Universität Paderborn
INSTITUT FÜR MATHEMATIK
Prof. Dr. Bernhard Krötz, Dr. Job Kuit

Wintersemester 2024–2025

Lineare Algebra 1

3. Übungsblatt - Ausgewählte Lösungen

Hausaufgabe 3.1 Sei G eine Gruppe. Zeigen Sie, dass G abelsch ist, falls $x^2 = e$ für alle $x \in G$ gilt. Geben Sie drei Beispiele für Gruppen mit der Eigenschaft, dass $x^2 = e$ für alle $x \in G$.
Lösung: Nehmen Sie an, dass $x^2 = e$ für alle $x \in G$. Dann gilt $x = x^{-1}$ für alle $x \in G$. Wenn $x, y \in G$, dann

$$xy = x^{-1}y^{-1} = (yx)^{-1} = yx.$$

Es folgt, dass G kommutativ ist.
$(\mathbb{F}_2, +)$, $\big(\mathrm{Abb}(X, \mathbb{F}_2), +\big)$ und $\big(\mathcal{P}(X), \oplus\big)$, wobei X eine Menge ist, sind Beispiele.

Hausaufgabe 3.2 Sei X eine Menge und $\mathrm{Abb}(X, \mathbb{F}_2)$ die Menge aller Abbildungen von X nach $\mathbb{F}_2$. Für $A \in \mathcal{P}(X)$ definieren wir

$$\mathbf{1}_A : X \to \mathbb{F}_2, \quad x \mapsto \begin{cases} 1 & (x \in A) \\ 0 & (x \notin A) \end{cases}$$

Sei

$$\phi : \mathcal{P}(X) \to \mathrm{Abb}(X, \mathbb{F}_2), \quad A \mapsto \mathbf{1}_A$$

(a) Zeigen Sie, dass ϕ ein Isomorphismus von Ringen ist.
Beweis: Wir zeigen zunächst, dass ϕ eine Bijektion ist. Sei

$$\psi : \mathrm{Abb}(X, \mathbb{F}_2) \to \mathcal{P}(X), \quad f \mapsto f^{-1}(\{1\}).$$

Es gilt

$$\begin{aligned} (\psi \circ \phi)(A) &= \psi(\mathbf{1}_A) = \mathbf{1}_A^{-1}(\{1\}) = A \qquad \big(A \in \mathcal{P}(X)\big), \\ (\phi \circ \psi)(f) &= \phi\big(f^{-1}(\{1\})\big) = \mathbf{1}_{f^{-1}(\{1\})} = f \qquad \big(f \in \mathrm{Abb}(X, \mathbb{F}_2)\big). \end{aligned}$$

Es folgt, dass ψ eine Umkehrabbildung von ϕ ist und damit, dass ϕ bijektiv ist. Für alle $A, B \in \mathcal{P}(X)$ gilt

$$\mathbf{1}_{A \oplus B}(x) = \begin{cases} 0 = 1 + 1 = \mathbf{1}_A(x) + \mathbf{1}_B(x) & (x \in A \wedge x \in B), \\ 1 = 1 + 0 = \mathbf{1}_A(x) + \mathbf{1}_B(x) & (x \in A \wedge x \notin B), \\ 1 = 0 + 1 = \mathbf{1}_A(x) + \mathbf{1}_B(x) & (x \notin A \wedge x \in B), \\ 0 = 0 + 0 = \mathbf{1}_A(x) + \mathbf{1}_B(x) & (x \notin A \wedge x \notin B) \end{cases}$$

und

$$\mathbf{1}_{A \cap B}(x) = \begin{cases} 1 = 1 \cdot 1 = \mathbf{1}_A(x) \cdot \mathbf{1}_B(x) & (x \in A \wedge x \in B), \\ 0 = 1 \cdot 0 = \mathbf{1}_A(x) \cdot \mathbf{1}_B(x) & (x \in A \wedge x \notin B), \\ 0 = 0 \cdot 1 = \mathbf{1}_A(x) \cdot \mathbf{1}_B(x) & (x \notin A \wedge x \in B), \\ 0 = 0 \cdot 0 = \mathbf{1}_A(x) \cdot \mathbf{1}_B(x) & (x \notin A \wedge x \notin B). \end{cases}$$

