Lösung Serie 12

Aufgabe 1 ist online auf https://echo.ethz.ch zu lösen. Schicken Sie Ihre Lösung bis spätestens **Freitag, 24. Dezember um 14:00 Uhr** ab.
Die schriftlichen Aufgaben können Sie am selben Tag in Ihrer Übungsstunde abgeben oder per SAM-Upload Tool https://sam-up.math.ethz.ch/?lecture=401-0171-00&serie=s01.

1. Betrachten Sie den $\mathbb{R}$-Vektorraum $F(\mathbb{R},\mathbb{R})$ der Funktionen von $\mathbb{R}$ nach $\mathbb{R}$ mit der Addition

$$(f+g)(x) := f(x)+g(x) \quad \forall f,g \in F(\mathbb{R},\mathbb{R})$$

und der skalaren Multiplikation

$$(\lambda f)(x) := \lambda f(x) \quad \forall f \in F(\mathbb{R},\mathbb{R}) \text{ und } \lambda \in \mathbb{R}.$$

Darin enthalten ist der Unterraum

$$P_2 := \{a_0 + a_1 x + a_2 x^2 \mid a_i \in \mathbb{R} \text{ für } i = 0,1,2\}$$

der Polynome mit Grad ≤ 2.
Welche der folgenden Aussagen sind richtig?

(a) $\text{span}\{x+1, x-1, x^2+1, x^2-1\}$ ist gleich P_2.

(b) $x+1, x-1, x^2+1, x^2-1$ sind linear unabhängig.

(c) $x+1, x-1, x^2+1, x^2-1$ bilden ein Erzeugendensystem von $F(\mathbb{R},\mathbb{R})$.

(d) $x+1, x-1, x^2+1, x^2-1$ bilden ein Erzeugendensystem von P_2.

Lösung: Korrekt sind (a) und (d), da:

✓ (a) $\text{span}\{x+1, x-1, x^2+1, x^2-1\}$ ist gleich P_2.
Richtig, denn man kann die drei Monome 1, x *und* x^2 *in der folgenden Weise*

$$1 = \frac{1}{2}(x+1) - \frac{1}{2}(x-1),$$
$$x = \frac{1}{2}(x+1) + \frac{1}{2}(x-1),$$
$$x^2 = (x^2+1) - \frac{1}{2}(x+1) + \frac{1}{2}(x-1)$$

als Linearkombination z.B. der ersten drei Vektoren $x+1$, $x-1$, x^2+1 darstellen und folglich auch alle Polynome vom Grad ≤ 2 innerhalb des Vektorraumes

$$P_2 = \mathrm{span}\{1, x, x^2\},$$

welcher als Standardbasis die drei Monome 1, x und x^2 besitzt.
Diese Relationen findet man, ausgehend von den Beobachtungen

$$\begin{aligned} 1 &= \frac{1}{2}(x+1) - \frac{1}{2}(x-1), \quad (*) \\ x &= (x+1) - 1 \quad \textit{oder} \quad x = (x-1) + 1, \\ x^2 &= (x^2+1) - 1 \end{aligned}$$

mit Einsetzen von $(*)$ als Ersatz für die 1 in den anderen Relationen.

Bemerkung: *Ebenfalls gelten*

(1) die Relationen

$$\begin{aligned} 1 &= \frac{1}{2}(x+1) - \frac{1}{2}(x-1), \\ x &= \frac{1}{2}(x+1) + \frac{1}{2}(x-1), \\ x^2 &= (x^2-1) + \frac{1}{2}(x+1) - \frac{1}{2}(x-1), \end{aligned}$$

welche die drei Monome 1, x und x^2 als Linearkombinationen der Vektoren $x+1$, $x-1$ und x^2-1 darstellen.

(2) die Relationen

$$\begin{aligned} 1 &= \frac{1}{2}(x^2+1) - \frac{1}{2}(x^2-1), \\ x &= (x+1) - \frac{1}{2}(x^2+1) + \frac{1}{2}(x^2-1), \\ x^2 &= \frac{1}{2}(x^2+1) + \frac{1}{2}(x^2-1), \end{aligned}$$

welche die drei Monome 1, x und x^2 als Linearkombinationen der Vektoren $x+1$, x^2+1 und x^2-1 darstellen.

