C = A + (B + C)$.
Da es sich auf beiden Seiten der Gleichung um Mengen handelt, reicht es aus, für alle $x \in X$ **zu zeigen**, dass $x \in (A + B) + C$ gdw. $x \in A + (B + C)$.
Sei also $x \in X$ beliebig. Es gilt

$$\begin{aligned} x \in A + (B + C) &\overset{(6·1)}{\iff} \text{exakt eines von } x \in A \text{ oder } x \in B + C \text{ gilt} \\ &\overset{(6·1)}{\iff} \text{exakt eines von } x \in A \text{ oder (exakt eines von } x \in B \text{ oder } x \in C) \text{ gilt} \\ &\iff \text{exakt eines von } x \in A \text{ oder } x \in B \text{ oder } x \in C \text{ gilt} \\ &\iff x \text{ in exakt einem von } A, B, \text{ oder } C \end{aligned}$$

und

$$\begin{aligned} x \in (A + B) + C &\overset{(6·1)}{\iff} \text{exakt eines von } x \in A + B \text{ oder } x \in C \text{ gilt} \\ &\overset{(6·1)}{\iff} \text{exakt eines von (exakt eines von } x \in A \text{ oder } x \in B) \text{ oder } x \in C \text{ gilt} \\ &\iff \text{exakt eines von } x \in A \text{ oder } x \in B \text{ oder } x \in C \text{ gilt} \\ &\iff x \text{ in exakt einem von } A, B, \text{ oder } C \end{aligned}$$

Darum gilt $x \in A+(B+C) \Leftrightarrow x \in (A+B)+C$ für alle $x \in X$. Also $A+(B+C) = (A+B)+C$ für alle $A, B, C \in R$. Also ist $(R, +)$ assoziativ.

Addition/Kommutativität: Seien $A, B \in R$ beliebig. **Zu zeigen:** $A + B = B + A$.
Es gilt

$$A + B \overset{\text{Defn}}{=} (A \cup B) \setminus (A \cap B) \overset{(*)}{=} (B \cup A) \setminus (B \cap A) \overset{\text{Defn}}{=} B + A,$$

wobei die Gleichung bei $(*)$ gilt, weil die Mengenoperationen, $\cap$ und $\cup$, bekanntermaßen kommutativ sind. Also ist $(R, +)$ kommutativ.

Addition/Nullelement: Wir behaupten, dass $0 := \emptyset$ das additive Neutralelement ist. Sei also $A \in R$ beliebig. **Zu zeigen:** $A + 0 = 0 + A = A$.
Wegen Kommutativität reicht es aus, $A + 0 = A$ zu zeigen. Es gilt

$$A + 0 \overset{\text{Defn}}{=} (A \cup \emptyset) \setminus (A \cap \emptyset) = A \setminus \emptyset = A$$

Also ist $\emptyset$ ein Neutralelement für $(R, +)$.

Addition/Inverses: Sei $A \in R$ beliebig. **Zu zeigen:** Es gibt ein Element $A' \in R$, so dass $A' + A = A + A' = 0$.
Wir betrachten als Möglichkeit $A' := A$:

$$A' + A = A + A \overset{\text{Defn}}{=} (A \cup A) \setminus (A \cap A) = A \setminus A = \emptyset.$$

Da wie bereits gezeigt, $\emptyset$ ein Neutralelement in $(R, +)$ ist, haben wir somit bewiesen, dass A sein eigenes additives Inverses ist.

Multiplikation/Assoziativität: Da die Mengenschnittoperation bekanntermaßen assoziativ ist, ist hier eigentlich nichts zu zeigen.

Multiplikation/Kommutativität: Da die Mengenschnittoperation bekanntermaßen kommutativ ist, ist hier eigentlich nichts zu zeigen.

Multiplikation/Einselement: Wir behaupten, dass $1 := X$ das multiplikative Neutralelement ist. Sei also $A \in R$ beliebig. **Zu zeigen:** $A \cdot 1 = 1 \cdot A = A$.
Wegen Kommutativität reicht es aus, $A \cdot 1 = A$ zu zeigen. Es gilt

$$A \cdot 1 = A \cap X = A,$$

weil $A \in R = \mathcal{P}(X)$ und damit $A \subseteq X$ gilt. Also ist X ein Neutralelement für $(R, \cdot)$.

Linksdistributivität: Seien $A, B, C \in R$ beliebig. **Zu zeigen:** $A \cdot (B + C) = (A \cdot B) + (A \cdot C)$.
Da es sich auf beiden Seiten der Gleichung um Mengen handelt, reicht es aus, für alle $x \in X$

zu zeigen, dass $x \in A \cdot (B + C)$ gdw. $x \in (A \cdot B) + (A \cdot C)$.
Sei also $x \in X$ beliebig. Es gilt

$$\begin{aligned} x \in A \cdot (B + C) &\overset{\text{Defn}}{\iff} x \in A \cap ((B \cup C) \setminus (B \cap C)) \\ &\overset{(6\cdot1)}{\iff} x \text{ in } A \text{ und } x \text{ in exakt einer der Mengen } B, C \\ &\iff x \text{ in exakt einer der Mengen } A \cap B, A \cap C \\ &\overset{(6\cdot1)}{\iff} x \in (A \cdot B) + (A \cdot C). \end{aligned}$$

Also gilt $A \cdot (B + C) = (A \cdot B) + (A \cdot C)$. Also weist $(R, +, \cdot)$ linksdistributivität auf.

Rechtsdistributivität: Da Multiplikation kommutativ ist, folgt Rechtsdistributivität automatisch aus Linksdistributivität.

Darum erfüllt $(R, +, \cdot)$ die Axiome eines Rings und dieser Ring hat ein Einselement und heißt kommutativ, weil hier Multiplikation kommutativ ist. ■

Beweis (von Behauptung 6·1, Ansatz II). Ein scharfes Auge erkennt, dass wir Teilmengen von X mit binären Tupeln identifizieren kann. Vielmehr wollen wir diese Menge von binären Tupeln mit einer bekannten algebraischen Struktur in Verbindung setzen, also betrachten wir konkret die Abbildungen

$$\begin{array}{rcccl} \Phi & : & \prod_{x\in X}\mathbb{Z}/2\mathbb{Z} & \to & \mathcal{P}(X) \\ & : & \alpha & \mapsto & \operatorname{supp}(\alpha) := \{x\in X \mid \alpha_x = 1\} \end{array}$$

$$\begin{array}{rcccl} \Psi & : & \mathcal{P}(X) & \to & \prod_{x\in X}\mathbb{Z}/2\mathbb{Z} \\ & : & A & \mapsto & (\mathbf{1}_A(x))_{x\in X} \end{array}$$

um Elemente aus dem einen Raum auf Elemente aus dem anderen zu übertragen. Nun ist $\mathbb{Z}/2\mathbb{Z}$ bekanntermaßen ein kommutativer Ring (eigentlich ein Körper). Darum ist das Produkt $\prod_{x\in X}\mathbb{Z}/2\mathbb{Z}$, versehen mit punktweise Addition und punktweise Multiplikation, ebenfalls ein kommutativer Ring.

Darum reicht es aus **zu zeigen**, dass Φ eine Bijektion ist, die die Operationen erhält (auch *Isomorphismus* genannt).

Bijektion: Wir beobachten, dass

$$\begin{array}{rcl} \Phi(\Psi(A)) &=& \{x\in X \mid \Psi(A)_x = 1\} \\ &=& \{x\in X \mid \mathbf{1}_A(x) = 1\} \\ &=& \{x\in X \mid x\in A\} \quad = \quad A \end{array}$$

für alle $A\in\mathcal{P}(X)$ und

$$\begin{array}{rcl} \Psi(\Phi(\alpha)) &=& (\mathbf{1}_{\Phi(\alpha)}(x))_{x\in X} \\ &=& (\mathbf{1}_{\{x'\in X\mid \alpha_{x'}=1\}}(x))_{x\in X} \\ &=& \left(\begin{cases} 1 & : \quad x\in\{x'\in X\mid\alpha_{x'}=1\} \\ 0 & : \quad \text{sonst} \end{cases}\right)_{x\in X} \\ &=& \left(\begin{cases} 1 & : \quad \alpha_x = 1 \\ 0 & : \quad \alpha_x = 0 \end{cases}\right)_{x\in X} \quad = \quad (\alpha_x)_{x\in X} = \alpha \end{array}$$

für alle $\alpha\in\prod_{x\in X}\mathbb{Z}/2\mathbb{Z}$. Also $\Phi\circ\Psi = \mathrm{id}$ und $\Psi\circ\Phi = \mathrm{id}$. Darum sind Φ und Ψ Bijektion (und invertieren einander).

Erhaltung der Operationen: Seien $\alpha,\beta\in\prod_{x\in X}\mathbb{Z}/2\mathbb{Z}$. **Zu zeigen:** $\Phi(\alpha+\beta) = \Phi(\alpha)+\Phi(\beta)$ und $\Phi(\alpha\cdot\beta) = \Phi(\alpha)\cdot\Phi(\beta)$. Es gilt

$$\begin{array}{rcl} \Phi(\alpha+\beta) &=& \{x\in X \mid (\alpha+\beta)_x = 1\} \\ &=& \{x\in X \mid \alpha_x+\beta_x = 1\}, \\ && \quad \text{da Operationen auf } \prod_{x\in X}\mathbb{Z}/2\mathbb{Z} \text{ punktweise definiert sind} \\ &=& \{x\in X \mid \alpha_x = 1 \text{ od. } \beta_x = 1, \text{ aber nicht beides}\} \\ &=& (\{x\in X\mid\alpha_x=1\}\cup\{x\in X\mid\beta_x=1\}) \\ && \setminus(\{x\in X\mid\alpha_x=1\}\cap\{x\in X\mid\beta_x=1\}) \\ &=& (\Phi(\alpha)\cup\Phi(\beta))\setminus(\Phi(\alpha)\cap\Phi(\beta)) \quad \text{per Konstruktion von } \Phi \\ &=& \Phi(\alpha)+\Phi(\beta) \quad \text{per Definition von Addition in } R \end{array}$$

und

$$\begin{array}{rcl} \Phi(\alpha\cdot\beta) &=& \{x\in X \mid (\alpha\cdot\beta)_x = 1\} \\ &=& \{x\in X \mid \alpha_x\cdot\beta_x = 1\}, \\ && \quad \text{da Operationen auf } \prod_{x\in X}\mathbb{Z}/2\mathbb{Z} \text{ punktweise definiert sind} \\ &=& \{x\in X \mid \alpha_x = 1 \text{ und. } \beta_x = 1\} \\ &=& \{x\in X \mid \alpha_x = 1\}\cap\{x\in X\mid\beta_x=1\} \\ &=& \Phi(\alpha)\cap\Phi(\beta) \quad \text{per Konstruktion von } \Phi \\ &=& \Phi(\alpha)\cdot\Phi(\beta) \quad \text{per Definition von Multiplikation in } R. \end{array}$$

Darum präserviert Φ die Operationen.

Zusammegefasst haben wir gezeigt, dass $(\mathcal{P}(X),+,\cdot)$ zu dem kommutativen Ring, $(\prod_{x\in X}\mathbb{Z}/2\mathbb{Z},+,\cdot)$ isomorph ist (und zwar mittels Φ), und damit dass $(R,+,\cdot)$ selbst ein kommutativer Ring ist. ■

Bemerkung. Aus diesem Beweis geht hervor, dass das Nullelement durch $\Phi((0)_{x\in X}) = \emptyset$ und das Einselement durch $\Phi((1)_{x\in X}) = X$ gegeben sind.

Aufgabe 6·2

Wir identifizieren $\mathbb{C}$ mit $\mathbb{R}^2$ mittel der Abbildungen

$$\begin{array}{rcl} z \in \mathbb{C} & \mapsto & \binom{\mathfrak{Re}(z)}{\mathfrak{Im}(z)} \in \mathbb{R}^2, \\ \mathbf{x} \in \mathbb{R}^2 & \mapsto & x_1 + \imath x_2 \in \mathbb{C}. \end{array}$$

(a) Behauptung. *Für alle $z \in \mathbb{C} \setminus \{0\}$ existieren eindeutige Werte $r \in (0, \infty)$ und $\alpha \in [0, 2\pi)$, dann $z = r \cdot \binom{\cos(\alpha)}{\sin(\alpha)}$ (unter der o. s. Identifizierung).* ◊

Beweis. Unter der Identifizierung können wir $z = \binom{x}{y}$ schreiben, wobei $x, y \in \mathbb{R}$. Da $z \neq 0 = \binom{0}{0}$, muss entweder $x \neq 0$ oder $y \neq 0$ gelten.

Zur **Existenz**: Sei $r := \sqrt{x^2 + y^2}$. Dann $r > 0$ weil $(x, y) \neq (0, 0)$.
Um α zu bestimmen, werden folgende Fälle aufgeführt:

Fall 1. $y = 0$. Dann $x \neq 0$ und in diesem Falle gilt $r = |x|$. Man setze $\alpha := \begin{cases} 0 & : \quad x > 0 \\ \pi & : \quad x < 0 \end{cases}$.
Dann $r\cos(\alpha) := \begin{cases} r & : \quad x > 0 \\ -r & : \quad x < 0 \end{cases} = x$ und $r\sin(\alpha) = 0$.

Fall 2. $y > 0$. Man setze $\alpha \in (0, \pi)$ der eindeutige Winkel mit $\cos(\alpha) = \frac{x}{r}$. Dann $r\cos(\alpha) = x$ und $r\sin(\alpha) = r\sqrt{1 - \cos^2(\alpha)} = \sqrt{r^2 - (r\cos(\alpha))^2} = \sqrt{(x^2 + y^2) - x^2} = \sqrt{y^2} = |y| = y$.

