Universität Paderborn
INSTITUT FÜR MATHEMATIK
Dr. Job Kuit

Sommersemester 2024

Lineare Algebra für Informatiker

1. Übungsblatt - Lösungen

Präsenzaufgabe 1.1 Sei $\mathbb{Q}(\sqrt{2}) := \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.

(a) Zeigen Sie, dass die übliche Multiplikation von reellen Zahlen $\mathbb{Q}(\sqrt{2}) \setminus \{0\}$ zu einer Gruppe macht.
Lösung: Für alle $a_1, a_2, b_1, b_2 \in \mathbb{Q}$ gilt

$$(a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) = (a_1a_2 + 2b_1b_2 + (a_1b_2) + a_2b_1)\sqrt{2} \in \mathbb{Q}(\sqrt{2}).$$

Die Multiplikation von reelle Zahlen ist assoziativ. Das Element $1 = 1 + 0\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ ist das neutrale Element für Multiplikation. Zum Schluss, wenn $a, b \in \mathbb{Q}$, dann ist

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2} \in \mathbb{Q}(\sqrt{2})$$

die Multiplikative inverse von $a + b\sqrt{2}$.

(b) Zeigen Sie, dass $\mathbb{Q}(\sqrt{2})$ mit der üblichen Addition und Multiplikation von reellen Zahlen ein Ring ist.
Lösung: Für alle $a_1, a_2, b_1, b_2 \in \mathbb{Q}$ gilt

$$(a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{2} \in \mathbb{Q}(\sqrt{2}).$$

Die Addition von reelle Zahlen ist assoziativ. Das Element $0 = 0+0\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ ist das neutrale Element für Addition. Wenn $a, b \in \mathbb{Q}$, dann ist $-a - b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ die Additive Inverse von $a + b\sqrt{2}$. Addition und Multiplikation reeller Zahlen erfüllen das Distributivgesetz.

Präsenzaufgabe 1.2 Sei p eine Primzahl. Sei R die Teilmenge aller rationalen Zahlen $\frac{m}{n}$, so dass $n \neq 0$ und n nicht durch p teilbar ist. Zeigen Sie, dass R ein Ring ist.
Lösung: Seien $m, m', n, n' \in \mathbb{Z}$, sodass n und n' ungleich 0 und nicht teilbar duch p sind. Dann ist nn' ungleich 0 und nicht teilbar durch p. Darum gilt

$$\frac{m}{n} + \frac{m'}{n'} = \frac{mn' + m'n}{nn'} \in R, \quad \frac{m}{n}\frac{m'}{n'} = \frac{mm'}{nn'} \in R \quad \text{und} \quad \frac{-m}{n} \in R.$$

Weiter sind die neutrale Elementen 0 und 1 für Addition bzw. Multiplikation in R enthalten, denn $0 = \frac{0}{1} \in R$ und $1 = \frac{1}{1} \in R$. Addition und Multiplikation von rationale Zahlen sind assoziativ und kommutativ und das Distributivgesetz gilt.

Präsenzaufgabe 1.3 Sie $(G, \star)$ eine Gruppe. Beweisen Sie die folgenden Aussagen.

(a) Wenn $x, y, z \in G$ und $x \star y = x \star z$, dann gilt $y = z$.
Lösung: Wenn $x \star y = x \star z$, dann

$$y = e \star y = (x^{-1} \star x) \star y = x^{-1} \star (x \star y) = x^{-1} \star (x \star z) = (x^{-1} \star x) \star z = e \star z = z.$$

(b) Wenn $x, y \in G$, dann $(x \star y)^{-1} = y^{-1} \star x^{-1}$.
Lösung: Es gilt

$$(x \star y) \star (y^{-1} \star x^{-1}) = x \star \big((y \star y^{-1}) \star x^{-1}\big) = x \star (e \star x^{-1}) = x \star x^{-1} = e.$$

Die Eindeutigkeit von Inversen impliziert, dass $(x \star y)^{-1} = y^{-1} \star x^{-1}$.