(3) die Relationen

$$\begin{aligned} 1 &= \frac{1}{2}(x^2+1) - \frac{1}{2}(x^2-1), \\ x &= (x-1) + \frac{1}{2}(x^2+1) - \frac{1}{2}(x^2-1), \\ x^2 &= \frac{1}{2}(x^2+1) + \frac{1}{2}(x^2-1), \end{aligned}$$

welche die drei Monome 1, x *und* x^2 *als Linearkombinationen der Vektoren* $x-1$, x^2+1 *und* x^2-1 *darstellen.*

Diese Relationen (1), (2) und (3) findet man gleich wie oben, ausgehend von den Beobachtungen

$$\begin{aligned} 1 &= \frac{1}{2}(x+1) - \frac{1}{2}(x-1), \quad (*) \\ 1 &= \frac{1}{2}(x^2+1) - \frac{1}{2}(x^2-1), \quad (**) \\ x &= (x+1) - 1, \\ x &= (x-1) + 1, \\ x^2 &= (x^2+1) - 1, \\ x^2 &= (x^2-1) + 1 \end{aligned}$$

mit Einsetzen von $(*)$ *und* $(**)$ *als Ersatz für die* 1 *in den anderen Relationen.*

(b) $x+1, x-1, x^2+1, x^2-1$ sind linear unabhängig.
Falsch, z.B. gilt die lineare Abhängigkeitsrelation

$$x^2 - 1 = (x^2+1) - (x+1) + (x-1),$$

welche sich aus der Beobachtung $x^2 - 1 = (x^2+1) - 2$ *mit dem obigen Ersatz* $2 = 2 \cdot 1 = 2 \cdot (*)$ *ergibt.*
Der vierte Vektor x^2-1 *lässt sich also mit den ersten drei Vektoren* $x+1$, $x-1$ *und* x^2+1 *erzeugen oder gleichbedeutend als Linearkombination von* $x+1$, $x-1$ *und* x^2+1 *darstellen.*
Ebenfalls gilt

(1) die lineare Abhängigkeitsrelation

$$x + 1 = (x-1) + (x^2+1) - (x^2-1),$$

welche sich aus der Beobachtung $x + 1 = (x-1) + 2$ *mit dem obigen Ersatz* $2 = 2 \cdot 1 = 2 \cdot (**)$ *ergibt.*

(2) die lineare Abhängigkeitsrelation

$$x - 1 = (x+1) - (x^2+1) + (x^2-1),$$

welche sich aus der Beobachtung $x - 1 = (x+1) - 2$ *mit dem obigen Ersatz* $2 = 2 \cdot 1 = 2 \cdot (**)$ *ergibt.*

(3) die lineare Abhängigkeitsrelation

$$x^2 + 1 = (x^2 - 1) + (x + 1) - (x - 1),$$

welche sich aus der Beobachtung $x^2 + 1 = (x^2 - 1) + 2$ *mit dem obigen Ersatz* $2 = 2 \cdot 1 = 2 \cdot (*)$ *ergibt.*

Bemerkung: *Auch alle anderen Vektoren (Polynome) in* P_2*, lassen sich mit der vorherigen Erklärung in (a) und den Relationen*

$$\begin{aligned} 1 &= \frac{1}{2}(x+1) - \frac{1}{2}(x-1), \\ x &= \frac{1}{2}(x+1) + \frac{1}{2}(x-1), \\ x^2 &= (x^2+1) - \frac{1}{2}(x+1) + \frac{1}{2}(x-1) \end{aligned}$$

aus (a) als Linearkombinationen von $x + 1$*,* $x - 1$ *und* $x^2 + 1$ *darstellen.*

(c) $x + 1, x - 1, x^2 + 1, x^2 - 1$ bilden ein Erzeugendensystem von $F(\mathbb{R}, \mathbb{R})$.
Falsch, z.B. ist das Polynom

$$x^3 \in F(\mathbb{R}, \mathbb{R})$$

vom Grad 3 *keine Linearkombination der gegebenen vier Polynome*

$$x + 1, x - 1, x^2 + 1, x^2 - 1,$$

da deren Grad ≤ 2 *ist.*
Es existiert auch gar kein Erzeugendensystem von $F(\mathbb{R}, \mathbb{R})$ *aus nur endlich vielen Vektoren. Das sieht man daran, dass die unendlich vielen Vektoren (Funktionen)*

$$\delta_0(x), \delta_1(x), \delta_2(x), \ldots, \delta_i(x), \ldots \in F(\mathbb{R}, \mathbb{R}),$$

wobei

$$\delta_i(x) = \begin{cases} 1, & \text{wenn } x = i; \\ 0, & \text{wenn } x \neq i \end{cases}$$

linear unabhängig sind, da sie alle an verschiedenen Stellen den Wert 1 *annehmen und sonst überall gleich Null sind.*

✓ (d) $x + 1, x - 1, x^2 + 1, x^2 - 1$ bilden ein Erzeugendensystem von P_2.
Richtig, dies ist per Definition äquivalent zur ersten Aussage (a), dass

$$\operatorname{span}\{x + 1, x - 1, x^2 + 1, x^2 - 1\} = P_2 = \operatorname{span}\{1, x, x^2\}.$$

2. Bestimmen Sie, ob

$$V = \mathbb{R}^3 = \left\{ \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} \middle| a_i \in \mathbb{R} \text{ für } i = 1, 2, 3 \right\},$$

versehen mit der Standard-Skalarmultiplikation $\cdot$ gegeben durch

$$\lambda \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} \lambda x_1 \\ \lambda x_2 \\ \lambda x_3 \end{pmatrix} \quad \text{für } \lambda \in \mathbb{R}$$

und der Addition $\oplus$, definiert durch

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \oplus \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} := \begin{pmatrix} x_1 + y_2 \\ x_2 - y_1 \\ x_3 + y_3 \end{pmatrix},$$

ein $\mathbb{R}$-Vektorraum ist.