Fall 3. $y < 0$. Man setze $\alpha \in (\pi, 2\pi)$ der eindeutige Winkel mit $\cos(\alpha) = \frac{x}{r}$. Dann $r\cos(\alpha) = x$ und $r\sin(\alpha) = r \cdot -\sqrt{1 - \cos^2(\alpha)} = -\sqrt{r^2 - (r\cos(\alpha))^2} = -\sqrt{(x^2 + y^2) - x^2} = -\sqrt{y^2} = -|y| = y$.

Darum gilt in allen Fällen $r \cdot \binom{\cos(\alpha)}{\sin(\alpha)} = \binom{r\cos(\alpha)}{r\sin(\alpha)} = \binom{x}{y} = z$.

Zur **Eindeutigkeit**: Seien $r_i \in (0, \infty)$, $\alpha_i \in [0, 2\pi)$ mit $r_i \cdot \binom{\cos(\alpha_i)}{\sin(\alpha_i)} = z$ für $i \in \{1, 2\}$. **Zu zeigen:** $r_1 = r_2$ und $\alpha_1 = \alpha_2$. Es gilt

$$\begin{array}{rcl} r_1^2 & = & r_1^2(\cos^2(\alpha_1) + \sin^2(\alpha_1)) \\ & = & (r_1\cos(\alpha_1))^2 + (r_1\sin(\alpha_1))^2 \\ & = & x^2 + y^2 \\ & = & (r_2\cos(\alpha_2))^2 + (r_2\sin(\alpha))^2 \\ & = & r_2^2(\cos^2(\alpha_2) + \sin^2(\alpha_2)) \qquad = \quad r_2^2, \end{array}$$

woraus sich ergibt, dass $r_1 = r_2$, weil $r_1, r_2 \geqslant 0$. Da $r_1, r_2 > 0$, folgt

$$\begin{array}{rcccccccc} \cos(\alpha_1) & = & \dfrac{r_1\cos(\alpha_1)}{r_1} & = & \dfrac{x}{r_1} & = & \dfrac{x}{r_2} & = & \dfrac{r_2\cos(\alpha_2)}{r_2} & = & \cos(\alpha_2) \\ \sin(\alpha_1) & = & \dfrac{r_1\sin(\alpha_1)}{r_1} & = & \dfrac{y}{r_1} & = & \dfrac{y}{r_2} & = & \dfrac{r_2\sin(\alpha_2)}{r_2} & = & \sin(\alpha_2) \end{array}$$

Da $\alpha_1, \alpha_2 \in [0, 2\pi)$ und wegen Injektivität von $\cos$ auf $[0, \pi)$ und $[\pi, 2\pi)$ und der Symmetrie um π, erhalten wir aus $\cos(\alpha_1) = \cos(\alpha_2)$, dass (i) $\alpha_1 = \alpha_2$ oder (ii) $\alpha_1 = 2\pi - \alpha_2$ gelten muss.
Falls (ii) gilt, so gilt $\sin(\alpha_1) = \sin(2\pi - \alpha_2) = -\sin(\alpha_2)$. Da aber $\sin(\alpha_1) = \sin(\alpha_2)$, folgt daraus $\sin(\alpha_2) = 0$, und damit (iii) $\alpha_2 = 0$ oder (iv) π. Falls (iii) gilt, so gilt wegen (ii) $\alpha_1 = 2\pi - 0 = 2\pi$, was ein Widerspruch ist, weil $\alpha_1 \in [0, 2\pi)$. Darum muss (iv) gelten. Wegen (ii) gilt also $\alpha_1 = 2\pi - \pi = \pi = \alpha_2$.
Zusammegefasst gilt entweder (i) $\alpha_1 = \alpha_2$ oder (ii), aus dem sich (iv) ergibt, was wiederum $\alpha_1 = \alpha_2$ zur Folge hat. D. h., in allen Fällen gilt $\alpha_1 = \alpha_2$.

Darum gelten $r_1 = r_2$ und $\alpha_1 = \alpha_2$. Also ist die Darstellung eindeutig. ■

(b) Behauptung. *Seien $z_1, z_2 \in \mathbb{C} \setminus \{0\}$ mit Darstellungen $z_i = r_i \cdot \binom{\cos(\alpha_i)}{\sin(\alpha_i)}$ für $i \in \{1, 2\}$. Dann gilt die Rechenregel $z_1 z_2 = r_1 r_2 \cdot \binom{\cos(\alpha_1 + \alpha_2)}{\sin(\alpha_1 + \alpha_2)}$.* ◊

Beweis. Multiplikation in $\mathbb{C}$ liefert

$$\begin{array}{rcl} z_1 z_2 & = & \binom{\mathfrak{Re}(z_1)\,\mathfrak{Re}(z_2) - \mathfrak{Im}(z_1)\,\mathfrak{Im}(z_2)}{\mathfrak{Re}(z_1)\,\mathfrak{Im}(z_2) + \mathfrak{Re}(z_1)\,\mathfrak{Im}(z_2)} \\ & = & \binom{r_1\cos(\alpha_1)\cdot r_2\cos(\alpha_2) - r_1\sin(\alpha_1)\cdot r_2\sin(\alpha_2)}{r_1\cos(\alpha_1)\cdot r_2\sin(\alpha_2) + r_1\cos(\alpha_1)\cdot r_2\sin(\alpha_2)} \end{array}$$

$$
\begin{aligned}
&= r_1 r_2 \begin{pmatrix} \cos(\alpha_1)\cos(\alpha_2) - \sin(\alpha_1)\sin(\alpha_2) \\ \cos(\alpha_1)\sin(\alpha_2) + \cos(\alpha_1)\sin(\alpha_2) \end{pmatrix} \\
&= r_1 r_2 \begin{pmatrix} \cos(\alpha_1+\alpha_2) \\ \sin(\alpha_1+\alpha_2) \end{pmatrix}.
\end{aligned}
$$

Die letzte Vereinfachung folgt aus der trigonometrischen Additionsregel. ■

(c) Behauptung (de Moivre). *Sei $z \in \mathbb{C}\backslash\{0\}$ mit Darstellungen $z = r \cdot \begin{pmatrix} \cos(\alpha) \\ \sin(\alpha) \end{pmatrix}$. Dann gilt die Potenzregel $z^n = r^n \cdot \begin{pmatrix} \cos(n\alpha) \\ \sin(n\alpha) \end{pmatrix}$ für alle $n \in \mathbb{N}$.* ◊

Beweis. Wir beweisen dies per Induktion über n.

Induktionsanfang: Die Gleichung gilt offensichtlich für $n = 1$.

Induktionsvoraussetzung: Sei $n > 1$. Angenommen, $z^{n-1} = r^{n-1} \cdot \begin{pmatrix} \cos((n-1)\alpha) \\ \sin((n-1)\alpha) \end{pmatrix}$.

Induktionsschritt: Zu zeigen: $z^n = r^n \cdot \begin{pmatrix} \cos(n\alpha) \\ \sin(n\alpha) \end{pmatrix}$.

Per rekursive Definition vom Potenzieren gilt zunächst $z^n = z^{n-1} \cdot z$ (Multiplikation innerhalb der Algebra $\mathbb{C}$). Aufgabe 6-2(b) zur Folge gilt somit

$$
\begin{aligned}
z^n = z^{n-1} \cdot z &\overset{\text{IV}}{=} r^{n-1} \cdot \begin{pmatrix} \cos((n-1)\alpha) \\ \sin((n-1)\alpha) \end{pmatrix} \cdot r \cdot \begin{pmatrix} \cos(\alpha) \\ \sin(\alpha) \end{pmatrix} \\
&\overset{(2b)}{=} r^{n-1} r \cdot \begin{pmatrix} \cos((n-1)\alpha + \alpha) \\ \sin((n-1)\alpha + \alpha) \end{pmatrix} \\
&= r^n \cdot \begin{pmatrix} \cos(n\alpha) \\ \sin(n\alpha) \end{pmatrix}.
\end{aligned}
$$

Darum gilt die Gleichung für n.

Also gilt die Gleichung für alle $n \in \mathbb{N}_0$. ■

Bemerkung. Wir können eigentlich zeigen, dass dies für alle $n \in \mathbb{Z}$ gilt. Für $n = 0$, gilt $z^0 = 1 + i0 = \binom{1}{0} = r^0 \cdot \begin{pmatrix} \cos(0\alpha) \\ \sin(0\alpha) \end{pmatrix}$. Für $n = -1$ liefert uns die Rechenregel für Multiplikation innerhalb $\mathbb{C}$, dass $r^{-1} \cdot \begin{pmatrix} \cos(-\alpha) \\ \sin(-\alpha) \end{pmatrix}$ eine hinreichende Konstruktion für ein Inverses von z ist, und darum ist dies wegen Eindeutigkeit des Inverses gleich z^{-1}. Für $n < 0$ allgemein wenden wir schließlich $z^n = (z^{-1})^{|n|} = (r^{-1} \cdot \begin{pmatrix} \cos(-\alpha) \\ \sin(-\alpha) \end{pmatrix})^{|n|} = (r^{-1})^{|n|} \cdot \begin{pmatrix} \cos(|n| \cdot -\alpha) \\ \sin(|n| \cdot -\alpha) \end{pmatrix} = r^n \cdot \begin{pmatrix} \cos(n\alpha) \\ \sin(n\alpha) \end{pmatrix}$ an. ◊

Aufgabe 6·3

Es sei K ein Körper und $F := K \times K$ versehen mit den Operationen $+, \cdot : F \times F \to F$, definiert vermöge

$$\begin{aligned}(a,b) + (a',b') &= (a+a', b+b') \\ (a,b) \cdot (a',b') &= (aa' - bb', ab' + a'b)\end{aligned}$$

für alle $a, b, a', b' \in K$.

Wir werden folgendes klassifizierendes Ergebnis verwenden, um die Aufgaben zu behandeln (und dieses Resultat dann anschließend beweisen).

Satz 6·6 $(F, +, \cdot)$ *ist genau dann ein Körper, wenn* $a^2 + b^2 \neq 0$ *innerhalb* K *für alle* $(a,b) \in F \setminus \{(0,0)\}$. ◊

(a) Behauptung. *Sei* $K = \mathbf{F}_2 = \mathbb{Z}/2\mathbb{Z}$. *Dann ist* $(F, +, \cdot)$ *kein Körper.* ◊

Beweis. Da $(a,b) := (1,1) \in F \setminus \{(0,0)\}$ und $a^2 + b^2 = 1 + 1 = 0$ innerhalb $K = \mathbb{Z}/2\mathbb{Z}$, ist Satz 6·6 zufolge F kein Körper. Es scheitert genau das Axiom der Existenz multiplikativer Inverser. (Nichtsdestotrotz bildet F einen kommutativen Ring mit Einselement.) ■

(b) Behauptung. *Sei* $K = \mathbf{F}_3 = \mathbb{Z}/3\mathbb{Z}$. *Dann ist* $(F, +, \cdot)$ *ein Körper.* ◊

Beweis. Laut Satz 6·6 reicht es aus für alle $(a,b) \in F \setminus \{(0,0)\}$ **zu zeigen**, dass $a^2 + b^2 \neq 0$ innerhalb $K = \mathbb{Z}/3\mathbb{Z}$. Sei also $(a,b) \in F \setminus \{(0,0)\}$ beliebig. Da $a \neq 0$ oder $b \neq 0$ gibt es folgende Fälle:

Fall 1. $a = 0$, $b \neq 0$. Dann $b = \pm 1 \mod 3$. Also $a^2 + b^2 = 0 + 1 = 1 \not\equiv 0 \mod 3$.

Fall 2. $a \neq 0$, $b = 0$. Dann $a = \pm 1 \mod 3$. Also $a^2 + b^2 = 1 + 0 = 1 \not\equiv 0 \mod 3$.

Fall 3. $a \neq 0$, $b \neq 0$. Dann $a, b = \pm 1 \mod 3$. Also $a^2 + b^2 = 1 + 1 = 2 \not\equiv 0 \mod 3$.

Also gilt in jedem Falle $a^2 + b^2 \neq 0$. Darum bildet F einen Körper. ■

Um Satz 6·6 zu beweisen, brauchen wir zunächst folgendes Zwischenresultat.

Lemma 6·9 $(F, +, \cdot)$ *ist genau dann ein Körper, wenn in der Teilstruktur* $(F, \cdot)$ *multiplikative Inverse existieren für jedes Element.* ◊

Beweis. Da die Teilstruktur, $(F, +)$, durch die Produktstruktur $(K, +) \times (K, +)$ gegeben ist, dessen Faktoren all kommutative Gruppen sind, ist $(F, +)$ eine kommutative Gruppe. Das heißt, die **Additionsaxiome** unter den Körperaxiomen sind allesamt erfüllt. (Insbesondere ist das Nullelement durch $0_F = (0,0)$ gegeben.)

