2. Gruppen, Körper, Vektorräume

Definition 2.1: Eine Gruppe ist ein Tupel $(G, \circ)$ eine Menge G mit einer abgeschlossenen Verknüpfung $\circ: G \times G \to G$, für die gilt:

1) $\exists e \in G: \forall x \in G$ gilt $e \circ x = x$ (Neutrales Element)
2) $\forall x \in G \ \exists x^{-1} \in G$ mit $x^{-1} \circ x = e$ (Inverses Element)
3) $\forall x, y, z \in G$ gilt: $(x \circ y) \circ z = x \circ (y \circ z)$ (Assoziativität)

Oft lässt man „$\circ$" weg und schreibt die Gruppe multiplikativ.
Aus 1) – 3) folgen:

1) $x x^{-1} = e$
2) $xe = x$
3) e ist eindeutig
4) x^{-1} ist eindeutig und $(x^{-1})^{-1} = x$

Gilt $\forall x, y \in G$ die Gleichheit $xy = yx$, so heißt G Abelsch.

Beispiele:

1) $(\mathbb{N}, +)$ ist keine Gruppe ($0 \notin \mathbb{N}$, und $\mathbb{N}$ hatte keine Inversen)
2) $(\mathbb{N}_0, +)$ ist Abelsche Gruppe ✓
3) $(\mathbb{Z}, +)$ ist Abelsche Gruppe ✓
4) Mit $\mathbb{Q}^* := \mathbb{Q} \setminus \{0\}$ ist $(\mathbb{Q}^*, \cdot)$ Abelsche Gruppe ✓
5) Symmetrische Gruppe für eine endliche Menge X: ($n := |X|$)
   $S_n := \{f \in X^X : f \text{ bijektiv}\}$, wobei die Verknüpfung die Komposition $\circ$ zweier Funktionen ist.
   Die Elemente von S_n heißen Permutation

Definition 2.2 Seien G, G' Gruppen. Das **direkte Produkt** $G \times G'$ ist wieder eine Gruppe mit der Verknüpfung

$$(x,x')(y,y') := (x \circ y, x' \circ' y')$$

$\rightsquigarrow$ Einselement (e,e'), inverses Element $(x,x')^{-1} = (x^{-1}, x'^{-1})$

Anwendung: $(\mathbb{R}, +)$ ist eine Abelsche Gruppe. Damit ist auch $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ (bei komponentenweiser Addition) wieder eine Abelsche Gruppe. (...) Auch $(\mathbb{R}^n, +)$ ist Abelsche Gruppe.

Definition 2.3: Ein **Körper** $(K, +, \cdot)$ mit $0 \in K$, $1 \in K$, $0 \neq 1$, ist eine Menge K mit zwei Verknüpfungen, sodass

1) $(K, +)$ ist Abelsche Gruppe mit $e = 0$
2) $(K^*, \cdot)$ ist Abelsche Gruppe mit $e = 1$
3) $x(y+z) = xy + xz$ } Distributivgesetze
4) $(x+y)z = xz + yz$ }

Beispiele: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$

Definition 2.4: Ein **Vektorraum** $(V, +, \cdot, \oplus, \odot)$ über einem Körper K $(K, +, \cdot)$ (K-VR) ist eine (additive) Abelsche Gruppe $(V, \oplus)$, welche mit Skalaren (Elementen aus K) multipliziert werden kann: $\odot: K, V \to V$, $(\alpha, x) \mapsto \alpha \odot x$. Es muss gelten:

1) $(\alpha \cdot \beta) \odot x = \alpha \odot (\beta \odot x)$ (Assoziativität)
2) $\alpha \odot (x \oplus y) = \alpha \odot x \oplus \alpha \odot y$ } (Distributivgesetze)
3) $(\alpha + \beta) \odot x = \alpha \odot x \oplus \beta \odot x$ }
4) $1 \odot x = x$

Die Elemente von V heißen **Vektoren**. Oft ist $K \in \{\mathbb{R}, \mathbb{C}\}$

Beispiele: 1) K^n, für beliebig Körper K, $n \in \mathbb{N}$.

2) K^X, für beliebige Menge $X \neq \emptyset$.