Lösung: Wir müssen überprüfen, ob die Rechenregeln (A1)-(M3) der Vorlesungswochen 10 und 11 für die vorgegebenen Operationen gelten. Für $x = \left(\begin{smallmatrix} x_1 \\ x_2 \\ x_3 \end{smallmatrix}\right) \in V = \mathbb{R}^3$ und $y = \left(\begin{smallmatrix} y_1 \\ y_2 \\ y_3 \end{smallmatrix}\right) \in V = \mathbb{R}^3$ gilt

$$x \oplus y = \begin{pmatrix} x_1 + y_2 \\ x_2 - y_1 \\ x_3 + y_3 \end{pmatrix}, \text{ aber } \quad y \oplus x = \begin{pmatrix} y_1 + x_2 \\ y_2 - x_1 \\ y_3 + x_3 \end{pmatrix},$$

also gilt im Allgemein <u>nicht</u> $x \oplus y = y \oplus x$ und das Kommutativgesetz (A1) der Addition $\oplus$ ist somit nicht erfüllt.
Daher ist $(V, \oplus, \cdot) = (\mathbb{R}^3, \oplus, \cdot)$ sicher kein $\mathbb{R}$-Vektorraum.

3. *Unterräume von* $\mathbb{R}^3$

(a) Sei V die folgende Menge von Vektoren:

$$V = \left\{ \begin{pmatrix} x \\ y \\ 3x - y \end{pmatrix} \in \mathbb{R}^3 \middle| x, y \in \mathbb{R} \right\}.$$

Zeigen Sie, dass V ein Unterraum des reellen Vektorraumes $\mathbb{R}^3$ ist.

(b) Ist die Menge

$$W = \left\{ \begin{pmatrix} x \\ 3x - 1 \\ x \end{pmatrix} \in \mathbb{R}^3 \middle| x \in \mathbb{R} \right\}$$

auch ein Unterraum von $\mathbb{R}^3$? Begründen Sie Ihre Antwort.

Lösung: Die zwei Mengen V und W sind offensichtlich beides nichtleere Teilmengen von $\mathbb{R}^3$.

(a) Wir zeigen, dass

$$V = \left\{ \begin{pmatrix} x \\ y \\ 3x - y \end{pmatrix} \in \mathbb{R}^3 \middle| x, y \in \mathbb{R} \right\}$$

ein Unterraum von $\mathbb{R}^3$ ist, indem wir die Abgeschlossenheit unter der Addition (1) und der Multiplikation mit Skalaren (2) zeigen (Vorlesungswoche 11):

(1) **Abgeschlossenheit unter der Addition:**
Seien mit $x = x_1$, $y = y_1$ und $x = x_2$, $y = y_2$

$$a = \begin{pmatrix} x_1 \\ y_1 \\ 3x_1 - y_1 \end{pmatrix} \in V \quad \text{und} \quad b = \begin{pmatrix} x_2 \\ y_2 \\ 3x_2 - y_2 \end{pmatrix} \in V.$$

Es gilt, dass

$$\begin{aligned} a + b &= \begin{pmatrix} x_1 \\ y_1 \\ 3x_1 - y_1 \end{pmatrix} + \begin{pmatrix} x_2 \\ y_2 \\ 3x_2 - y_2 \end{pmatrix} \\ &= \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 \\ 3x_1 - y_1 + 3x_2 - y_2 \end{pmatrix} \\ &= \begin{pmatrix} x_1 + x_2 \\ y_1 + y_2 \\ 3(x_1 + x_2) - (y_1 + y_2) \end{pmatrix} \\ &= \begin{pmatrix} x_3 \\ y_3 \\ 3x_3 - y_3 \end{pmatrix} \in V, \end{aligned}$$

wobei

$$\begin{aligned} x_3 &= x_1 + x_2, \\ y_3 &= y_1 + y_2. \end{aligned}$$

(2) **Abgeschlossenheit unter der Multiplikation mit Skalaren:**
Für $a = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix}$ wie oben und $\alpha \in \mathbb{R}$, dann gilt

$$\alpha a = \alpha \cdot \begin{pmatrix} x_1 \\ y_1 \\ 3x_1 - y_1 \end{pmatrix} = \begin{pmatrix} \alpha x_1 \\ \alpha y_1 \\ 3\alpha x_1 - \alpha y_1 \end{pmatrix} = \begin{pmatrix} x_4 \\ y_4 \\ 3x_4 - y_4 \end{pmatrix} \in V,$$

wobei

$$x_4 = \alpha x_1,$$
$$y_4 = \alpha y_1.$$

Also ist V ein Unterraum von $\mathbb{R}^3$.