Bei den **Multiplikationsaxiomen** sehen wir dass Kommutativität offensichtlich gilt, weil die o. s. Definitions von Multiplikation in den Argumenten offensichtlich symmetrisch ist, und weil die Operationen in K kommutativ sind. Es gilt auch $(a,b) \cdot (1,0) = (a \cdot 1 - b \cdot 0, a \cdot 0 + 1 \cdot b) = (a,b)$, sodass $1_F := (1,0)$ das Einselement von F ist. Assoziativität von Multiplikation ist auch erfüllt, weil

$$\begin{aligned}(a,b) \cdot ((a',b') \cdot (a'',b'')) &= (a,b) \cdot (a'a'' - b'b'', a'b'' + a''b') \\ &= (a(a'a'' - b'b'') - b(a'b'' + a''b'), a(a'b'' + a''b') + (a'a'' - b'b'')b) \\ &= (aa'a'' - ab'b'' - ba'b'' - ba''b', aa'b'' + aa''b' + a'a''b - b'b''b) \\ &= \boxed{(aa'a'' - ab'b'' - a'bb'' - a''bb', aa'b'' + aa''b' + a'a''b - bb'b'')}\end{aligned}$$

und

$$\begin{aligned}((a,b) \cdot (a',b')) \cdot (a'',b'') &= (aa' - bb', ab' + a'b) \cdot (a'',b'') \\ &= ((aa' - bb')a'' - (ab' + a'b)b'', (aa' - bb')b'' + a''(ab' + a'b)) \\ &= (aa'a'' - bb'a'' - ab'b'' - a'bb'', aa'b'' - bb'b'' + a''ab' + a''a'b) \\ &= \boxed{(aa'a'' - ab'b'' - a'bb'' - a''bb', aa'b'' + aa''b' + a'a''b - bb'b'')} \\ &= (a,b) \cdot ((a',b') \cdot (a'',b''))\end{aligned}$$

für alle $(a,b), (a',b'), (a'',b'') \in F$. Darum ist $(F, \cdot)$ assoziativ, kommutativ, und hat ein Neutralelement.

Wegen Kommutativität von Multiplikation in F, ist **Distributitivität** zu Linksdistributivität äquivalent, und da

$$\begin{aligned}(a,b)\cdot((a',b')+(a'',b'')) &= (a,b)\cdot(a'+a'',b'+b'')\\ &= (a(a'+a'')-b(b'+b''),a(b'+b'')+(a'+a'')b)\\ &= ((aa'-bb')+(aa''-bb''),(ab'+a'b)+(ab''+a''b))\\ &= (aa'-bb',ab'+a'b)+(aa''-bb'',ab''+a''b)\\ &= (a,b)\cdot(a',b')+(a,b)/cdot(a'',b'')\end{aligned}$$

für alle $(a,b),(a',b'),(a'',b'')\in F$, ist dies erfüllt.

Anhand der o. s. Erkenntnisse darüber, welchen Axiomen $(F,+,\cdot)$ bereits genügt, erhalten wir, dass $(F,+,\cdot)$ genau dann ein Körper, wenn in $(F,\cdot)$ jedes Element ein Inverses hat. ■

Jetzt können wir uns dem Beweis von Satz 6·6 widmen

Beweis (von Satz 6·6). Laut Lemma 6·9 gilt $(F,+,\cdot)$ ein Körper gdw. jedes Element in F hat ein multiplikatives Inverses. Darum reicht es aus **zu zeigen**, dass

$$\forall(a,b)\in F\setminus\{0_F\}:\exists(a',b')\in F:(a,b)\cdot(a',b')=1_F \iff \forall(a,b)\in F\setminus\{0_F\}:a^2+b^2\neq 0$$

gilt.[a]

($\Longleftarrow$). Angenommen, $a^2+b^2\neq 0$ für alle $(a,b)\in F\setminus\{0_F\}$. Sei $(a,b)\in F\setminus\{0_F\}$ beliebig. **Zu zeigen:** (a,b) sei innerhalb F invertierbar.
Per Annahme gilt nun $r:=a^2+b^2\neq 0$ und somit ist r innerhalb K invertierbar. Setze $(a',b'):=(r^{-1}a,-r^{-1}b)$. Dann

$$\begin{aligned}(a,b)\cdot(a',b') &= (a\cdot r^{-1}a-b(-r^{-1}b),a(-r^{-1}b)+(r^{-1}a)b)\\ &= (r^{-1}(a^2+b^2),0)\\ &= (r^{-1}r,0)\\ &= (1,0)\\ &= 1_F.\end{aligned}$$

Also ist jedes $(a,b)\in F\setminus\{0_F\}$ innerhalb F invertierbar.

($\Longrightarrow$). Angenommen, jedes Element in $F\setminus\{0_F\}$ sei invertierbar.
Wie oben erklärt, ist $(F,+,\cdot)$ somit ein Körper.
Sei $(a,b)\in F\setminus\{0_F\}$ beliebig. **Zu zeigen:** $a^2+b^2\neq 0$.
Da $(a,b)\neq 0_F=(0,0)$, gilt $a\neq 0$ oder $b\neq 0$ und damit gilt auch $(a,-b)\in F\setminus\{0_F\}$.
Da F ein Körper ist, sind (a,b) und $(a,-b)$ und folglich auch das Produkt $(a,b)\cdot(a,-b)$ invertierbar.
Da F ein Körper ist, bedeutet dies wiederum, dass $(a,b)\cdot(a,-b)\neq 0_F$ gilt. Nun,

$$(a,b)\cdot(a,-b) = (aa-b(-b),a(-b)+ab) = (a^2+b^2,0).$$

Darum gilt $(a^2+b^2,0)=(a,b)\cdot(a,-b)\neq 0_F=(0,0)$, woraus sich $a^2+b^2\neq 0$ ergibt. ■ **(Satz 6·6)**

[a] Man beachte: Wegen multiplikativer Kommutativität folgt aus $(a,b)\cdot(a',b')=1_F$, dass auch $(a',b')\cdot(a,b)=1_F$ gilt.

TEIL II
Selbstkontrollenaufgaben

SKA Blatt 4

Woche 4

SKA 4·1

Seien X, Y nicht leere Mengen. Einer Abbildung, $f : X \to Y$, können wir eindeutig die Relation $\mathsf{Gph}(f) := \{(x, y) \in X \times Y \mid f(x) = y\}$ zuordnen. Dies nennt sich der **Graph von** f (siehe [Sin20, §2.3]—dort wird dies mit Γ_f bezeichnet). Hier ist $\mathsf{Gph}(f)$ also eine Relation auf $X \times Y$. In der Tat *setzen* manche Werke Funktionen mit ihrem Graphen gleich (siehe bspw. [Jec97, S.11]), aber dies ist streng genommen nicht die ganze Wahrheit.

SKA 4·2

Hinweis: Hier scheint im Punkt (ii) etwas verwechselt worden zu sein.

Seien M, N Mengen und $R \subseteq M \times N$.

Behauptung 4·1 *Angenommen, R erfülle folgende Eigenschaften:*

- **(i)** $\forall x \in M : \exists y \in N : (x, y) \in R$
- **(ii)** $\forall x \in M : \forall y, y' \in N : (x, y), (x, y') \in R \Rightarrow y = y'$

Dann existiert eine (notwendigerweise eindeutige) Funktion, $f : M \to N$, so dass $\mathsf{Gph}(f) = R$. ◊

Beweis. Wir definieren $f : M \to N$ durch

$$f(x) \quad = \quad y$$

für $(x, y) \in R$. Offensichtlich gilt $\mathsf{Gph}(f) = \{(x, y) \in M \times N \mid f(x) = y\} = \{(x, y) \in M \times N \mid (x, y) \in R\} = R$.

Zu zeigen: (1) f ist überall definiert; (2) f ist wohldefiniert.

Überall definiert: Sei $x \in M$. **Zu zeigen:** $f(x) = y$ für ein $y \in N$.
Eigenschaft besagt, dass ein $y \in M$ existiert, so dass $(x, y) \in R$. Per Konstruktion erhalten wir, dass $f(x) = y$ gilt.

Wohldefiniertheit: Seien $x \in M$ und $y, y' \in N$. Angenommen, $f(x) = y$ und $f(x) = y'$.
Zu zeigen: $y = y'$.
Aus $f(x) = y$ und $f(x) = y'$ folgt $(x, y), (x, y') \in R$ per Konstruktion von f.
Eigenschaft besagt, dass $y = y'$.

Darum ist f eine Abbildung zwischen M und N und $\mathsf{Gph}(f) = R$. ■

SKA 4·3

Sei $X = \{a, b, c\}$ und betrachte die binäre Relation, $(\mathcal{P}(X), \leqslant)$, definiert durch

$$A \leqslant B \quad \Longleftrightarrow \quad X \setminus A \subseteq X \setminus B$$

für $A, B \in \mathcal{P}(X)$.

Behauptung. $(\mathcal{P}(X), \leqslant)$ *ist eine partielle Ordnung (auch »Halbordnung« genannt).* $\Diamond$

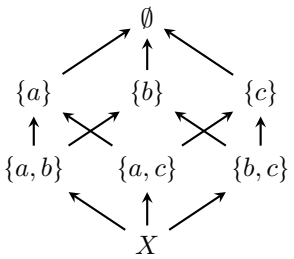
Es gibt nun 3 Ansätze, um dies zu zeigen.

Beweis (Ansatz I). Beobachte, dass für $A, B \in \mathcal{P}(X)$

$$\begin{aligned} A \leqslant B &\overset{\text{Defn}}{\iff} X \setminus A \subseteq X \setminus B \\ &\implies X \setminus (X \setminus A) \supseteq X \setminus (X \setminus B) \\ &\implies A \supseteq B, \text{ da } A, B \subseteq X \\ &\implies X \setminus A \subseteq X \setminus B \\ &\overset{\text{Defn}}{\iff} A \leqslant B, \end{aligned}$$

also $A \leqslant B \Leftrightarrow A \supseteq B$. Darum kann $(\mathcal{P}(X), \leqslant)$ mit $(\mathcal{P}(X), \supseteq)$ identifiziert werden. Letzteres ist bekanntermaßen eine Halbordnung. ■ **(Ansatz I)**

Beweis (Ansatz II). Im konkreten Falle von $X = \{a, b, c\}$ können wir die Relation durch ein *Hasse-Diagramm* skizzieren:



Man sieht, dass dies einen *Verband* und damit insbesondere eine Halbordnung bildet. ■ **(Ansatz II)**

Beweis (Ansatz III). Wir gehen die Axiome einer Halbordnung durch:

Reflexivität: Sei $A \in \mathcal{P}(X)$ beliebig. **Zu zeigen:** $A \leqslant A$.
Offensichtlich gilt $X \setminus A \subseteq X \setminus A$.
Per Konstruktion gilt also $A \leqslant A$.

Antisymmetrie: Seien $A, A' \in \mathcal{P}(X)$ beliebig.
Zu zeigen: $A \leqslant A'$ und $A' \leqslant A \Rightarrow A = A'$.
Es gilt

$$\begin{aligned} A \leqslant A' \text{ und } A' \leqslant A &\iff X \setminus A \subseteq X \setminus A' \text{ und } X \setminus A' \subseteq X \setminus A && \text{(per Konstruktion)} \\ &\implies X \setminus A = X \setminus A' && \text{(per Definition von Mengengleichheit)} \\ &\implies A = A', && \text{da } A, A' \subseteq X. \end{aligned}$$

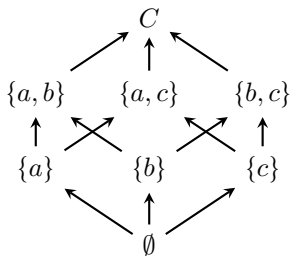
Transitivität: Seien $A, A', (a'', b'') \in \mathcal{P}(X)$ beliebig.
Zu zeigen: $A \leqslant A'$ und $A' \leqslant A'' \Rightarrow A \leqslant A''$.
Es gilt

$$\begin{aligned} A \leqslant A' \text{ und } A' \leqslant A'' &\iff X \setminus A \subseteq X \setminus A' \text{ und } X \setminus A' \subseteq X \setminus A'' \text{ (per Konstruktion)} \\ &\implies X \setminus A \subseteq X \setminus A'' \\ &\iff A \leqslant A'' \text{ (per Konstruktion).} \end{aligned}$$

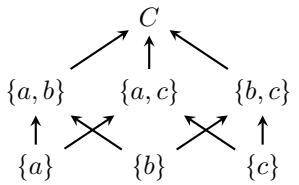
Darum erfüllt $(\mathcal{P}(X), \leqslant)$ die Axiome einer Halbordnung. ■ **(Ansatz III)**

SKA 4·4

Betrachten wir die Halbordnung aus [Sin20, Beispiel 2.4.2(2)]. Es sei also $C = \{a, b, c\}$ und die durch folgendes *Hasse-Diagramm* dargestellte Ordnungsrelation auf $\mathcal{P}(C)$:



Wenn wir das Element $\emptyset$ von $\mathcal{P}(C)$ entfernen sieht die Struktur folgendermaßen aus



Offensichtlich hat $(\mathcal{P}(C) \setminus \{\emptyset\}, \subseteq)$ kein kleinstes Element. Die Menge der minimalen Elementen ist durch $\{\{a\}, \{b\}, \{c\}\}$ gegeben. Also gibt es 3 minimale Elemente.

SKA 4·5

Sei W die Menge aller Wörter und Σ die Menge aller Buchstaben. O. E. können wir annehmen, dass jedes Wort $w \in W$ der Länge $|w| \geqslant 2$ ist. (In Sprachen wie Englisch, Russisch, usw. ist dies nicht der Fall, aber wir könnten diese trivialen Wörter einfach ausschließen.)

Betrachten wir die Relation $(W, \sim)$ gegeben durch

$$w \sim w' \quad :\Longleftrightarrow \quad f(w) = f(w), \tag{4·1}$$

wobei $f : W \to \Sigma$ die Abbildung mit $f(w) = 1$. Buchstabe in w für alle $w \in W$ ist.

Dann per Konstruktion reduziert f die Relation $(W, \sim)$ auf $(\Sigma, =)$. Aufgrund dessen und da $(\Sigma, =)$ eine Äquivalenzrelation ist, ist $(W, \sim)$ automatisch eine Äquivalenzrelation auch.

Eigentlich spielt est keine Rolle, wie die Funktion, f, aussieht. Solange die Reduktion (4·1) gilt, bleibt $(W, \sim)$ eine Äquivalenzrelation. Dies gilt also insbesondere ebenfalls, wenn f den zweitletzten Buchstaben von Wörtern berechnet.