Es folgt, dass $\phi(A \oplus B) = \phi(A) + \phi(B)$ und $\phi(A \cap B) = \phi(A) \cdot \phi(B)$ für alle $A, B \in \mathcal{P}(X)$. Weiter gilt $\phi(X) = \mathbf{1}_X$. Weil $\mathbf{1}_X$ die konstante Funktion gleich 1 ist, ist $\mathbf{1}_X$ das neutrale Element für Multiplikation in $\mathrm{Abb}(X, \mathbb{F}_2)$.

(b) Nehmen Sie an, dass X eine endliche Menge ist. Beweisen Sie, dass es genau $2^{|X|}$ Abbildungen von X nach $\{0,1\}$ gibt.
Beweis mit Induktion: Wenn $|X| = 1$, dann

$$\mathrm{Abb}(X, \mathbb{F}_2) = \{\mathbf{1}_\emptyset, \mathbf{1}_X\}$$

und darum $|\mathrm{Abb}(X, \mathbb{F}_2)| = 2$. Sei $n \in \mathbb{N}$ und nehmen Sie an, dass $|\mathrm{Abb}(Y, \mathbb{F}_2)| = 2^n$ für jede Menge Y mit $|Y| = n$. Sei X eine Menge mit $|X| = n+1$ und sei $x_0 \in X$. Wir definieren

$$F_0 = \{f : X \to \mathbb{F}_2 : f(x_0) = 0\} \quad \text{und} \quad F_1 = \{f : X \to \mathbb{F}_2 : f(x_0) = 1\}.$$

Dann gilt $\mathrm{Abb}(X, \mathbb{F}_2) = F_0 \cup F_1$ und $F_0 \cap F_1 = \emptyset$, und damit

$$|\mathrm{Abb}(X, \mathbb{F}_2)| = |F_0| + |F_1|.$$

Sei $Y = X \setminus \{x_0\}$. Einschränkung auf Y ergibt bijektive Abbildungen

$$F_0 \to \mathrm{Abb}(Y, \mathbb{F}_2), \quad f \mapsto f|_Y$$
$$F_1 \to \mathrm{Abb}(Y, \mathbb{F}_2), \quad f \mapsto f|_Y.$$

Darum gilt $|F_0| = |F_1| = |\mathrm{Abb}(Y, \mathbb{F}_2)$. Da $|Y| = |X| - 1 = n$, besitzt $\mathrm{Abb}(Y, \mathbb{F}_2)$ nach der Induktionsvoraussetzung 2^n Elemente. Es folgt

$$|\mathrm{Abb}(X, \mathbb{F}_2)| = 2 \cdot 2^n = 2^{n+1}.$$

(c) Folgern Sie, dass $|\mathcal{P}(X)| = 2^{|X|}$.
Beweis: Da ϕ eine Bijektion ist, gilt $|\mathcal{P}(X)| = |\mathrm{Abb}(X, \mathbb{F}_2)| = 2^{|X|}$.

Hausaufgabe 3.3 Sie X eine Menge. Sei $m : \mathcal{P}(X) \to \mathbb{F}_2$ einen Ringhomomorphismus und sei $U = m^{-1}(\{1\})$. Beweisen Sie folgenden Aussagen.