(b) Betrachte nun die Menge

$$W = \left\{ \begin{pmatrix} x \\ 3x-1 \\ x \end{pmatrix} \in \mathbb{R}^3 \middle| x \in \mathbb{R} \right\}.$$

Seien mit $x = x_1$ und $x = x_2$

$$a = \begin{pmatrix} x_1 \\ 3x_1 - 1 \\ x_1 \end{pmatrix} \in W \quad \text{und} \quad b = \begin{pmatrix} x_2 \\ 3x_2 - 1 \\ x_2 \end{pmatrix} \in W.$$

Dann gilt

$$\begin{aligned} a + b &= \begin{pmatrix} x_1 \\ 3x_1 - 1 \\ x_1 \end{pmatrix} + \begin{pmatrix} x_2 \\ 3x_2 - 1 \\ x_2 \end{pmatrix} \\ &= \begin{pmatrix} x_1 + x_2 \\ 3x_1 + 3x_2 - 2 \\ x_1 + x_2 \end{pmatrix} \\ &= \begin{pmatrix} x_1 + x_2 \\ 3(x_1 + x_2) - 2 \\ x_1 + x_2 \end{pmatrix} \notin W, \end{aligned}$$

da nur das Element

$$\begin{pmatrix} x_1 + x_2 \\ 3(x_1 + x_2) - 1 \\ x_1 + x_2 \end{pmatrix} \in W$$

mit $x = x_1 + x_2$ in W liegt.
Daher ist die Menge W mit den Vektorraumoperationen von $\mathbb{R}^3$ also sicherlich kein Unterraum von $\mathbb{R}^3$, da die Menge W versehen mit diesen Vektorraumoperationen unter der Addition nicht abgeschlossen ist.

Alternativ lässt sich argumentieren, dass W den Nullvektor nicht enthält, sondern nur den Vektor $\begin{pmatrix} 0 \\ -1 \\ 0 \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$, aber jeder Unterraum muss den Nullvektor enthalten, da ein Unterraum wiederum ein Vektorraum ist.

4. *Der Vektorraum $\mathbb{Z}_2^n$ über dem Körper $\mathbb{Z}_2$*

(a) Die Menge $\mathbb{Z}_2 := \{0, 1\}$, versehen mit den Rechenregeln

$\oplus$	0	1
0	0	1
1	1	0

$\odot$	0	1
0	0	0
1	0	1

ist ein Körper. Das heisst, es gelten bezüglich Addition $\oplus$ und Multiplikation $\odot$ die selben Rechenregeln wie in $\mathbb{R}, \mathbb{C}$ oder $\mathbb{Q}$. Versehen Sie

$$V = \mathbb{Z}_2^n = \left\{(x_1, x_2, \ldots, x_n)^T \mid x_i \in \mathbb{Z}_2 \text{ für } i = 1, 2, \ldots, n\right\}$$

mit den passenden Vektoroperationen und zeigen Sie, dass V damit ein Vektorraum über dem Körper $\mathbb{Z}_2$ wird.

(b) Sei die Menge C gegeben durch

$$C = \{x \in \mathbb{Z}_2^n \mid x_1 + x_2 + \ldots + x_n \text{ ist gerade}\},$$

wobei $x = (x_1, x_2, \ldots, x_n)^T$.
Zeigen Sie, dass C ein Unterraum von $\mathbb{Z}_2^n$ ist.

Bemerkung: C ist ein sogenannter 1-fehlererkennender Code: Wird ein Bit einer Nachricht $x \in C$ falsch übermittelt, kann der Empfänger dies feststellen (wie?) und die Wiederholung der Übermittlung veranlassen.

Lösung:

(a) Man definiere in $\mathbb{Z}_2^n$ die Vektorraumoperationen gleich wie in $\mathbb{R}^n$, nämlich

$$\begin{aligned}(x_1, x_2, \ldots, x_n)^T + (y_1, y_2, \ldots, y_n)^T &:= (x_1 \oplus y_1, x_2 \oplus y_2, \ldots, x_n \oplus y_n)^T,\\ \alpha \cdot (x_1, x_2, \ldots, x_n)^T &:= (\alpha \odot x_1, \alpha \odot x_2, \ldots, \alpha \odot x_n)^T \quad \text{für} \quad \alpha \in \mathbb{Z}_2.\end{aligned}$$

Man rechnet analog wie im Fall $\mathbb{R}^n$ nach, dass für $\mathbb{Z}_2^n$ die folgenden Rechnenregeln (A0)-(M3) aus den Vorlesungswochen 10 und 11 gelten, denn es gilt:

(A0) Es gilt $\mathbb{Z}_2^n \neq \emptyset$:
Die Menge $\mathbb{Z}_2^n$ ist nicht leer, da zum Beispiel $(1, 1, \ldots, 1) \in \mathbb{Z}_2^n$ ist.