SKA 4·6

(a) $$\begin{aligned} \textstyle\sum_{i=2}^{6}(-1)^i i^2 &= (-1)^2 \cdot 2^2 + (-1)^3 \cdot 3^2 + (-1)^4 \cdot 4^2 + (-1)^5 \cdot 5^2 + (-1)^6 \cdot 6^2 \\ &= 4 - 9 + 16 - 25 + 36 = 22 \end{aligned}$$

(b) $$\begin{aligned} \textstyle\prod_{j=1}^{4}(2j-1) &= (2 \cdot 1 - 1) + (2 \cdot 2 - 1) + (2 \cdot 3 - 1) + (2 \cdot 4 - 1) \\ &= 1 - 3 + 5 - 7 = -4 \end{aligned}$$

SKA 4·7

Behauptung 4·3 *Bezeichne mit $\Phi(n)$ die Aussage*

$$\textstyle\sum_{i=1}^{n}(-1)^i i^2 \quad = \quad (-1)^n \frac{1}{2} n(n+1). \tag{4·2}$$

Dann gilt $\forall n \in \mathbb{N} : \Phi(n)$. ◊

Beweis. Wir zeigen Behauptung 4·3 stumpf per Induktion.

Induktionsanfang: Sei $n = 1$. Dann

$$\begin{aligned}\sum_{i=1}^{n}(-1)^i i^2 &= (-1)^1 1^2 = -1\\ (-1)^n \tfrac{1}{2}n(n+1) &= (-1)^1 \tfrac{1}{2}\cdot 1\cdot(1+1) = -1\end{aligned}$$

Also gilt (4·2). Also gilt $\Phi(1)$.

Induktionsvoraussetzung: Sei $n > 1$. Angenommen, $\Phi(n-1)$ gilt.

Induktionsschritt: **Zu zeigen:** $\Phi(n)$ gilt, d. h. Gleichung (4·2) gilt.
Es gilt

$$\begin{aligned}\sum_{i=1}^{n}(-1)^i i^2 &= \sum_{i=1}^{n-1}(-1)^i i^2 + (-1)^n n^2\\ &= (-1)^{n-1}\tfrac{1}{2}(n-1)(n-1+1) + (-1)^n n^2\\ &\quad \text{wegen der IV}\\ &= (-1)^n\cdot(-\tfrac{1}{2}n(n-1) + n^2)\\ &= (-1)^n\cdot(-\tfrac{1}{2}n^2 + \tfrac{1}{2}n + n^2)\\ &= (-1)^n\cdot(\tfrac{1}{2}n^2 + \tfrac{1}{2}n)\\ &= (-1)^n\tfrac{1}{2}n(n+1).\end{aligned}$$

Also gilt (4·2). Also gilt $\Phi(n)$.

Also gilt $\forall n \in \mathbb{N} : \Phi(n)$. ■

Für die Summe $\sum_{i=3}^{n}(-1)^i i^2$ ist der Ausdruck lediglich

$$\begin{aligned}\sum_{i=3}^{n}(-1)^i i^2 &= \sum_{i=1}^{n}(-1)^i i^2 - (-1)^1\cdot 1 - (-1)^2 2^2\\ &= (-1)^n\tfrac{1}{2}n(n+1) - 3\end{aligned}$$

für alle $n \geqslant 3$. Sollten wir dies per Induktion beweisen wollen, brauchen wir lediglich im o. s. Beweis den **Induktionsanfang** auf $n = 3$ zu ändern. Der Rest bleibt erhalten.

Bemerkung 4·4 Man merkt, dass Induktion mit Deduzieren (»Ableiten«) nichts zu tun hat. Induktion ist schließlich nur ein Werkzeug, um Behauptungen zu *verifizieren*. Sie verschafft uns aber keine Mittel, um *auf die Behauptungen zu kommen*. In diesem konkreten Falle wurde Vorarbeit geleistet und *direkt* argumentiert, um auf den Ausdruck in (4·2) zu kommen. Ohne diese Arbeit wären wir auf diesen Ausdruck gar nicht gekommen. In dieser Vorarbeit steckt also die eigentliche mathematische Arbeit und dies bedarf etwas Kreativität, Intuition, usw. Häufig reicht diese Vorarbeit aber nur, um auf eine sinnvolle Behauptung zu kommen, und zum Schluss runden wir dies mit Induktion ab, um formal die behauptete Aussage zu bestätigen. Das ist die eigentliche Rolle von Induktion als Beweismittel. ♢

SKA 4·8

Kurzes Argument:
Wenn jede Farbe jeweils auf maximal 1 Karte vorkommt, gibt es $\leqslant 4\cdot 1$ Karten. Aber 5 Karten werden gewählt.

Ausführliches Argument:
Seien $X := \{\clubsuit, \diamondsuit, \heartsuit, \spadesuit\}$ die Menge der Farben und $Y := \{1,2,3,4,5\}$ die Indizes der Karten. Sei $f : X \to \mathcal{P}(Y)$ die Funktion, die der Wahl entspricht, d. h.

$$f(x) \quad = \quad \{y \in Y \mid \text{Karte } y \text{ hat Farbe } x\}$$

für alle Farben $x \in X$.

Nun, jede Karte, $y \in Y$, hat eine Farbe, sodass $y \in f(x)$ für ein $x \in X$. Also $Y \subseteq \bigcup_{x\in X} f(x)$. Und per Definition $f(x) \subseteq Y$ für alle $x \in X$. Darum $\bigcup_{x\in X} f(x) \subseteq Y$. Also

$$Y \quad = \quad \bigcup_{x\in X} f(x)$$

Andererseits sind die Mengen $(f(x))_{x\in X}$ paarweise disjunkt, da jede Karte höchstens eine Farbe hat. Also ist $(f(x))_{x\in X}$ eine *Partition* von Y. Darum

$$\begin{aligned}&|Y| = |\textstyle\bigcup_{x\in X} f(x)| = \sum_{x\in X}|f(x)| \leqslant |X|\cdot \max_{x\in X}|f(x)|\\ \Longrightarrow\quad &\max_{x\in X}|f(x)| \geqslant |Y|/|X| = 5/4 > 1\\ \Longrightarrow\quad &\exists x \in X : |f(x)| > 1\\ \Longrightarrow\quad &\exists x \in X : |f(x)| \geqslant 2\end{aligned}$$

Nach der Definition von f heißt dies, es gibt eine Farbe, $x \in \{\clubsuit, \diamondsuit, \heartsuit, \spadesuit\}$, so dass $\geqslant 2$ der gezogenen Karten der Farbe x sind.

SKA 4·9

Kurzes Argument:
Wenn jeder Kalendartag jeweils von maximal 17 Studierenden gefeiert wird, gibt es $\leqslant 366 \cdot 17 = 6222$ Studierende. Aber es gibt $\geqslant 7000$ Studierende.

Ausführliches Argument:
Seien $X = \{1.\text{ Jan}, 2.\text{ Jan}, \ldots, 31.\text{ Dez}\}$ die Menge der Kalendartage und $Y = \{x \mid x \text{ ein/e Studierende/r an der Uni Leipzig}\}$. Sei $f : X \to \mathcal{P}(Y)$ die Funktion, die der Wahl entspricht, d. h.

$$f(x) \quad = \quad \{y \in Y \mid \text{Studierende/r } y \text{ hat am Tag } x \text{ Geburtstag}\}$$

für alle Kalendartage $x \in X$.

Nun, jede/r Studierende/r, $y \in Y$, hat einen Geburtstag, sodass $y \in f(x)$ für ein $x \in X$. Also $Y \subseteq \bigcup_{x\in X} f(x)$. Und per Definition $f(x) \subseteq Y$ für alle $x \in X$. Darum $\bigcup_{x\in X} f(x) \subseteq Y$. Also

$$Y \quad = \quad \bigcup_{x\in X} f(x)$$

Andererseits sind die Mengen $(f(x))_{x\in X}$ paarweise disjunkt, da jede/r Studierende/r höchstens einen Geburtstag hat. Also ist $(f(x))_{x\in X}$ eine *Partition* von Y. Darum

$$\begin{array}{ll} & |Y| = |\bigcup_{x\in X} f(x)| = \sum_{x\in X} |f(x)| \leqslant |X| \cdot \max_{x\in X} |f(x)| \\ \Longrightarrow & \max_{x\in X} |f(x)| \geqslant |Y|/|X| \geqslant 7000/366 > 19 \\ \Longrightarrow & \exists x \in X : |f(x)| > 19 \\ \Longrightarrow & \exists x \in X : |f(x)| \geqslant 20 \end{array}$$

Nach der Definition von f heißt dies, es gibt einen Kalendartag, $x \in \{1.\text{ Jan}, 2.\text{ Jan}, \ldots, 31.\text{ Dez}\}$, so dass mindestens 20 Studierende x als Geburtstag feiern. Insbesondere gibt es 18 Menschen, die den gleichen Geburtstag feiern.

SKA 4·10

Behauptung 4·5 *Bezeichne mit $\Phi(n)$ die Aussage*

- *Für alle endlichen Mengen, $E_1, E_2, \ldots, E_n$, gilt $|\prod_{i=1}^n E_i| = \prod_{i=1}^n |E_i|$.*

Dann gilt $\forall n \in \mathbb{N} : \Phi(n)$. ◊

Beweis. Wir zeigen dies per Induktion mit den Fällen $n \leqslant 2$ als Induktionsanfang.

Induktionsanfang: Sei $n = 1$. Dann für alle Mengen, E_1

$$|\prod_{i=1}^1 E_i| \quad = \quad |E_1| \quad = \quad \prod_{i=1}^1 |E_i|$$

Also gilt $\Phi(1)$.

Sei $n = 2$. Laut Lemma 4·6 (siehe unten) gilt für alle endlichen Mengen E_1, E_2

$$|\prod_{i=1}^2 E_i| \quad = \quad |E_1 \times E_2| \quad = \quad |E_1| \cdot |E_2| \quad = \quad \prod_{i=1}^2 |E_i|.$$

Also gilt $\Phi(2)$.

Induktionsvoraussetzung: Sei $n > 2$. Angenommen, $\Phi(n-1)$ gilt.

Induktionsschritt: Seien $E_1, E_2, \ldots, E_n$ beliebige endliche Mengen.
Zu zeigen: $|\prod_{i=1}^n E_i| = \prod_{i=1}^n |E_i|$ gilt.
Es gilt

$$\begin{array}{lll} |\prod_{i=1}^n E_i| & = & |\prod_{i=1}^{n-1} E_i \times E_n| \\ & = & |\prod_{i=1}^{n-1} E_i| \cdot |E_n|, \quad \text{da } \Phi(2) \text{ gilt} \\ & = & \prod_{i=1}^{n-1} |E_i| \cdot |E_n| \quad \text{wegen der IV} \\ & = & \prod_{i=1}^{n} |E_i|. \end{array}$$

Also gilt $\Phi(n)$.

Also gilt $\forall n \in \mathbb{N} : \Phi(n)$. ■

Wir müssen noch den Fall für 2 Mengen beweisen.

Lemma 4·6 *Seien X, Y beliebige endliche Mengen. Dann $|X \times Y| = |X| \cdot |Y|$.* ◊

Beweis. Wir zeigen dies direkt. Seien $m := |X|$ und $n := |Y|$. Wegen Endlichkeit liegen m, n in $\mathbb{N}_0$.

Falls $m = 0$ oder $n = 0$, so gilt $X = \emptyset$ oder $Y = \emptyset$ und damit

$$|X \times Y| \quad = \quad |\emptyset| \quad = \quad 0 \quad = \quad m \cdot n \quad = \quad |X| \cdot |Y|.$$

Beschränken wir uns also auf den Famm $m, n > 0$. Per Definition von Kardinalität (siehe [Sin20, §3.3, S.54]) existieren also Bijektionen

$$\begin{array}{rcccl} f & : & \{0, 1, \ldots, m-1\} & \to & X, \\ g & : & \{0, 1, \ldots, n-1\} & \to & Y. \end{array}$$

(Wir fangen aus praktischen Gründen mit 0 statt 1 an.)
Definiere nun

$$\begin{array}{rcccl} h & : & \{0, 1, \ldots, mn-1\} & \mapsto & X \times Y \\ & : & k & \mapsto & (f(\mathsf{mod}(k, m)), g([k/m])), \end{array}$$

wobei $[\cdot] : \mathbb{R} \to \mathbb{Z}$ die Gaußklammerfunktion, die reelle Zahlen *abrundet*.
Zu zeigen: h ist eine wohldefinierte Bijektion.

Wohldefiniertheit: Für alle $k \in \{0, 1, \ldots, mn-1\}$ gilt $i := \mathsf{mod}(k, m) \in \{0, 1, \ldots, m-1\} = \mathsf{dom}(f)$ und $j := [k/m] \in \{0, 1, \ldots, n-1\} = \mathsf{dom}(g)$, sodass $f(i) \in X$ und $g(j) \in Y$ und damit $h(k) = (f(i), g(j)) \in X \times Y$.