(a) $X \in U$ und $\emptyset \notin U$.
Beweis: Da m ein Ringhomomorphismus ist und X das neutrale Element für Multiplikation $\cap$, ist $m(X)$ das neutrale Element für Multiplikation in $\mathbb{F}_2$. Es folgt, dass $m(X) = 1$ und damit $X \in U$. Weiter is $\emptyset$ das neutrale Element für Addition $\oplus$ und darum ist $m(\emptyset)$ das neutrale Element für Addition in $\mathbb{F}_2$. Es folgt, dass $m(\emptyset) = 0$ und darum $\emptyset \notin U$.

(b) Für alle $A, B \in U$ gilt $m(A \cap B) = 1$.
Beweis: Da m ein Ringhomomorphismus ist, gilt $m(A \cap B) = m(A) \cdot m(B)$ für alle $A, B \in \mathcal{P}(X)$. Wenn $A, B \in U$, dann $m(A) = m(B) = 1$ und damit $m(A \cap B) = 1 \cdot 1 = 1$.

(c) Für alle $A \in \mathcal{P}(X)$ gilt $A \in U$ oder $X \setminus A \in U$.
Beweis: Sei $A \in \mathcal{P}(X)$. Es gilt $X = A \oplus (X \setminus A)$. Da m ein Ringhomomorphismus ist, folgt $1 = m(X) = m(A) + m(X \setminus A)$. Wenn $A \notin U$, dann $m(A) = 0$. Es folgt, dass $m(X \setminus A) = 1$ und damit $X \setminus A \in U$. Dies zeigt, dass $A \in U$ oder $X \setminus A \in U$.

(d) Wenn $A, B \in \mathcal{P}(X)$ und $A \subseteq B$, dann $m(A)m(B \setminus A) = 0$. Wenn zusätzlich $A \in U$, dann $B \setminus A \notin U$.
Beweis: Es gilt

$$m(A)m(B \setminus A) = m\big(A \cap (B \setminus A)\big) = m(\emptyset) = 0.$$

Wenn $A \in U$, dann $m(A) = 1$. Weil $m(A)m(B \setminus A) = 0$, folgt $m(B \setminus A) = 0$.

(e) Wenn $A \in U$, $B \in \mathcal{P}(X)$ und $A \subseteq B$, dann $B \in U$.
Beweis: Es gilt $m(B) = m\big(A \oplus (B \setminus A)\big) = m(A) + m(B \setminus A) = 1 + m(B \setminus A)$. Nach der vorherigen Teilaufgabe gilt $m(B \setminus A) = 0$, und damit $m(B) = 1$.

Hausaufgabe 3.4 Sei p eine Primzahl.

(a) Zeigen Sie, dass es für jedes $n \in \mathbb{Z}$ genau ein $r \in \{0, 1, 2, \ldots, p-1\}$ gibt, sodass $n - r$ durch p teilbar ist.
Beweis: Sei $k \in \mathbb{Z}$, sodass $kp \leq n < (k+1)p$. Sei $r = n - kp$. Dann $0 \leq r < p$ und $n - r = kp$ is teilbar durch p. Wenn $r' \in \{0, 1, 2, \ldots, p-1\}$ und $n - r'$ ist auch teilbar durch p, dann ist $r - r' = (n - r') - (n - r)$ auch teilbar durch p. Weil $-p < r - r' < p$, folgt, dass $r - r' = 0$.

Sei $x \in \mathbb{Z}$ und nehmen Sie an, dass x nicht durch p teilbar ist.

(b) Seien $k, l \in \{1, 2, \ldots, p-1\}$ mit $k \neq l$. Zeigen Sie, dass $kx - lx$ nicht durch p teilbar ist.
Beweis: Weil $-(p-1) \leq k - l \leq p - 1$ und $k \neq l$ ist $k - l$ nicht teilbar durch p. Da p eine Primzahl und x nicht teilbar durch p ist, ist $(k-l)x$ nicht durch p teilbar.

Seien $X := \{x, 2x, 3x, \ldots, (p-1)x\}$ und $Y := \{1, 2, 3, \ldots, p-1\}$. Sei weiter $\rho : X \to Y$ die Abbildung, sodass $n - \rho(n)$ für alle $n \in X$ durch p teilbar ist. (Diese Abbildung existiert nach Teilaufgabe (a).)