(A1) Kommutativigesetz der Addition + auf $\mathbb{Z}_2^n$:
Es gilt

$$\begin{aligned}x + y &= (x_1, x_2, \ldots, x_n)^T + (y_1, y_2, \ldots, y_n)^T\\ &= (x_1 \oplus y_1, x_2 \oplus y_2, \ldots, x_n \oplus y_n)^T\\ &= (y_1 \oplus x_1, y_2 \oplus x_2, \ldots, y_n \oplus x_n)^T\\ &= (y_1, y_2, \ldots, y_n)^T + (x_1, x_2, \ldots, x_n)^T\\ &= y + x,\end{aligned}$$

da $\oplus$ kommutativ ist und somit $x_i \oplus y_i = y_i \oplus x_i$ für alle $x_i, y_i \in \mathbb{Z}_2$ gilt, weil

$$\begin{aligned} 0 \oplus 0 &= 0, \\ 0 \oplus 1 = 1 \oplus 0 &= 1, \\ 1 \oplus 1 &= 0. \end{aligned}$$

(A2) Assoziativgesetz der Addition + auf $\mathbb{Z}_2^n$:
Es gilt

$$\begin{aligned} (x+y)+z &= \big((x_1, x_2, \ldots, x_n)^T + (y_1, y_2, \ldots, y_n)^T\big) + (z_1, z_2, \ldots, z_n)^T \\ &= (x_1 \oplus y_1, x_2 \oplus y_2, \ldots, x_n \oplus y_n)^T + (z_1, z_2, \ldots, z_n)^T \\ &= ((x_1 \oplus y_1) \oplus z_1, (x_2 \oplus y_2) \oplus z_2, \ldots, (x_n \oplus y_n) \oplus z_n)^T \\ &= (x_1 \oplus (y_1 \oplus z_1), x_2 \oplus (y_2 \oplus z_2), \ldots, x_n \oplus (y_n \oplus z_n))^T \\ &= (x_1, x_2, \ldots, x_n)^T + (y_1 \oplus z_1, y_2 \oplus z_2, \ldots, y_n \oplus z_n)^T \\ &= (x_1, x_2, \ldots, x_n)^T + \big((y_1, y_2, \ldots, y_n)^T + (z_1, z_2, \ldots, z_n)^T\big) \\ &= x + (y+z), \end{aligned}$$

da $\oplus$ assoziativ ist und somit $(x_i \oplus y_i) \oplus z_i = x_i \oplus (y_i \oplus z_i)$ für alle $x_i, y_i, z_i \in \mathbb{Z}_2$ gilt, weil

$$\begin{aligned} &\underbrace{(0 \oplus 0)}_{=0} \oplus 0 = 0 \oplus 0 = 0 \oplus \underbrace{(0 \oplus 0)}_{=0}, \\ &\underbrace{(0 \oplus 0)}_{=0} \oplus 1 = 0 \oplus 1 = 0 \oplus \underbrace{(0 \oplus 1)}_{=1}, \\ &\underbrace{(0 \oplus 1)}_{=1} \oplus 0 = 1 \oplus 0 = 0 \oplus 1 = 0 \oplus \underbrace{(1 \oplus 0)}_{=1}, \\ &\underbrace{(0 \oplus 1)}_{=1} \oplus 1 = 1 \oplus 1 = 0 = 0 \oplus 0 = 0 \oplus \underbrace{(1 \oplus 1)}_{=0}, \\ &\underbrace{(1 \oplus 0)}_{=1} \oplus 0 = 1 \oplus 0 = 1 \oplus \underbrace{(0 \oplus 0)}_{=0}, \\ &\underbrace{(1 \oplus 0)}_{=1} \oplus 1 = 1 \oplus 1 = 1 \oplus \underbrace{(0 \oplus 1)}_{=1}, \\ &\underbrace{(1 \oplus 1)}_{=0} \oplus 0 = 0 \oplus 0 = 0 = 1 \oplus 1 = 1 \oplus \underbrace{(1 \oplus 0)}_{=1}, \\ &\underbrace{(1 \oplus 1)}_{=0} \oplus 1 = 0 \oplus 1 = 1 \oplus 0 = 1 \oplus \underbrace{(1 \oplus 1)}_{=0}. \end{aligned}$$

(A3) Existenz des Nullelementes:
Es gilt mit dem Nullelement

$$0 = (0, 0, \ldots, 0)^T,$$

dass

$$\begin{aligned} x + 0 &= (x_1, x_2, \ldots, x_n)^T + (0, 0, \ldots, 0)^T \\ &= (x_1 \oplus 0, x_2 \oplus 0, \ldots, x_n \oplus 0)^T \\ &= (x_1, x_2, \ldots, x_n)^T \\ &= x, \end{aligned}$$

da $x_i \oplus 0 = x_i$ für alle $x_i \in \mathbb{Z}_2$, weil

$$\begin{aligned} 0 \oplus 0 &= 0, \\ 1 \oplus 0 &= 1. \end{aligned}$$

(A4) Existenz des additiven Inversen:
Das additive Inverse zum Element $x = (x_1, x_2, \ldots, x_n)^T$ ist