Injektivität: Seien $k_1, k_2 \in \{0, 1, \ldots, mn-1\}$ beliebig. **Zu zeigen:** $h(k_1) = h(k_2) \Rightarrow k_1 = k_2$.
Nach [Sin20, Satz 3.4.2] existieren (eindeutige) Werte $q_1, q_2 \in \mathbb{Z}$ und $r_1, r_2 \in \{0, 1, \ldots, m-1\}$, so dass

$$\begin{array}{rcl} k_1 & = & mq_1 + r_1, \\ k_2 & = & mq_2 + r_2. \end{array} \tag{4·3}$$

Daraus lässt sich ableiten, dass $\mathsf{mod}(k_1, m) = r_1$, $\mathsf{mod}(k_2, m) = r_2$, $[k_1/m] = q_1$, und $[k_2/m] = q_2$. Darum gilt

$$\begin{array}{rcl} h(k_1) = h(k_2) & \overset{\text{Defn}}{\iff} & (f(r_1), g(q_1)) = (f(r_2), g(q_2)) \\ & \implies & f(r_1) = f(r_2) \text{ und } g(q_1) = g(q_2) \\ & \implies & r_1 = r_2 \text{ und } q_1 = q_2 \\ & & \text{da } f, g \text{ injektiv sind} \\ & \overset{(4\cdot3)}{\implies} & k_1 = mq_1 + r_1 = mq_2 + r_2 = k_2. \end{array}$$

Surjektivität: Sei $(x, y) \in X \times Y$. **Zu zeigen:** $(x, y) \in \mathsf{ran}(h)$.
Wegen der Surjektivität von f, g existieren nun $i \in \{0, 1, \ldots, m-1\}$ und $j \in \{0, 1, \ldots, n-1\}$, so dass $f(i) = x$ und $g(j) = y$.
Setze nun $k := mj + i$.
Dann $\mathsf{mod}(k, m) = i$ und $[k/m] = j$, sodass $h(k) = (f(i), g(j)) = (x, y)$.
Also gilt $(x, y) \in \mathsf{ran}(h)$.

Darum ist h ist eine wohldefinierte Bijektion, woraus sich per Definition von Kardinalität direkt ergibt, dass $|X \times Y| = mn = |X| \cdot |Y|$. ■

SKA 4·11

Um ein Argument zurückzuweisen, reicht es häufig aus, das Argument einfach *ausführlich* aufzuschreiben. Wir nehmen die Ausführung und formalisieren diese:

Behauptung. *Bezeichne mit $G(x)$, dass x ein Goldfisch ist. Für $n \in \mathbb{N}$ bezeichne mit $\Phi(n)$ folgende Aussage*

- *Für alle n-elementigen Mengen, X, von Fischen, wenn $\exists x \in X : G(x)$, dann $\forall x \in X : G(x)$.*

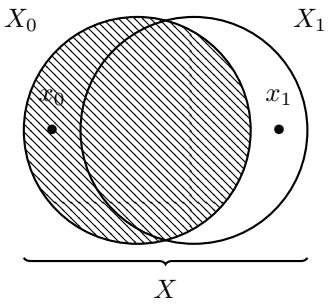
Dann $\forall n \in \mathbb{N} : \Phi(n)$ ◊

Beweis (ungültiges Argument). Dies wird per Induktion argumentiert.

Induktionsanfang: Betrachte eine 1-elementige Menge, X, von Fischen.
Angenommen, ein $x_0 \in X$ mit $G(x_0)$ existiere.
Da X nur dieses eine Element enthält, gilt offensichtlich $\forall x \in X : G(x)$.

Induktionsvoraussetzung: Sei $n \in \mathbb{N}$ mit $n \geqslant 1$. Angenommen, $\Phi(n)$ gilt.

Induktionsschritt: Sei X eine $n+1$-elementige Menge von Fischen.
Angenommen, ein $x_0 \in X$ mit $G(x_0)$ existiere. **Zu zeigen:** Für alle $x \in X$ gilt $G(x)$.
Fixiere einen anderen Fisch $x_1 \in X \setminus \{x_0\}$, was möglich ist, weil $|X| = n + 1 \geqslant 2$.
Setze $X_0 := X \setminus \{x_1\}$ und $X_1 := X \setminus \{x_0\}$.
Da $x_1 \neq x_0$, sind X_0, X_1 verschiedene n-elementige Mengen:



Fokussieren wir uns zunächst auf X_0 (die schattierte Teilmenge).
Da X_0 n-elementig ist und $x_0 \in X_0$ und $G(x_0)$, gilt per IV (†) $\forall x \in X_0 : G(x)$.

Wähle nun irgendeinen der Fische, $\tilde{x} \in X_0$ und setze $X' := X \setminus \{\tilde{x}\}$.
O. E. können wir $\tilde{x} := x_0$ wählen, sodass $X' = X_1$ gilt.
Die Teilmenge X_1 ist nun eine n-elementige Menge mit mindestens $n - 1$ Goldfischen.
Also $\exists x \in X_1 : G(x)$.
Per IV gilt also $\forall x \in X_1 : G(x)$.
Daraus und aus (†) folgt $\forall x \in X : G(x)$, da ja $X = X_0 \cup X_1$.

Darum gilt $\Phi(n+1)$.

Darum gilt $\forall n \in \mathbb{N} : \Phi(n)$. ■

Das Problem mit diesem Argument steckt im Induktionsschritt an genau dieser Stelle:

> *Also* $\exists x \in X' : G(x)$.

Im ursprünglichen Text ist dies die problematische Stelle:

> *Jetzt können wir aber auch einen der Goldfische rausnehmen und haben wieder ein Aquarium mit n Fischen und mindestens einem Goldfisch.*

Zurück aber zu unserer Formalisierung:
Wir haben etwas ausführlicher gezeigt, dass die Menge X' mindestens $n - 1$ Goldfische enthält. Wenn wir $\tilde{x} := x_0$ wählen entspricht dies der Größe des Schnitts $X_0 \cap X_1$. Das Diagramm mag andeuten, dass dieser Schnitt nicht leer ist, aber das Diagramm täuscht. Im Induktionsschritt setzen wir nur voraus, dass $n \geqslant 1$. Darum ist $n - 1 > 0$ nur garantiert, wenn stattdessen $n' \geqslant 2$ vorausgesetzt wird.

Das heißt das Induktionsargument ist faul, weil der Schritt $1 \rightsquigarrow 2$ implizit übersprungen wird.

SKA Blatt 5

Woche 5

SKA 5·2

Betrachtet sei die Teilbarkeitsrelation $(\mathbb{Z}, |)$. Wir prüfen, welche Axiome erfüllt sind und beurteilen aufgrund dessen, ob es sich um eine Äquivalenzrelation, partielle Ordnung, Abbildung, usw. handelt.

Reflexivität: Sei $a \in \mathbb{Z}$ beliebig. **Zu prüfen:** $a \mid a$?
Es gilt $a = 1 \cdot a$ und $1 \in \mathbb{Z}$.
Darum gilt $a \mid a$.
Also ist $(\mathbb{Z}, |)$ reflexiv.

Symmetrie: Betrachte bspw. $2, 10 \in \mathbb{Z}$.
Es gilt $2 \mid 10$ aber $10 \nmid 2$.
Darum ist $(\mathbb{Z}, |)$ nicht symmetrisch.

Antisymmetrie: Betrachte bspw. $2, -2 \in \mathbb{Z}$.
Es gelten $2 \mid -2$ und $-2 \mid 2$, aber $2 \neq -2$.
Darum ist $(\mathbb{Z}, |)$ nicht antisymmetrisch.

Transitivität: Seien, $a, b, c \in \mathbb{Z}$. **Zu prüfen:** $(a \mid b$ und $b \mid c) \Rightarrow a \mid c$?
Es gilt:

$$\begin{aligned} a \mid b \text{ und } b \mid c &\iff \exists k, j \in \mathbb{Z} : c = kb,\ b = ja \\ &\implies \exists k, j \in \mathbb{Z} : c = (kj)a \\ &\implies \exists m \in \mathbb{Z} : c = ma \\ &\iff a \mid c. \end{aligned}$$

Also ist $(\mathbb{Z}, |)$ transitiv.

Totalität: Betrachte bspw. $5, 7 \in \mathbb{Z}$.
Dann $5 \nmid 7$, $7 \nmid 5$, und $5 \neq 7$.
Darum ist $(\mathbb{Z}, |)$ nicht total.

Linkstotalität: Sei $a \in \mathbb{Z}$. **Zu prüfen:** $\exists b \in \mathbb{Z} : a \mid b$?
Wegen Reflexivität gilt nun $a \mid a$.
Also ist $(\mathbb{Z}, |)$ linkstotal.

Rechtseindeutigkeit: Betrachte bspw. $2, 10, 100 \in \mathbb{Z}$.
Es gilt $2 \mid 10$ und $2 \mid 100$, aber $10 \neq 100$.
Darum ist $(\mathbb{Z}, |)$ nicht rechtseindeutig.

Daraus folgt, dass $(\mathbb{Z}, |)$ weder eine Äquivalenzrelation noch eine (lineare) Ordnungsrelation noch eine partielle Ordnungsrelation ist. Und es gibt keine Funktion $f : \mathbb{Z} \to \mathbb{Z}$, so dass $\mathrm{Gph}(f) = |$.

Bemerkung: Man kann aber zeigen, das die Beschränkungen $(\mathbb{N}_0, |)$ und $(\mathbb{N}, |)$ zusätzlich Antisymmetrie aufweisen, sodass diese partielle Ordnungsrelationen sind.

SKA 5·3

Seien $a, b \in \mathbb{Z}$ mit $b > 0$. Um a durch b (mit Rest) zu teilen, setzt man

$$\begin{array}{rcl} q & := & [a/b] \in \mathbb{Z} \\ r & := & a - b \cdot q \in \mathbb{Z}. \end{array}$$

wobei $[\cdot] : \mathbb{R} \to \mathbb{Z}$ die Gaußklammerfunktion ist, die reelle Zahlen *abrundet*. Per Definition gilt

$$q \leqslant a/b < q + 1$$

also

$$0 \leqslant a - b \cdot q < b$$

Darum $r \in \{0, 1, \ldots, b - 1\}$.

Um dies aber *per Hand* bzw. im Kopf zu machen, verwendet man iterative Algorithmen, die aus Schritten besteht: a und b durch »einfachere« Zahlen ersetzen; mit einfacheren Zahlen teilen; Nachjustieren.

Welche Methode auch immer man anwendet hat dies mit dem Existenz-Teil des Beweises zu tun.

SKA 5·4

Behauptung 5·1 *Es gilt*

- **(i)** $\mathsf{ggT}(a, b) = \mathsf{ggT}(b, a)$*;*
- **(ii)** $\mathsf{ggT}(a, b) = \mathsf{ggT}(|a|, |b|)$*;*
- **(iii)** $\mathsf{ggT}(a, 0) = \mathsf{ggT}(0, a) = |a|$*, solange* $a \neq 0$*;*
- **(iv)** $\mathsf{ggT}(ca, cb) = |c|\,\mathsf{ggT}(a, b)$*, solange* $b, c \neq 0$*;*

für $a, b, c \in \mathbb{Z}$. ◊

Beweis. **(i):** Es gilt $\mathsf{ggT}(a, b) = \max\{d \in \mathbb{N} : d \mid a, b\} = \max\{d \in \mathbb{N} : d \mid b, a\} = \mathsf{ggT}(b, a)$.

(ii): Sei $d, x \in \mathbb{Z}$. Dann ist es einfach zu sehen, dass $d \mid x \Leftrightarrow d \mid |x|$.
Darum gilt $\mathsf{ggT}(a, b) = \max\{d \in \mathbb{N} : d \mid a, b\} = \max\{d \in \mathbb{N} : d \mid |a|, |b|\} = \mathsf{ggT}(|a|, |b|)$.

(iii): Laut (i) reicht es aus **zu zeigen** $\mathsf{ggT}(a, 0) = |a|$.
Es gilt $\mathsf{ggT}(a, 0) = \max D$, wobei $D := \{d \in \mathbb{N} : d \mid a, 0\}$.
(I) Setze $d_0 := |a| > 0$. Offensichtlich gilt $d_0 \mid a, 0$.
(II) Für alle $d \in \mathbb{N}$ gilt $d \mid a \Rightarrow |\frac{a}{d}| \geqslant 1$ (da $a, d \neq 0$) $\Rightarrow d \leqslant |a| = d_0$.
Daraus ergibt sich,

$$d_0 \overset{\text{(I)}}{\in} D \subseteq \{d \in \mathbb{N} : d \mid a\} \overset{\text{(II)}}{\subseteq} \{d \in \mathbb{N} : d \leqslant d_0\}$$

woraus sich ergibt, dass $d_0 \leqslant \max D \leqslant d_0$. Also $\mathsf{ggT}(a, 0) = \max D = d_0 = |a|$.

(iv): Setze $d_1 := \mathsf{ggT}(a, b)$ und $d_2 := \mathsf{ggT}(ca, cb)$. **Zu zeigen:** $d_2 = |c|d_1$.
Wir zeigen dies durch zwei Ungleichungen.
Es gilt

$$\begin{array}{rcl} d_1 \mid a, b & \Longleftrightarrow & \exists k, j \in \mathbb{Z} : a = kd_1 \text{ und } b = jd_1 \\ & \Longleftrightarrow & \exists k, j \in \mathbb{Z} : ca = kcd_1 \text{ und } cb = jcd_1 \\ & \Longleftrightarrow & \exists k, j \in \mathbb{Z} : ca = k|c|d_1 \text{ und } cb = j|c|d_1 \\ & & \text{da man z. B. } k \text{ durch } -k \text{ ersetzen kann} \\ & \Longleftrightarrow & |c|d_1 \mid ca, cb \end{array}$$

Per Maximalität von d_2 unter den positiven Teilern, folgt $\boxed{|c|d_1 \leqslant d_2}$.
Andererseits existieren nach dem *Lemma von Bézout* $u, v \in \mathbb{Z}$, so dass

$$d_1 = \mathsf{ggT}(a, b) = ua + vb$$

woraus sich ergibt, dass

$$\frac{|c|d_1}{d_2} \quad = \quad \underbrace{\pm u\frac{ca}{d_2} + \pm v\frac{cb}{d_2}}_{=:w} \tag{5·1}$$

Da $d_2 \mid ca, cb$ ist die rechte Seite von (5·1) in $\mathbb{Z}$. Und da $|c|, d_1, d_2 > 0$, ist die linke Seite von (5·1) strikt positiv, sodass $w \geqslant 1$ gilt. Darum $\boxed{|c|d_1 = w \cdot d_2 \geqslant 1 \cdot d_2}$. ■

Bemerkung. Ohne das *Lemma von Bézout* ist ein Beweis vom Letzten Punkt praktisch unmachbar.