(c) Wenn $x, y \in G$, dann gibt es eindeutige Elemente $w, z \in G$, sodass $w \star x = y$ und $x \star z = y$.
Lösung: Sei $w = y \star x^{-1}$. Dann gilt $w \star x = (y \star x^{-1}) \star x = y \star (x^{-1} \star x) = y \star e = y$. Wenn $w' \in G$ und $w' \star x = y$, dann gilt $w' = w' \star e = w' \star (x \star x^{-1}) = (w' \star x) \star x^{-1} = y \star x^{-1} = w$.
Sei $z = x^{-1} \star y$. Dann gilt $x \star z = x \star (x^{-1} \star y) = (x \star x^{-1}) \star y = e \star y = y$. Wenn $z' \in G$ und $x \star z' = y$, dann gilt $z' = e \star z' = (x^{-1} \star x) \star z' = x^{-1} \star (x \star z') = x^{-1} \star y = z$.

Präsenzaufgabe 1.4

(a) Bestimmen Sie $\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix} \circ \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{bmatrix}$.
Lösung: $\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix} \circ \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{bmatrix}$.

(b) Schreiben Sie $\begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{bmatrix}$ als eine Komposition von Transpositionen.
Lösung: $\begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{bmatrix} \circ \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{bmatrix}$ oder $\begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{bmatrix} =$ $\begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{bmatrix} \circ \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{bmatrix} \circ \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{bmatrix} \circ \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{bmatrix}$.

Präsenzaufgabe 1.5 Wir betrachten $\{\pm 1\}$ zusammen versehen mit der üblichen Multiplikation von Zahlen als eine Gruppe. Sei $n \in \mathbb{N}$. Ziel dieser Aufgabe ist es zu zeigen, dass es einen Gruppenhomomorphismus $\mathrm{sign} : S_n \to \{\pm 1\}$ mit der Eigenschaft gibt, dass $\mathrm{sign}(\sigma) = -1$ für jede Transposition $\sigma \in S_n$.

(a) Sei $f : \mathbb{R}^n \to \mathbb{R}$ eine Funktion. Für $\sigma \in S_n$ sei $\sigma(f) : \mathbb{R}^n \to \mathbb{R}$ die Abbildung gegeben durch

$$\sigma(f)(x_1, x_2, \ldots, x_n) = f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}) \qquad \big((x_1, \ldots, x_n) \in \mathbb{R}^n\big).$$

Zeigen Sie, dass

$$\sigma\big(\tau(f)\big) = (\sigma \circ \tau)(f) \qquad (\sigma, \tau \in S_n).$$

Lösung: Es gilt

$$\begin{aligned} \sigma\big(\tau(f)\big)(x_1, \ldots, x_n) &= \tau(f)(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = f(x_{\sigma(\tau(1))}, \ldots x_{\sigma(\tau(n))}) \\ &= \big((\sigma \circ \tau)(f)\big)(x_1, \ldots, x_n). \end{aligned}$$

(b) Betrachten Sie jetzt die Funktion

$$f : \mathbb{R}^n \to \mathbb{R}, \quad (x_1, \ldots, x_n) \mapsto \prod_{1 \le i < j \le n} (x_i - x_j).$$

Zeigen Sie, dass $\sigma(f) = \pm f$ für jedes $\sigma \in S_n$.
Lösung: Wir definieren die Mengen

$$\begin{aligned} P &= \{(i,j) : i,j \in \{1,\dots,n\} \text{ mit } i \neq j\}, \\ P_+ &= \{(i,j) : i,j \in \{1,\dots,n\} \text{ mit } i < j\} \\ P_- &= \{(i,j) : i,j \in \{1,\dots,n\} \text{ mit } i > j\}. \end{aligned}$$