$$-x = (x_1, x_2, \ldots, x_n)^T$$

und jedes Element $x \in \mathbb{Z}_2^n$ ist daher sein eigenes additives Inverses $-x = x$. Dies gilt, da

$$\begin{aligned} x + (-x) &= (x_1, x_2, \ldots, x_n)^T + (x_1, x_2, \ldots, x_n)^T \\ &= (x_1 \oplus x_1, x_2 \oplus x_2, \ldots, x_n \oplus x_n)^T \\ &= 0, \end{aligned}$$

weil $x_i \oplus x_i = 0$ für alle $x_i \in \mathbb{Z}_2$, da

$$\begin{aligned} 0 \oplus 0 &= 0, \\ 1 \oplus 1 &= 0. \end{aligned}$$

(M1) 1. Gesetz der Skalarmultiplikation:
Es gilt

$$\begin{aligned} (\alpha \odot \beta)x &= (\alpha \odot \beta) \cdot (x_1, x_2, \ldots, x_n)^T \\ &= ((\alpha \odot \beta) \odot x_1, (\alpha \odot \beta) \odot x_2, \ldots, (\alpha \odot \beta) \odot x_n)^T \\ &= (\alpha \odot (\beta \odot x_1), \alpha \odot (\beta \odot x_2), \ldots, \alpha \odot (\beta \odot x_n))^T \\ &= \alpha \cdot (\beta \odot x_1, \beta \odot x_2, \ldots, \beta \odot x_n)^T \\ &= \alpha \cdot \big(\beta \cdot (x_1, x_2, \ldots, x_n)^T\big) \\ &= \alpha(\beta x), \end{aligned}$$

da $(\alpha \odot \beta) \odot x_i = \alpha \odot (\beta \odot x_i)$ für alle $\alpha, \beta, x_i \in \mathbb{Z}_2$, weil

$$
\begin{aligned}
&\underbrace{(0 \odot 0)}_{=0} \odot 0 = 0 \odot 0 = 0 \odot \underbrace{(0 \odot 0)}_{=0},\\
&\underbrace{(0 \odot 0)}_{=0} \odot 1 = 0 \odot 1 = 0 = 0 \odot 0 = 0 \odot \underbrace{(0 \odot 1)}_{=0},\\
&\underbrace{(0 \odot 1)}_{=0} \odot 0 = 0 \odot 0 = 0 \odot \underbrace{(1 \odot 0)}_{=0},\\
&\underbrace{(0 \odot 1)}_{=0} \odot 1 = 0 \odot 1 = 0 = 0 \odot 0 = 0 \odot \underbrace{(1 \odot 1)}_{=0},\\
&\underbrace{(1 \odot 0)}_{=0} \odot 0 = 0 \odot 0 = 0 = 1 \odot 0 = 1 \odot \underbrace{(0 \odot 0)}_{=0},\\
&\underbrace{(1 \odot 0)}_{=0} \odot 1 = 0 \odot 1 = 1 \odot 0 = 1 \odot \underbrace{(0 \odot 1)}_{=0},\\
&\underbrace{(1 \odot 1)}_{=1} \odot 0 = 1 \odot 0 = 1 \odot \underbrace{(1 \odot 0)}_{=0},\\
&\underbrace{(1 \odot 1)}_{=1} \odot 1 = 1 \odot 1 = 1 \odot \underbrace{(1 \odot 1)}_{=1}.
\end{aligned}
$$

(M2) 2. Gesetz der Skalarmultiplikation $\cdot$:
Es gilt

$$
\begin{aligned}
(\alpha \oplus \beta) \cdot x &= (\alpha \oplus \beta) \cdot (x_1, x_2, \ldots, x_n)^T\\
&= ((\alpha \oplus \beta) \odot x_1, (\alpha \oplus \beta) \odot x_2, \ldots, (\alpha \oplus \beta) \odot x_n)^T\\
&= ((\alpha \odot x_1) \oplus (\beta \odot x_1), (\alpha \odot x_2) \oplus (\beta \odot x_2), \ldots, (\alpha \odot x_n) \oplus (\beta \odot x_n))^T\\
&= (\alpha \odot x_1, \alpha \odot x_2, \ldots, \alpha \odot x_n)^T + (\beta \odot x_1, \beta \odot x_2, \ldots, \beta \odot x_n)^T\\
&= \alpha \cdot (x_1, x_2, \ldots, x_n)^T + \beta \cdot (x_1, x_2, \ldots, x_n)^T\\
&= \alpha x + \beta x,
\end{aligned}
$$

da $(\alpha \oplus \beta) \odot x_i = (\alpha \odot x_i) \oplus (\beta \odot x_i)$ für alle $\alpha, \beta, x_i \in \mathbb{Z}_2$, weil