SKA 5·5

Seien $a = 57$ und $b = 21$. Dann gilt $a = qb + r$, wobei $q = 2$ und $\boxed{r = 15}$. Es gilt $\text{ggT}(a, b) = 3$[a] und $\text{ggT}(b, r) = 3$[b] Also gilt $\text{ggT}(a, b) = \text{ggT}(b, \text{mod}(a, b))$, genau wie [Sin20, Lemma 3.4.5] allgemein besagt.

SKA 5·6

Für jeden Fall berechnen wir $\text{ggT}(a, b)$ mittels des Euklidischen Algorithmus (siehe [Sin20, Satz 3.4.7]).

a	b	Restberechnung (symbolisch)	Restberechnung (Werte)
1529	170	$a = b \cdot q_1 + r_1$	$1529 = 170 \cdot 8 + 169$
		$b = r_1 \cdot q_2 + r_2$	$170 = 169 \cdot 1 + \boxed{\mathbf{1}}$
		$r_1 = r_2 \cdot q_3 + r_3$	$169 = 1 \cdot 169 + 0$
13758	21	$a = b \cdot q_1 + r_1$	$13758 = 21 \cdot 655 + \boxed{\mathbf{3}}$
		$b = r_1 \cdot q_2 + r_2$	$21 = 3 \cdot 7 + 0$
210	45	$a = b \cdot q_1 + r_1$	$210 = 45 \cdot 4 + 30$
		$b = r_1 \cdot q_2 + r_2$	$45 = 30 \cdot 1 + \boxed{\mathbf{15}}$
		$r_1 = r_2 \cdot q_3 + r_3$	$30 = 15 \cdot 2 + 0$
1209	102	$a = b \cdot q_1 + r_1$	$1209 = 102 \cdot 11 + 87$
		$b = r_1 \cdot q_2 + r_2$	$102 = 87 \cdot 1 + 15$
		$r_1 = r_2 \cdot q_3 + r_3$	$87 = 15 \cdot 5 + 12$
		$r_2 = r_3 \cdot q_4 + r_4$	$15 = 12 \cdot 1 + \boxed{\mathbf{3}}$
		$r_3 = r_4 \cdot q_5 + r_5$	$12 = 3 \cdot 4 + 0$

SKA 5·7

Wir verwenden die Berechnungen aus der Tabelle in SKA 5.6.

a	b	Rest (symbolisch)	Rest (Werte)
1529	170	$r_1 = a - 8 \cdot b$	$169 = 1 \cdot a + -8 \cdot b$
		$r_2 = b - 1 \cdot r_1$	$\boxed{1 = -\mathbf{1} \cdot a + \mathbf{9} \cdot b}$
13758	21	$r_1 = a - 655 \cdot b$	$\boxed{3 = \mathbf{1} \cdot a + -\mathbf{655} \cdot b}$
210	45	$r_1 = a - 4 \cdot b$	$30 = 1 \cdot a + -4 \cdot b$
		$r_2 = b - 1 \cdot r_1$	$\boxed{15 = -\mathbf{1} \cdot a + \mathbf{5} \cdot b}$
1209	102	$r_1 = a - 11 \cdot b$	$87 = 1 \cdot a + -11 \cdot b$
		$r_2 = b - 1 \cdot r_1$	$15 = -1 \cdot a + 12 \cdot b$
		$r_3 = r_1 - 5 \cdot r_2$	$12 = 6 \cdot a + -71 \cdot b$
		$r_4 = r_2 - 1 \cdot r_3$	$\boxed{3 = -\mathbf{7} \cdot a + \mathbf{83} \cdot b}$

[a] weil $r = 3 \cdot 5$ und $3, 5 \in \mathbb{P}$ und nur $3 \mid 57$ gilt.
[b] weil $r = 3 \cdot 5$ und $3, 5 \in \mathbb{P}$ und nur $3 \mid 21$ gilt.

SKA 5·8

Das Lemma von Bézout wird mittels des Euklidischen Algorithmus bewiesen.
Korollar 3.4.10 baut darauf und charakterisiert, wann zwei Zahlen teilerfremd sind.
Lemma 3.4.12 baut darauf und zeigt $\forall i : b, a_i$ teilerfremd $\Rightarrow b, \prod_{i=1}^{n} a$ teilerfremd.
Satz 3.4.14 baut darauf und zeigt $p \mid \prod_{i=1}^{n} a_i \Rightarrow \exists i : p \mid a_i$ für p prim.

Dieses letzte Ergebnis wird im Induktionsargument instrumentalisiert, um Primzerlegungen der Länge k, l auf Primfaktorzerlegungen der Länge $k-1, l-1$ zu reduzieren, um das Induktionsargument voranzubringen.

Bemerkung 5·2 In der Algebra gibt es zwei Begriffe, die bei gewöhnlichen Primzahlen, sich anwenden lassen: *Irriduzibilität* und *prim*. Die Definition in abstrakten Kontexten von *prim* entspricht der Eigenschaft in [Sin20, Satz 3.4.14], während *Irriduzibilität* eher sich auf die Teilbarkeit bezieht. Etwas »Zufälligerweise« handelt es sich bei $\mathbb{Z}$ um eine Art von Struktur, in der diese zwei Konzepte zusammenfallen. Wie in fast allen technischen Bereichen sollte man auf solche »Zufälligkeiten« achten: Irgendwann befindet man sich in einer Situation, wo man feiner unterscheiden muss und es nicht mehr selbstverständlich ist, zwei Konzepte als identisch zu behandeln. ◊

SKA 5·10

Siehe [Sin20, Satz 3.5.1]. Hier eine Alternative:
Für $r = 0$ setze man $q_r := 1$ und $p_r := 0$. Und für alle anderen rationalen Zahlen, $r \in \mathbb{Q} \setminus \{0\}$, wähle

$$\begin{aligned} q_r &:= \min \overbrace{\{n \in \mathbb{N} \mid q_r \cdot r \in \mathbb{Z}\}}^{D(r)} \in \mathbb{N} \\ p_r &:= q_r \cdot r \in \mathbb{Z}. \end{aligned}$$

Da r rational ist, ist $D(r)$ per Definition nicht leer. Darum ist die Wahl von q_r und p_r wohldefiniert und per Konstruktion gilt $p_r/q_r = r$. (Für $r = 0$ gilt ebenfalls offensichtlich $p_r/q_r = r$.) Damit haben wir die Existenz einer kanonischen Darstellung begründet.

Stimmt dies mit der Konstruktion im [Sin20, Satz 3.5.1] überein?

Für $r = 0$ gilt offensichtlich $\mathsf{ggT}(p_r, q_r) = 1$. Für $r \in \mathbb{Q} \setminus \{0\}$ gilt $d := \mathsf{ggT}(p_r, q_r) = 1$, denn sonst wäre $\frac{q_r}{d}$ eine positive natürliche Zahl in $D(r)$, da $\frac{q_r}{d} \cdot r = \frac{q_r \cdot r}{d} = \frac{p_r}{d} \in \mathbb{Z}$, während $\frac{q_r}{d} < q_r$ (strikt), was ein Widerspruch zur Minimalität ist. Darum entspricht unserer Darstellung der im [Sin20, Satz 3.5.1].

SKA 5·12

Behauptung (vgl. [Sin20, Satz 3.5.3]). *Sei $p \in \mathbb{P}$ eine Primzahl. Dann $\nexists x \in \mathbb{Q} : x^2 = p$.* ◊

Beweis. Angenommen, dies sei nicht der Fall. Dann existieren $a \in \mathbb{Z}$ und $b \in \mathbb{N}$ mit $(\frac{a}{b})^2 = p$. Wir konstruieren nun per Rekursion eine Folge $((a_n, b_n))_{n\in\mathbb{N}} \subseteq \mathbb{Z} \times \mathbb{N}$ mit der Eigenschaft, dass $(\frac{a_n}{b_n})^2 = p$ und $(b_n)_{n\in\mathbb{N}}$ strikt monoton absteigend ist:

- Setze $a_0 := a$ und $b_0 = b$. Offensichtlich gilt per Wahl $(\frac{a_n}{b_n})^2 = p$.
- Sei $n > 0$. Angenommen, wir haben bereits $((a_k, b_k))_{k=0}^{n-1}$ konstruiert. Aus $(\frac{a_n}{b_n})^2 = p$ folgt nun $a_n^2 = pb_n^2$. Daraus folgt $p \mid a_n \cdot a_n$ und damit gilt (vgl. [Sin20, Satz 3.4.14]) $p \mid a_n$, weil p prim ist. Da $b_n^2 = p \cdot (\frac{a_n}{p})^2$ und da $\frac{a_n}{p} \in \mathbb{Z}$, erhalten wir ebenfalls $p \mid b_n \cdot b_n$ und wiederum $p \mid b_n$.

  Setze also $a_{n+1} := \frac{a_n}{p}$ und $b_{n+1} := \frac{b_n}{p}$. Dann wie oben gezeigt wurde, gilt $a_{n+1} \in \mathbb{Z}$ und $b_{n+1} \in \mathbb{N}$. Offensichtlich gilt $(\frac{a_{n+1}}{b_{n+1}})^2 = (\frac{a_n}{b_n})^2 = p$. Und, da $p > 1$, gilt $b_{n+1} < b_n$.

Darum funktioniert die rekursive Konstruktion. Da nun $(b_n)_{n\in\mathbb{N}} \subseteq \mathbb{N}$ eine strikt monoton absteigende Folge ist, haben wir einen Widerspruch erreicht, weil $(\mathbb{N}, \leqslant)$ eine Wohlordnungsrelation ist. ■

SKA 5·13

Behauptung (vgl. [Sin20, Satz 3.5.5]). *Seien $a, b, c \in \mathbb{R}$ mit $a \neq 0$. Dann existiert eine Nullstelle von $ax^2 + bx + c$ gdw. $\Delta \geqslant 0$, wobei $\Delta := b^2 - 4ac$.* ◊

Beweis. Zunächst berechnen wir eine Umformung: Sei $x \in \mathbb{R}$. Dann

$$\begin{aligned} ax^2 + bx + c = 0 &\iff 4a(ax^2 + bx + c) = 0 \quad \text{da } a \neq 0 \\ &\iff (2ax)^2 + 2b(2ax) + b^2 = b^2 - 4ac \\ &\iff (2ax + b)^2 = \Delta. \end{aligned} \tag{5·2}$$

Falls $\Delta \geqslant 0$, so existiert ein $\sqrt{\Delta} \geqslant 0$ mit $\sqrt{\Delta}^2 = \Delta$. Darum gilt

$$ax^2 + bx + c = 0 \overset{(5·2)}{\iff} (2ax + b)^2 = \Delta \iff 2ax + b = \pm\sqrt{\Delta} \iff x = \tfrac{-b+\sqrt{\Delta}}{2a}$$

für alle $x \in \mathbb{R}$. Das heißt, falls $\Delta \geqslant 0$, hat das Polynom reellwertige Nullstellen, und zwar sind die Nullstellen durch $\{\frac{-b+\sqrt{\Delta}}{2a}\}$ gegeben.

Falls $\Delta < 0$, so existieren keine Nullstellen. Angenommen, dies sei nicht der Fall. Fixiere eine Lösung $x \in \mathbb{R}$ und setze $\alpha := 2ax + b \in \mathbb{R}$. Aus (5·2) folgt nun $\Delta = \alpha^2$. Aber $\alpha^2 \geqslant 0$ für alle $\alpha \in \mathbb{R}$. Dies ist ein Widerspruch. ■

SKA 5·14

Die Gruppe von Bijektionen von $\{1, 2\}$ auf $\{1, 2\}$ entspricht der Permutationsgruppe S_2. Dies hat $2! = 2$ Elemente, die standardgemäß mit folgenden Labels bezeichnet werden:

Label	Beschreibung des Elements
e	Funktion, die alles fixiert
$(1\ 2)$	Funktion, die 1 und 2 tauscht

Die Gruppentafel sieht folgendermaßen aus:

		h	
	gh	e	$(1\ 2)$
g	e	e	$(1\ 2)$
	$(1\ 2)$	$(1\ 2)$	e

Die Gruppe von Bijektionen von $\{1, 2, 3\}$ auf $\{1, 2, 3\}$ entspricht der Permutationsgruppe S_3. Dies hat $3! = 6$ Elemente, die standardgemäß mit folgenden Labels bezeichnet werden:

Label	Beschreibung des Elements
e	Funktion, die alles fixiert
$(2\ 3)$	Funktion, die 2 und 3 tauscht
$(1\ 2)$	Funktion, die 1 und 2 tauscht
$(1\ 2\ 3)$	Funktion, die $1 \mapsto 2 \mapsto 3 \mapsto 1$ abbildet
$(1\ 3\ 2)$	Funktion, die $1 \mapsto 3 \mapsto 2 \mapsto 1$ abbildet
$(1\ 3)$	Funktion, die 1 und 3 tauscht