(c) Zeigen Sie, dass ρ bijektiv ist.
Beweis: Seien $n_1, n_2 \in X$, sodass $\rho(n_1) = \rho(n_2)$. Dann ist $n_1 - n_2 = \big(n_1 - \rho(n_1)\big) - \big(n_2 - \rho(n_2)\big)$ durch p teilbar. Seien $k_1, k_2 \in \{1, \ldots, p-1\}$, sodass $n_1 = k_1 x$ und $n_2 = k_2 x$. Weil x nicht durch p teilbar ist und $n_1 - n_2 = (k_1 - k_2)x$ teilbar durch p ist, folgt, dass $k_1 - k_2$ teilbar durch p ist. Weil $-(p-1) \leq k_1 - k_2 \leq p-1$, zeigt dies, dass $k_1 = k_2$ und damit $n_1 = n_2$. Damit ist bewiesen, dass ρ injektiv ist. Weil $|X| = |Y| = p - 1 < \infty$ folgt, dass ρ bijektiv ist.

(d) Zeigen Sie, dass $\left(\prod_{n \in X} n\right) - \left(\prod_{m \in Y} m\right)$ durch p teilbar ist.
Beweis: Weil ρ eine Bijektion ist, gilt

$$\left(\prod_{n \in X} n\right) - \left(\prod_{m \in Y} m\right) = \left(\prod_{n=1}^{p-1} n\right) - \left(\prod_{n=1}^{p-1} \rho(n)\right)$$

Wir werden mit Induktion beweisen, dass $\left(\prod_{n=1}^{k} n\right) - \left(\prod_{n=1}^{k} \rho(n)\right)$ für alle $k \in \{1, \ldots, p-1\}$ durch p teilbar ist. Da $1 - \rho(1)$ durch p teilbar ist, ist die Aussage für $k = 1$ wahr. Wenn $k \in \{1, \ldots, p-2\}$ und $\left(\prod_{n=1}^{k} n\right) - \left(\prod_{n=1}^{k} \rho(n)\right)$ durch p teilbar ist, dann folgt aus der Tatsache, dass $(k+1) - \rho(k+1)$ durch p teilbar ist, dass auch

$$\begin{aligned}
&\left(\prod_{n=1}^{k+1} n\right) - \left(\prod_{n=1}^{k+1} \rho(n)\right) \\
&\qquad = (k+1)\left(\left(\prod_{n=1}^{k} n\right) - \left(\prod_{n=1}^{k} \rho(n)\right)\right) + \big((k+1) - \rho(k+1)\big)\left(\prod_{n=1}^{k} \rho(n)\right)
\end{aligned}$$

durch p teilbar ist.

(e) Folgern Sie, dass $(p-1)!x^{p-1} - (p-1)!$ durch p teilbar ist.
Beweis: Es gilt

$$(p-1)!x^{p-1} - (p-1)! = \left(\prod_{n\in X} n\right) - \left(\prod_{m\in Y} m\right).$$

Nach der vorherigen Teilaufgabe ist $(p-1)!x^{p-1} - (p-1)!$ durch p teilbar.

(f) Beweisen Sie den kleinen Satz von Fermat:

Sei p eine Primzahl. Wenn $x \in \mathbb{Z}$ nicht durch p teilbar ist, dann ist $x^{p-1} - 1$ durch p teilbar.

Beweis: Da p eine Primzahl ist und keine der Zahlen $1, 2, \ldots, p-1$ durch p teilbar ist, ist auch $(p-1)!$ nicht durch p teilbar. Weil

$$(x^{p-1} - 1)(p-1)! = (p-1)!x^{p-1} - (p-1)!$$

durch p teilbar ist, folgt, dass $x^{p-1} - 1$ durch p teilbar ist.