Es gilt

$$P = P_+ \cup P_- \quad \text{und} \quad P_+ \cap P_- = \emptyset.$$

Sei $\sigma \in S_n$. Weil σ eine Bijektion $\{1,\dots,n\} \to \{1,\dots,n\}$ ist, ist $\sigma(i) \neq \sigma(j)$, wenn $i \neq j$ und ist die Abbildung

$$\Sigma : P \to P; \quad (i,j) \mapsto \big(\sigma(i), \sigma(j)\big)$$

eine Bijektion. Für jedes $(i,j) \in P$ gilt, dass $(i,j) \in \Sigma(P_+)$ genau dann, wenn $(j,i) \notin \Sigma(P_+)$. Darum ist P_+ die disjunkte Vereinigung

$$P_+ = \{(i,j) \in P_+ : (i,j) \in \Sigma(P_+)\} \sqcup \{(i,j) \in P_+ : (j,i) \in \Sigma(P_+)\}. \tag{1}$$

Nach Definition gilt

$$f(x_1,\dots,x_n) = \prod_{(i,j)\in P_+} (x_i - x_j) \qquad \big((x_1,\dots,x_n) \in \mathbb{R}^n\big).$$

Es folgt, dass für alle $(x_1,\dots,x_n) \in \mathbb{R}^n$ gilt

$$\begin{aligned} \sigma(f)(x_1,\dots,x_n) &= \prod_{(i,j)\in P_+} (x_{\sigma(i)} - x_{\sigma(j)}) = \prod_{\left(\sigma^{-1}(k),\sigma^{-1}(l)\right)\in P_+} (x_k - x_l) \\ &= \prod_{(k,l)\in\Sigma(P_+)} (x_k - x_l) = \left(\prod_{\substack{(k,l)\in\Sigma(P_+) \\ (k,l)\in P_+}} (x_k - x_l)\right)\left(\prod_{\substack{(k,l)\in\Sigma(P_+) \\ (l,k)\in P_+}} (x_k - x_l)\right) \\ &= \left(\prod_{\substack{(k,l)\in\Sigma(P_+) \\ (k,l)\in P_+}} (x_k - x_l)\right)\left(\prod_{\substack{(n,m)\in\Sigma(P_+) \\ (m,n)\in P_+}} (-1)(x_m - x_n)\right) \end{aligned}$$

Wenn $N_\sigma = |\{(i,j) \in P_+ : (j,i) \in \Sigma(P_+)\}|$, dann folgt aus (1)

$$\begin{aligned} \sigma(f)(x_1,\dots,x_n) &= (-1)^{N_\sigma}\left(\prod_{\substack{(k,l)\in\Sigma(P_+) \\ (k,l)\in P_+}} (x_k - x_l)\right)\left(\prod_{\substack{(n,m)\in\Sigma(P_+) \\ (m,n)\in P_+}} (x_m - x_n)\right) \\ &= (-1)^{N_\sigma} \prod_{(i,j)\in P_+} (x_i - x_j) = (-1)^{N_\sigma} f(x_1,\dots,x_n) \end{aligned}$$

Weil dies wahr ist für alle $(x_1,\dots,x_n) \in \mathbb{R}^n$, können wir folgern, dass

$$\sigma(f) = (-1)^{N_\sigma} f.$$

(c) Definieren Sie $\operatorname{sign} : S_n \to \{\pm 1\}$ durch

$$\sigma(f) = \operatorname{sign}(\sigma) f \qquad (\sigma \in S_n).$$

Zeigen Sie, dass sign ein Gruppenhomomorphismus ist.
Lösung: Zu zeigen ist, dass $\mathrm{sign}(\sigma \circ \tau) = \mathrm{sign}(\sigma)\mathrm{sign}(\tau)$ für alle $\sigma, \tau \in S_n$. Es gilt

$$(\sigma \circ \tau)(f) = \mathrm{sign}(\sigma \circ \tau) f$$

Andererseits gilt nach (a)

$$(\sigma \circ \tau)(f) = \sigma\big(\tau(f)\big) = \sigma\big(\mathrm{sign}(\tau) f\big) = \mathrm{sign}(\tau)\sigma(f) = \mathrm{sign}(\sigma)\mathrm{sign}(\tau) f.$$

Weil f nicht konstant gleich 0 ist, folgt $\mathrm{sign}(\sigma \circ \tau) = \mathrm{sign}(\sigma)\mathrm{sign}(\tau)$.