$$
\begin{aligned}
&\underbrace{(0 \oplus 0)}_{=0} \odot 0 = 0 \odot 0 = 0 = 0 \oplus 0 = \underbrace{(0 \odot 0)}_{=0} \oplus \underbrace{(0 \odot 0)}_{=0},\\
&\underbrace{(0 \oplus 0)}_{=0} \odot 1 = 0 \odot 1 = 0 = 0 \oplus 0 = \underbrace{(0 \odot 1)}_{=0} \oplus \underbrace{(0 \odot 1)}_{=0},\\
&\underbrace{(0 \oplus 1)}_{=1} \odot 0 = 1 \odot 0 = 0 = 0 \oplus 0 = \underbrace{(0 \odot 0)}_{=0} \oplus \underbrace{(1 \odot 0)}_{=0},\\
&\underbrace{(0 \oplus 1)}_{=1} \odot 1 = 1 \odot 1 = 1 = 0 \oplus 1 = \underbrace{(0 \odot 1)}_{=0} \oplus \underbrace{(1 \odot 1)}_{=1},\\
&\underbrace{(1 \oplus 0)}_{=1} \odot 0 = 1 \odot 0 = 0 = 0 \oplus 0 = \underbrace{(1 \odot 0)}_{=0} \oplus \underbrace{(0 \odot 0)}_{=0},\\
&\underbrace{(1 \oplus 0)}_{=1} \odot 1 = 1 \odot 1 = 1 = 1 \oplus 0 = \underbrace{(1 \odot 1)}_{=1} \oplus \underbrace{(0 \odot 1)}_{=0},\\
&\underbrace{(1 \oplus 1)}_{=0} \odot 0 = 0 \odot 0 = 0 = 0 \oplus 0 = \underbrace{(1 \odot 0)}_{=0} \oplus \underbrace{(1 \odot 0)}_{=0},\\
&\underbrace{(1 \oplus 1)}_{=0} \odot 1 = 0 \odot 1 = 0 = 1 \oplus 1 = \underbrace{(1 \odot 1)}_{=1} \oplus \underbrace{(1 \odot 1)}_{=1}.
\end{aligned}
$$

Distributivgesetz der Addition $+$ und Skalarmultiplikation $\cdot$:

$$
\begin{aligned}
\alpha \cdot (x + y) &= \alpha \cdot \big((x_1, x_2, \ldots, x_n)^T + (y_1, y_2, \ldots, y_n)^T\big)\\
&= \alpha \cdot (x_1 \oplus y_1, x_2 \oplus y_2, \ldots, x_n \oplus y_n)^T\\
&= (\alpha \odot (x_1 \oplus y_1), \alpha \odot (x_2 \oplus y_2), \ldots, \alpha \odot (x_n \oplus y_n))^T\\
&= ((\alpha \odot x_1) \oplus (\alpha \odot y_1), (\alpha \odot x_2) \oplus (\alpha \odot y_2), \ldots, (\alpha \odot x_n) \oplus (\alpha \odot y_n))^T\\
&= (\alpha \odot x_1, \alpha \odot x_2, \ldots, \alpha \odot x_n)^T + (\alpha \odot y_1, \alpha \odot y_2, \ldots, \alpha \odot y_n)^T\\
&= \alpha \cdot (x_1, x_2, \ldots, x_n)^T + \alpha \cdot (y_1, y_2, \ldots, y_n)^T\\
&= \alpha x + \alpha y,
\end{aligned}
$$

da $\alpha \odot (x_i \oplus y_i) = (\alpha \odot x_i) \oplus (\alpha \odot y_i)$ für alle $\alpha, x_i, y_i \in \mathbb{Z}_2$, weil

$$
\begin{aligned}
0 \odot \underbrace{(0 \oplus 0)}_{=0} &= 0 \odot 0 = 0 = 0 \oplus 0 = \underbrace{(0 \odot 0)}_{=0} \oplus \underbrace{(0 \odot 0)}_{=0}, \\
0 \odot \underbrace{(0 \oplus 1)}_{=1} &= 0 \odot 1 = 0 = 0 \oplus 0 = \underbrace{(0 \odot 0)}_{=0} \oplus \underbrace{(0 \odot 1)}_{=0}, \\
0 \odot \underbrace{(1 \oplus 0)}_{=1} &= 0 \odot 1 = 0 = 0 \oplus 0 = \underbrace{(0 \odot 1)}_{=0} \oplus \underbrace{(0 \odot 0)}_{=0}, \\
0 \odot \underbrace{(1 \oplus 1)}_{=0} &= 0 \odot 0 = 0 = 0 \oplus 0 = \underbrace{(0 \odot 1)}_{=0} \oplus \underbrace{(0 \odot 1)}_{=0}, \\
1 \odot \underbrace{(0 \oplus 0)}_{=0} &= 1 \odot 0 = 0 = 0 \oplus 0 = \underbrace{(1 \odot 0)}_{=0} \oplus \underbrace{(1 \odot 0)}_{=0}, \\
1 \odot \underbrace{(0 \oplus 1)}_{=1} &= 1 \odot 1 = 1 = 0 \oplus 1 = \underbrace{(1 \odot 0)}_{=0} \oplus \underbrace{(1 \odot 1)}_{=1}, \\
1 \odot \underbrace{(1 \oplus 0)}_{=1} &= 1 \odot 1 = 1 = 1 \oplus 0 = \underbrace{(1 \odot 1)}_{=1} \oplus \underbrace{(1 \odot 0)}_{=0}, \\
1 \odot \underbrace{(1 \oplus 1)}_{=0} &= 1 \odot 0 = 0 = 1 \oplus 1 = \underbrace{(1 \odot 1)}_{=1} \oplus \underbrace{(1 \odot 1)}_{=1}.
\end{aligned}
$$