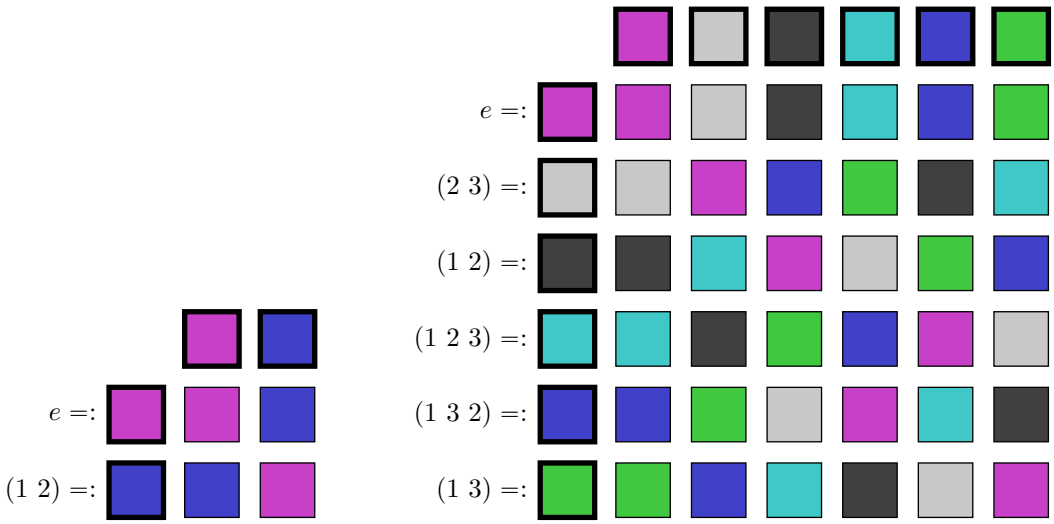
Die Gruppentafel sieht folgendermaßen aus:

		h					
	gh	e	$(2\ 3)$	$(1\ 2)$	$(1\ 2\ 3)$	$(1\ 3\ 2)$	$(1\ 3)$
g	e	e	$(2\ 3)$	$(1\ 2)$	$(1\ 2\ 3)$	$(1\ 3\ 2)$	$(1\ 3)$
	$(2\ 3)$	$(2\ 3)$	e	$(1\ 3\ 2)$	$(1\ 3)$	$(1\ 2)$	$(1\ 2\ 3)$
	$(1\ 2)$	$(1\ 2)$	$(1\ 2\ 3)$	e	$(2\ 3)$	$(1\ 3)$	$(1\ 3\ 2)$
	$(1\ 2\ 3)$	$(1\ 2\ 3)$	$(1\ 2)$	$(1\ 3)$	$(1\ 3\ 2)$	e	$(2\ 3)$
	$(1\ 3\ 2)$	$(1\ 3\ 2)$	$(1\ 3)$	$(2\ 3)$	e	$(1\ 2\ 3)$	$(1\ 2)$
	$(1\ 3)$	$(1\ 3)$	$(1\ 3\ 2)$	$(1\ 2\ 3)$	$(1\ 2)$	$(2\ 3)$	e

(*Achtung: Tafel wurde per Code generiert, also ist die Reihenfolge möglicherweise nicht »ästhetisch«.*)

SKA 5·15

An der Tafel lässt sich leicht erkennen, ob eine Gruppe kommutativ ist: eine Gruppe, G, ist genau dann kommutativ, wenn die Gruppentafel symmetrisch ist. Hierbei sollte man darauf achten, dass die *Labels* der Elemente gar keine Rolle spielen. Um diese Urteil also leichter treffen zu können ersetzen wir die Elemente durch verschieden gefärbte Quadrate:



(a) S_2 (b) S_3

Abbildung 5.1: Gruppentafel mit Elementen durch Farben ersetzt

Nach den o. s. Tafeln ist die erste Gruppe, S_2, kommutativ und die zweite, S_3, nicht.

SKA Blatt 6

Woche 6

SKA 6·1

Betrachte die Verknüpfung $(\mathbb{N}, *)$, die vermöge $a * b := a^b$ definiert wird. Wir prüfen das *Assoziativitätsgesetz*. Seien zu diesem Zwecke erstmals $a, b, c \in \mathbb{N}$. Dann

$$\begin{array}{rclcrcl} a * (b * c) & = & a * b^c & = & a^{b^c}, & & \\ (a * b) * c & = & a^b * c & = & (a^b)^c & = & a^{bc}. \end{array} \tag{6·1}$$

Darum

$$\begin{array}{rcl} a * (b * c) = (a * b) * c & \overset{(6·1)}{\iff} & a^{b^c} = a^{bc} \\ & \iff & a = 1 \text{ oder } b^c = bc \\ & \iff & a = 1 \text{ oder } b^{c-1} = c. \end{array} \tag{6·2}$$

Diese analytische Untersuchung hilft uns, ein **Gegenbeispiel** zu finden: Seien $a := 2$, $b := 3$, $c := 2$. Dann $a \neq 1$ und $b^{c-1} = 3^1 \neq c$. Darum laut (6·2) gilt $a * (b * c) \neq (a * b) * c$.

Also erfüllt $(\mathbb{N}, *)$ das Assoziativitätsaxiom nicht.

SKA 6·2

Die Multiplikationstabelle für $(R, +, \cdot)$ mit $R = \{0, 1\}$ ist wie folgt

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

SKA 6·3

Betrachte $\{0, 1, a\}$ mit folgenden Operationen $+$, $\cdot$:

$+$	0	1	a
0	0	1	a
1	1	a	0
a	a	0	1

$\cdot$	0	1	a
0	0	0	0
1	0	1	a
a	0	a	1

Diese Struktur ist offensichtlich isomorph zu $(\mathbb{Z}/3\mathbb{Z}, +, \cdot)$ mittels $0 \mapsto 0$, $1 \mapsto 1$, $a \mapsto 2$. Da $(\mathbb{Z}/3\mathbb{Z}, +, \cdot)$ ein Körper ist, ist $(\{0, 1, a\}, +, \cdot)$ ebenfalls wegen des Isomorphismus ein Körper. Insbesondere sind die o. s. definierten Operationen assoziativ.

SKA 6·4

Behauptung. *Sei K ein Körper und seien $x, y \in K$ mit $xy = 0$. Dann gilt $x = 0$ oder $y = 0$.* $\Diamond$

Beweis. Angenommen, dies sei nicht der Fall. Dann $x \neq 0$ und $y \neq 0$. Darum existieren multiplikative Inverse, $x^{-1}, y^{-1} \in K$. Aus $xy = 0$ folgt dann

$$1 \;=\; y^{-1}y \;=\; y^{-1}1y \;=\; y^{-1}(x^{-1}x)y \;=\; (y^{-1}x^{-1})(xy) \;=\; (y^{-1}x^{-1})0 \;=\; 0.$$

Das ist ein Widerspruch! ■

Bemerkung. Wir haben hier den Satz $\forall a \in K : a \cdot 0 = 0$ (siehe [Sin20, Satz 4.2.2]) in Anspruch genommen.

SKA 6·5

Sei $R = \mathbb{Z}/6\mathbb{Z}$ versehen mit Addition und Multiplikation modulo 6.
Beachte: das additive Neutralelement ist die Äquivalenzklasse $[0]$.
Für $x = [2]$ und $y = [3]$ gilt $x, y \neq [0]$ und aber $xy = [2 \cdot 3] = [6] = [0]$.

Bemerkung. Wir nennen solche Elemente *Nullteiler*.

SKA 6·6

(a)

$$z_1 := \frac{2\imath}{5-3\imath} = \frac{2\imath\cdot(5+3\imath)}{5^2+3^2} = \frac{-6+10\imath}{34} = -\tfrac{3}{17} + \imath\tfrac{5}{17}$$
$$\implies \mathfrak{Re}(z_1) = -\tfrac{3}{17}, \quad \mathfrak{Im}(z_1) = \tfrac{5}{17}.$$

$$z_2 := \frac{3-2\imath}{1+2\imath} = \frac{(3-2\imath)\cdot(1-2\imath)}{1^2+2^2} = \frac{(3+(-2)(-2)\imath^2)) + (-6+-2)\imath}{5} = \frac{(3-4)+-8\imath}{5} = -\tfrac{1}{5} + \imath\tfrac{8}{5}$$
$$\implies \mathfrak{Re}(z_2) = -\tfrac{1}{5}, \quad \mathfrak{Im}(z_2) = \tfrac{8}{5}.$$

(b)

Gaußverfahren angewandt auf $(A|\mathbf{b})$:

$$\left(\begin{array}{cc|c} 1+\imath & 1 & 0 \\ -2 & 2-\imath & 1 \end{array}\right)$$

Wende die Zeilentransformation $Z_1 \rightsquigarrow (1-\imath)\cdot Z_1$ an:

$$\left(\begin{array}{cc|c} 2 & 1-\imath & 0 \\ -2 & 2-\imath & 1 \end{array}\right)$$

Wende die Zeilentransformation $Z_2 \rightsquigarrow Z_2 + Z_1$ an:

$$\left(\begin{array}{cc|c} 2 & 1-\imath & 0 \\ 0 & 3-2\imath & 1 \end{array}\right)$$

Aus der Stufenform erschließt sich

$$\begin{array}{rclcl} y &=& \frac{1}{3-2\imath} &=& \frac{3+2\imath}{3^2+2^2} \;=\; \frac{3+2\imath}{13} \\ x &=& \frac{1}{2}(-(1-\imath)y) &=& -\frac{1}{2}\frac{3-\imath}{13} \;=\; \frac{-3+\imath}{26}. \end{array}$$

SKA 6·7

(a) Es gilt $4 \cdot 7 \equiv -1 \cdot 2 \equiv -2 \equiv 3$ modulo 5.

(b) Es gilt $2^{100031} \equiv (-1)^{\text{ungerade Zahl}} \equiv -1 \equiv 2$ modulo 3.
Es gilt $2^{100302} \equiv (-1)^{\text{gerade Zahl}} \equiv 1$ modulo 3.

(c) Für $\mathbb{Z}/5\mathbb{Z}$ ist die Menge an Möglichkeiten klein, sodass wir per *brute force* das Inverse von 3 bestimmen können:

n	0	1	2	3	4
$3 \cdot n$	0	3	$\boxed{1}$	4	2

Darum gilt $3 \cdot 2 \equiv 1$ modulo 5, sodass $\boxed{3^{-1} = 2}$ in $\mathbb{Z}/5\mathbb{Z}$.

Für den Fall $\mathbb{Z}/103\mathbb{Z}$ gibt es deutlich mehr Möglichkeiten, sodass es ein Versuch durch rohe Gewalt nicht mehr sinnvoll ist. Darum wenden wir das Lemma von Bézout an und lesen das Resultat daraus.

Zur Erinnerung: Durch den Euklidischen Algorithmus auf $(a := 103,\, b := 21)$ angewandt erhalten wir ganze Zahlen, $u, v \in \mathbb{Z}$, so dass $u \cdot 103 + v \cdot 21 = \text{ggT}(103, 21)$ gilt. Da aber $103 \in \mathbb{P}$ und $1 < 21 < 103$, gilt $\text{ggT}(103, 21) = 1$, sodass die o. s. Identität $1 \equiv u \cdot 103 + v \cdot 21 \equiv 0 + v \cdot 21$ modulo 103 liefert, was wiederum bedeutet, dass $21^{-1} = v$ in $\mathbb{Z}/103\mathbb{Z}$.

Zunächst führen wird also den Euklidischen Algorithmus auf $a = 103$ und $b = 21$ aus:

Restberechnung (symbolisch)	Restberechnung (Werte)
$a = b \cdot q_1 + r_1$	$103 = 21 \cdot 4 + 19$
$b = r_1 \cdot q_2 + r_2$	$21 = 19 \cdot 1 + 2$
$r_1 = r_2 \cdot q_3 + r_3$	$19 = 2 \cdot 9 + \boxed{\mathbf{1}}$
$r_2 = r_3 \cdot q_4 + r_4$	$2 = 1 \cdot 2 + 0$

Also gilt $\text{ggT}(103, 21) = 1$ wie erwartet. Und jetzt kehren wir die Ausdrücke um, um die Koeffizienten u, v zu bestimmen:

Rest (symbolisch)	Rest (Werte)
$r_1 = a - 4 \cdot b$	$19 = 1 \cdot a + -4 \cdot b$
$r_2 = b - 1 \cdot r_1$	$2 = -1 \cdot a + 5 \cdot b$
$r_3 = r_1 - 9 \cdot r_2$	$\boxed{1 = \mathbf{10} \cdot a + \mathbf{-49} \cdot b}$

Darum liefert uns das Bézout Lemma $1 = 10 \cdot a - 49 \cdot b = 10 \cdot 103 - \boxed{49} \cdot 21$. Also gilt wie oben $\boxed{21^{-1} = -49 = 54}$ in $\mathbb{Z}/103\mathbb{Z}$.
(Man prüft dies: $21 \cdot 54 = 1134 = 103 \cdot 11 + 1 \equiv 1$ modulo 103. Also ist das Ergebnis richtig!)

(d) Wir führen das Gaußverfahren zuerst in $\mathbb{Z}$ durch, nur achten wir darauf, niemals mit Vielfachen von 11 oder 13 zu multiplizieren:

Gaußverfahren angewandt auf $(A|\mathbf{b})$:

$$\left(\begin{array}{cc|c} 2 & -3 & 0 \\ 10 & 7 & -5 \end{array}\right)$$

Wende die Zeilentransformation $Z_2 \rightsquigarrow Z_2 - 5 \cdot Z_1$ an:

$$\left(\begin{array}{cc|c} 2 & -3 & 0 \\ 0 & 22 & -5 \end{array}\right)$$

Wir wenden die Zeilentransformation $Z_1 \rightsquigarrow 7 \cdot Z_1 + Z_2$ an und erhalten das äquivalente System (†):

$$\left(\begin{array}{cc|c} 14 & 1 & -5 \\ 0 & 22 & -5 \end{array}\right)$$

In $\mathbb{Z}/11\mathbb{Z}$ ist das System ab (†)

LGS modulo 11:

$$\left(\begin{array}{cc|c} \mathbf{3} & 1 & 6 \\ 0 & 0 & \mathbf{6} \end{array}\right)$$

$\Longrightarrow$ $\boxed{\text{System unlösbar}}$, da $6 \neq 0$ in $\mathbb{Z}/11\mathbb{Z}$.