(d) Zeigen Sie, dass $\mathrm{sign}(\sigma) = -1$ für jede Transposition $\sigma \in S_n$.
Lösung: Sei σ eine Transposition. Seien $k, l \in \{1, \ldots, n\}$, sodass $k \neq l$, $\sigma(k) = l$, $\sigma(l) = k$ und $\sigma(i) = i$, falls $i \neq k, l$. Sei $\tau \in S_n$ gegeben durch

$$\tau : \begin{cases} 1 & \mapsto k \\ 2 & \mapsto l \\ k & \mapsto 1 \\ l & \mapsto 2 \\ i & \mapsto i \quad (i \neq 1, 2, k, l) \end{cases},$$

falls $k \neq 2$ und

$$\tau : \begin{cases} 1 & \mapsto l \\ l & \mapsto 1 \\ i & \mapsto i \quad (i \neq 1, l) \end{cases},$$

falls $k = 2$.

Dann ist $\sigma_0 := \tau \circ \sigma \circ \tau \in S_n$ die Transposition

$$\sigma_0 : \begin{cases} 1 & \mapsto 2 \\ 2 & \mapsto 1 \\ i & \mapsto i \quad (i \neq 1, 2) \end{cases}$$

Es gilt $\mathrm{sign}(\sigma_0) = \mathrm{sign}(\tau)^2 \mathrm{sign}(\sigma) = \mathrm{sign}(\sigma)$. Es reicht darum zu zeigen, dass $\mathrm{sign}(\sigma_0) = -1$. Wenn $3 \leq i < j \leq n$, dann

$$x_{\sigma_0(1)} - x_{\sigma_0(i)} = x_2 - x_i, \quad x_{\sigma_0(2)} - x_{\sigma_0(i)} = x_1 - x_i, \quad \text{und} \quad x_{\sigma_0(i)} - x_{\sigma_0(j)} = x_i - x_j.$$

Darum gilt

$$\prod_{\substack{1 \leq i < j \leq n \\ (i,j) \neq (1,2)}} (x_{\sigma(i)} - x_{\sigma(j)}) = \prod_{\substack{1 \leq i < j \leq n \\ (i,j) \neq (1,2)}} (x_i - x_j).$$

Weil $x_{\sigma(1)} - x_{\sigma(2)} = -x_1 + x_2$, folgt $\sigma_0(f) = -f$ und damit $\mathrm{sign}(\sigma_0) = -1$.

(e) Sei $n = 4$. Bestimmen Sie $\mathrm{sign}\left(\begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{bmatrix}\right)$.
Lösung: Nach 1.4(b) und (d) gilt

$$\begin{aligned} \mathrm{sign}\left(\begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{bmatrix}\right) &= \mathrm{sign}\left(\begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{bmatrix} \circ \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{bmatrix}\right) \\ &= \mathrm{sign}\left(\begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{bmatrix}\right) \cdot \left(\begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{bmatrix}\right) = (-1)(-1) = 1. \end{aligned}$$

Präsenzaufgabe 1.6 Zeigen Sie, dass $n^3 - 4n$ teilbar ist durch 3 für alle $n \in \mathbb{Z}$.
Lösung: Wir betrachten den Ring $\mathbb{Z}/3\mathbb{Z}$. Es genügt zu zeigen, dass in $\mathbb{Z}/3\mathbb{Z}$ die Identität $[n^3 - 4n] = [0]$ für jedes $n \in \mathbb{Z}$ gilt. Es gilt

$$[n^3 - 4n] = [n^3] - [4n] = [n]^3 - [4] \cdot [n] = [n]^3 - [1] \cdot [n] = [n]^3 - [n].$$

Nun prüft man entweder, dass $[n]^3 = [n]$ für alle $[n] \in \mathbb{Z}/3\mathbb{Z}$ (dies ist ein Spezialfall des kleinen Satzes von Fermat), oder man rechnet weiter

$$[n]^3 - [n] = [n]([n] - [1])([n] + [1])$$

Weil entweder $[n] = [0]$, oder $[n] = [1]$ oder $[n] = -[1]$, folgt, dass

$$[n]([n] - [1])([n] + [1]) = [0]$$

für alle $n \in \mathbb{Z}$.