(M3) Skalare Multiplikation mit $1 \in \mathbb{Z}_2$:
Es gilt

$$
\begin{aligned}
1 \cdot x &= 1 \cdot (x_1, x_2, \ldots, x_n)^T \\
&= (1 \odot x_1, 1 \odot x_2, \ldots, 1 \odot x_n)^T \\
&= (x_1, x_2, \ldots, x_n)^T \\
&= x,
\end{aligned}
$$

da $1 \odot x_i = x_i$ für alle $x_i \in \mathbb{Z}_2$, weil

$$
\begin{aligned}
1 \odot 0 &= 0, \\
1 \odot 1 &= 1.
\end{aligned}
$$

Dies zeigt, dass $\mathbb{Z}_2^n$ mit den oben definierten Vektorraumoperationen ein Vektorraum über $\mathbb{Z}_2$ ist.

(b) Wir zeigen die Abgeschlossenheit von C unter der Addition und der Multiplikation mit Skalaren (Vorlesungswoche 11).

Für $x = (x_1, x_2, \ldots, x_n) \in C$ und $y = (y_1, y_2, \ldots, y_n) \in C$ gilt

(1) $x_1 + x_2 + \cdots + x_n$ gerade, und

(2) $y_1 + y_2 + \cdots + y_n$ gerade.

Daraus folgt, dass

$$(x_1 + y_1) + (x_2 + y_2) + \cdots + (x_n + y_n) = (x_1 + x_2 + \cdots + x_n) + (y_1 + y_2 + \cdots + y_n)$$

auch eine gerade Zahl ist. Damit ist aber auch

$$(x_1 \oplus y_1) + (x_2 \oplus y_2) + \cdots + (x_n \oplus y_n)$$

eine gerade Zahl, da $x_i + y_i$ genau dann gerade (ungerade) ist, wenn $x_i \oplus y_i$ gerade (ungerade) ist. Dies zeigt, dass

$$x + y = (x_1 \oplus y_1, x_2 \oplus y_2, \ldots, x_n \oplus y_n)^T$$

in C liegt und C somit unter der Addition + abgeschlossen ist.

Ausserdem gilt für $x \in C$ und $\alpha \in \mathbb{Z}_2$, da $\odot$ genau dasselbe tut wie die Standardmultiplikation auf $\mathbb{Z}_2$, dass

$$(\alpha \odot x_1 + \alpha \odot x_2 + \cdots \alpha \odot x_n) = \alpha(x_1 + x_2 + \cdots + x_n) = \begin{cases} x_1 + x_2 + \cdots + x_n, & \text{für } \alpha = 1; \\ 0, & \text{für } \alpha = 0. \end{cases}$$

Da die rechte Seite in beiden Fällen eine gerade Zahl ist, gilt

$$\alpha \cdot x = (\alpha \odot x_1, \alpha \odot x_2, \ldots, \alpha \odot x_n)^T \in C$$

und C ist daher auch abgeschlossen unter der Multiplikation $\cdot$ mit Skalaren.

Folglich ist die Menge C ein Untervektorraum von $\mathbb{Z}_2^n$.

Erklärung zur Bemerkung: Wir nehmen an, dass die Nachricht $x = (1011101)$ von einem Sender an einen Empfänger übermittelt werden soll. Geschieht das einfach so, kann der Empfänger schlecht beurteilen, ob die Übertragung korrekt funktioniert hat oder ob eines der ankommenden Bits fehlerhaft ist.
Um hier mehr Sicherheit zu erhalten, wird der Nachricht x hinten ein zusätzliches Bit angehängt, sodass das Resultat in C liegt, also dass die Summe der einzelnen Bits gerade ist. Die neue Nachricht lautet in unserem Fall also $x' = (10111011)$. Erhält der Empfänger nun beispielsweise eine Nachricht mit ungerader Bitsumme, so weiss er, dass bei der Übertragung ein Fehler passiert sein muss und er kann die Wiederholung der Übermittlung veranlassen. Bei diesem Beispiel wird ein Fehler bei zwei Bits natürlich nicht mehr erkannt. Man kann aber k-fehlererkennende Codes finden für beliebige $k \in \mathbb{N}$, welche bei bis zu jeweils k fehlerhaften Bits "Alarm schlagen". Diese sind jedoch aufwändiger, wodurch die Länge der Nachricht zunimmt und die Übertragung entsprechend länger dauert (und ebenso fehleranfälliger wird). Hier muss man - je nach Verwendungszweck - einen Kompromiss eingehen.