In $\mathbb{Z}/13\mathbb{Z}$ ist das System ab (†)

LGS modulo 13:

$$\left(\begin{array}{cc|c} 1 & 1 & 8 \\ 0 & 9 & 8 \end{array}\right)$$

Wende die Zeilentransformationen $Z_1 \rightsquigarrow 9 \cdot Z_1 - \cdot Z_2$ an:

$$\left(\begin{array}{cc|c} \mathbf{9} & 0 & -1 \\ 0 & \mathbf{9} & 8 \end{array}\right)$$

Daraus ergibt sich die Lösung in $\mathbb{Z}/13\mathbb{Z}$:

$$\begin{array}{rclcll} x_1 & = & 9^{-1} \cdot -1 & = & 3 \cdot -1 & = & \boxed{10} \\ x_2 & = & 9^{-1} \cdot 8 & = & 3 \cdot 8 & = & \boxed{11}. \end{array}$$

Also ist $\boxed{\mathbf{x} = \left(\begin{smallmatrix} 10 \\ 11 \end{smallmatrix}\right)}$ die Lösung des LGS in $\mathbb{Z}/13\mathbb{Z}$.

ALso ist das LGS innerhalb $\mathbb{Z}/13\mathbb{Z}$ lösbar, aber nicht innerhalb $\mathbb{Z}/11\mathbb{Z}$.

SKA 6·8

Satz. *Sei $p \in \mathbb{P}$ eine Primzahl. Für jedes $m \in \mathbb{Z}$ mit $p \nmid m$ ist die Abbildung $M_m : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$, die vermöge $M_m([x]) = [m] \cdot [x] (= [mx])$ definiert wird, wohldefiniert und injektiv. Insbesondere existert ein $[x] \in \mathbb{Z}/p\mathbb{Z}$, so dass $[m] \cdot [x] = [1]$.* ◊

Beweis. Dass diese Abbildung wohldefiniert ist, folgt aus der Wohldefiniertheit von Modularmultiplikation.

Injektivität:
Seien $[x], [x'] \in \mathbb{Z}/p\mathbb{Z}$. Angenommen $M_m([x]) = M_m([x'])$. **Zu zeigen:** $[x] = [x']$.
Aus $M_m([x]) = M_m([x'])$ folgt $[mx] = [mx']$ per Konstruktion der Abbildung M_m.
Per Definition der Äquivalenzklassen gilt somit $mx \equiv mx'$ modulo p.
Daraus folgt $p \mid (mx - mx')$, also $p \mid m \cdot (x - x')$.
Da p prim ist, gilt $p \mid m$ oder $p \mid (x - x')$ (siehe [Sin20, Satz 3.4.14]).
Per Voraussetzung auf m folgt daraus, dass $p \mid (x - x')$.
Daraus folgt $x \equiv x'$ modulo p, und somit $[x] = [x']$ per Definition der Äquivalenzklassen.
Darum ist M_m injektiv.

Da nun $\mathbb{Z}/p\mathbb{Z}$ endlich ist, sind injektive Abbildungen zwischen $\mathbb{Z}/p\mathbb{Z}$ und sich selbst automatisch surjektiv.
Per Surjektivität existiert ein Element $[x] \in \mathbb{Z}/p\mathbb{Z}$, so dass $[1] = M_m([x]) = [m] \cdot [x]$.
Das heißt, $[m]$ ist invertierbar innerhalb $\mathbb{Z}/p\mathbb{Z}$. ■

Bemerkung. Die letzte Aussage in diesem Satz gilt auch allgemeiner: Sind $n, m \in \mathbb{Z}$ teilerfremd, dann ist $[m]$ innerhalb $\mathbb{Z}/n\mathbb{Z}$ invertierbar. Falls n nicht prim ist, muss man sich allerdings bei der Injektivitätsargumentation mehr bemühen. Einfacher ist also natürlich die Anwendung von dem Lemma von Bézout.

TEIL III
Quizzes

Quiz 1

Woche 1

Behauptung. *Das LGS*

$$\begin{array}{rcrcl} -x & + & a \cdot y & = & 3 \\ a \cdot x & - & 4y & = & 0 \end{array}$$

ist genau dann lösbar, wenn $a \in \mathbb{R} \setminus \{\pm 2\}$. ◊

Beweis. Sei $a \in \mathbb{R}$ beliebig. Wir führen das Gaußverfahren aus:

Ursprüngliches LGS $(A_\alpha | b_\beta)$:

$$\left(\begin{array}{cc|c} -1 & a & 3 \\ a & -4 & 0 \end{array}\right)$$

Wende die Zeilentransformationen $Z_2 \rightsquigarrow a \cdot Z_1 + Z_2$ an:

$$\left(\begin{array}{cc|c} 1 & a & 3 \\ 0 & a^2 - 4 & 3a \end{array}\right)$$

Wenn $a \in \{\pm 2\}$, ist das LGS unlösbar, da in der 2. Zeile links nur 0 Einträge stehen und rechts ± 6.
Wenn $a \notin \{\pm 2\}$, gibt es zwei Stufen und damit ist das LGS lösbar.
Also gilt die Behauptung. ■

Quiz 2

Woche 2

Sei L die Gerade $\{\mathbf{v} + t\mathbf{w} \mid t \in \mathbb{R}\} \subseteq \mathbb{R}^3$, wobei

$$\mathbf{v} \quad = \quad \begin{pmatrix} -4 \\ 2 \\ 5 \end{pmatrix}, \quad \mathbf{w} \quad = \quad \begin{pmatrix} 2 \\ -6 \\ 12 \end{pmatrix}.$$

(1) Behauptung. *Der Punkt,* $\mathbf{x} = \begin{pmatrix} -3 \\ -1 \\ 11 \end{pmatrix}$*, liegt in der Geraden,* L*.* ◊

Beweis. Es gilt

$$\begin{aligned} \mathbf{x} \in L \quad &\iff \quad \exists t \in \mathbb{R} : \mathbf{x} = \mathbf{v} + t\mathbf{w} \\ &\iff \quad \exists t \in \mathbb{R} : \mathbf{x} - \mathbf{v} = t\mathbf{w} \\ &\iff \quad \exists t \in \mathbb{R} : \begin{pmatrix} 1 \\ -3 \\ 6 \end{pmatrix} = t \begin{pmatrix} 2 \\ -6 \\ 12 \end{pmatrix} \end{aligned}$$

Nun ist die letzte Aussage wahr, da der Ausdruck innerhalb des Existenzquantors offensichtlich unter $t = \frac{1}{2}$ wahr ist. Darum gilt $\mathbf{x} \in L$. ■

(2) Fixiere einen Vektor, $\mathbf{w}_\perp \in \mathbb{R}^3$, der zu $\mathbf{w}$ normal ist. Z. B. können wir

$$\mathbf{w}_\perp \quad = \quad \begin{pmatrix} 3 \\ -1 \\ 0 \end{pmatrix}$$

wählen. Dann gilt $\langle \mathbf{w}, \mathbf{w}_\perp \rangle = 0$, sodass die Vektoren normal zueinander stehen.

Nun, für $\mathbf{x} \in L$ setze

$$L_{\mathbf{x}} \quad := \quad \{\mathbf{x} + s \cdot \mathbf{w}_\perp \mid s \in \mathbb{R}\}.$$

Dann gilt offensichtlich $\mathbf{x} \in L \cap L_{\mathbf{x}}$.
Andererseits, da die Richtungsvektoren in den Geraden nicht linear abhängig sind, (da sie normal zueinander stehen), gilt $|L \cap L_{\mathbf{x}}| \leqslant 1$.
Darum gilt $L \cap L_{\mathbf{x}} = \{\mathbf{x}\}$.

Quiz 3

Woche 3

(a) **Behauptung.** *Seien X, Y beliebige Mengen und $f : X \to Y$ eine Funktion. Sei $B \subseteq Y$ beliebig. Dann gilt $f(f^{-1}(B)) = f(X) \cap B$. Insbesondere gilt $f(f^{-1}(B)) \subseteq B$* $\Diamond$

Beweis. Für $y \in Y$ gilt

$$\begin{aligned}
y \in f(f^{-1}(B)) &\iff \exists x \in f^{-1}(B) : f(x) = y \\
&\iff \exists x : (x \in f^{-1}(B) \text{ und } f(x) = y) \\
&\iff \exists x : (x \in X \text{ und } f(x) \in B \text{ und } f(x) = y) \\
&\iff \exists x \in X : (f(x) \in B \text{ und } f(x) = y) \\
&\iff \exists x \in X : (y = f(x) \text{ und } y \in B) \\
&\iff (\exists x \in X : y = f(x)) \text{ und } y \in B \\
&\iff y \in f(X) \text{ und } y \in B \\
&\iff y \in f(X) \cap B.
\end{aligned}$$

Darum gilt $f(f^{-1}(B)) = f(X) \cap B \subseteq B$. ■

(b) Aus (a) folgt:

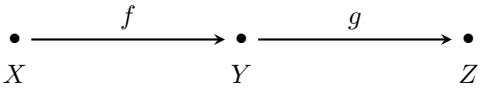
- f surjektiv $\implies f(f^{-1}(B)) = f(X) \cap B = Y \cap B = B$ für alle $B \subseteq Y$;
- f nicht surjektiv $\implies f(f^{-1}(Y)) = f(X) \cap Y = f(X) \subset Y$ (strikt).

Darum ist es notwendig und hinreichend, eine nicht-surjektive Funktion als Beispiel zu nehmen. Hier ein minimales Beispiel $X = \{0\}$ und $Y = \{1, 2\}$ und $B = Y$ und $f : X \to Y$ definiert durch $f(0) = 1$. Dann $f(f^{-1}(B)) = f(f^{-1}(Y)) = f(X) = \{1\} \subset Y$ (strikt).

Quiz 4

Woche 4

Gegeben seien Mengen X, Y, Z, und Funktionen $f : X \to Y$ und $g : Y \to Z$. Wir betrachten die Komposition $g \circ f : X \to Z$



(a) Behauptung. *$g \circ f$ injektiv $\Rightarrow$ f injektiv.* ◊

Beweis. Angenommen, $g \circ f$ sei injektiv. **Zu zeigen:** f ist injektiv
Zu zeigen: Für alle $x_1, x_2 \in X$ gilt $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.
Seien also $x_1, x_2 \in X$ beliebig. Es gilt:

$$\begin{aligned} f(x_1) = f(x_2) &\implies g(f(x_1)) = g(f(x_2)) \\ &\implies (g \circ f)(x_1) = (g \circ f)(x_2) \\ &\implies x_1 = x_2, \text{ da } g \circ f \text{ injektiv.} \end{aligned}$$

Also ist f injektiv. ■

(b) Behauptung. *f, g injektiv $\Rightarrow$ $g \circ f$ injektiv.* ◊

Beweis. Angenommen, f, g seien injektiv. **Zu zeigen:** $g \circ f$ ist injektiv
Zu zeigen: Für alle $x_1, x_2 \in X$ gilt $(g \circ f)(x_1) = (g \circ f)(x_2) \Rightarrow x_1 = x_2$.
Seien also $x_1, x_2 \in X$ beliebig. Es gilt:

$$\begin{aligned} (g \circ f)(x_1) = (g \circ f)(x_2) &\implies g(f(x_1)) = g(f(x_2)) \\ &\implies f(x_1) = f(x_2), \text{ da } g \text{ injektiv} \\ &\implies x_1 = x_2, \text{ da } f \text{ injektiv.} \end{aligned}$$

Also ist $g \circ f$ injektiv. ■

Quiz 5

Woche 5

Behauptung. *Seien $n \in \mathbb{N}$ und $p \in \mathbb{P}$ mit $n < p \leqslant 2n$. Dann gilt $p \mid \binom{2n}{n}$.* ◊

Beweis. Aus $n < p \leqslant 2n$, d. h. $p \in \{n+1, n+2, \ldots, 2n\}$, folgt (i) $p \mid \prod_{i=n+1}^{2n} i$.
Es gilt nun

$$\prod_{i=n+1}^{2n} i \quad = \quad \frac{\prod_{i=1}^{2n} i}{n!} \quad = \quad n! \frac{(2n)!}{n!(2n-n)!} \quad = \quad n! \binom{2n}{n}. \tag{5·1}$$

Aus (i) und (5·1) folgt also (ii) $p \mid \binom{2n}{n} \cdot n!$.
Beachte, dass p eine Primzahl ist und $n!, \binom{2n}{n} \in \mathbb{Z}$.
Aus (ii) und [Sin20, Satz 3.4.14] folgt also $p \mid \binom{2n}{n}$ oder $p \mid n!$.

Angenommen, $p \nmid \binom{2n}{n}$.
Dann muss laut des o. s. Arguments $p \mid n! (= \prod_{i=1}^{n} i)$ gelten.
Eine weitere Anwendung von [Sin20, Satz 3.4.14] liefert, dass $p \mid i_0$ für ein $i_0 \in \{1, 2, \ldots, n\}$.
Aber dann gilt $1 \leqslant p \leqslant i_0 \leqslant n$. Das widerspricht der Voraussetzung, dass $n < p$.
Darum stimmt die Annahme nicht. Das heißt, $p \mid \binom{2n}{n}$. ■

Literaturverzeichnis

[EFT18] Heinz-Dieter Ebbinghaus, Jörg Flum, and Wolfgang Thomas. *Einführung in die mathematische Logik*. 2018.

[Jec97] Thomas Jech. *Set Theory*. Springer-Verlag, 1997.

[Sin20] Rainer Sinn. Lineare Algebra I: Skript zur Veranstaltung Universität Leipzig. Vorlesungsskript, 2020.

[Wal16] Stefan Waldmann. *Lineare Algebra 1: Die Grundlagen für Studierende der Mathematik und Physik*. Springer Berlin Heidelberg, 2016.