$K^X = \{ f : X \to K \}$ ist VR mit:

$(\alpha f + g)(x) := \alpha f(x) + g(x)$

Die Nullabbildung $0 \in K^X$ ist neutrales Element von $(K^X, +)$

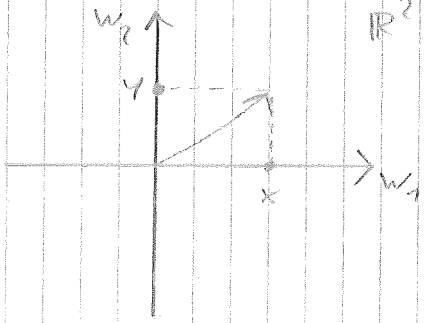
Definition 2.5: Ist V ein K-VR und $W \subseteq V$ mit $0 \in W$.
Dann heißt W Untervektorraum (UVR) von V, wenn $\forall x, y \in W$
$\forall \lambda \in K$ gilt: $x + \lambda y \in W$.
Jeder UVR von V ist auch wieder ein K-VR.

Frage: Was ist korrekt? Für W_1, W_2 UVR von V:

1) $W_1 \cup W_2$ ist UVR von V. ✗

2) $W_1 \cap W_2$ ist UVR von V. ✓

Gegenbeispiel zu 1): $V = \mathbb{R}^2$, $W_1 = \mathbb{R} \times \{0\}$, $W_2 = \{0\} \times \mathbb{R}$



$x \in W_1$, $y \in W_2$

$\Rightarrow x, y \in W_1 \cup W_2$

ABER: $x + y \notin W_1 \cup W_2$

Wie „baut" man (U)VR?

1) **Lemma 2.6:** Sei V ein VR und $M \subseteq V$. Definiere

$\langle M \rangle := \bigcap \{ W : W \subseteq V, W \text{ ist UVR}, W \supseteq M \}$

Dann ist $\langle M \rangle$ ein UVR von V. Es ist der kleinste UVR von V, der die Menge M enthält. $\langle M \rangle$ heißt der von M erzeugte UVR.

Frage: Warum gilt $\langle M \rangle \neq \emptyset$? $[0 \in \langle M \rangle]$

2) **Definition 2.7:** Sei V ein K-VR und $M \subseteq V$. Die Menge alle Linearkombinationen von Vektoren aus M heißt

$$\operatorname{Span} M = \left\{ x \in V : \; x = \sum_{i=1}^{n} \alpha_i x_i \text{ für ein } n \in \mathbb{N} \text{ und } \alpha_i \in K,\ x_i \in M \right\},$$

oder die **lineare Hülle von M**. Man setzt $\operatorname{Span} \emptyset = \{0\}$

Satz 2.8: $\operatorname{Span} M = \langle M \rangle$ die Vektorraumsumme

3) **Definition 2.9:** Seien W_1, W_2 UVR des K-VR V. Definiere

$$W_1 + W_2 := \left\{ z \in V : \exists x \in W_1, y \in W_2 \text{ mit } z = x + y \right\}$$

Dies ist ein UVR von V. Es gilt: $W_1 + W_2 = \operatorname{Span}(W_1 \cup W_2)$

→ Dies löst das „Problem" des Gegenbeispiels zu 1) von gestern.

(Geht mit ungeklärter Logik.)

Definition 2.10: Sei V ein VR, $W \subseteq V$ ein UVR und M eine Menge. M heißt **Erzeugendenmenge von W**, falls $\operatorname{Span} M = W$.

Beispiel: $M = \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$ ist Erzeugendenmenge von $\mathbb{R}^2$.

Menge ↕ Familie

Definition 2.11: Sei V ein K-VR.

1) Die Familie $(x_i)_{i=1,\dots,n}$ heißt **injektiv**, falls die Vektoren $x_1, \dots, x_n$ paarweise verschieden sind, d.h. $x_i \neq x_j \; \forall i \neq j$.

2) Die Familie $(x_i)_{i=1,\dots,n}$ in V heißt **linear unabhängig**, falls aus $\sum_{i=1}^{n} \alpha_i x_i = 0$ folgt, dass alle $\alpha_i = 0$ sind.

3) Eine (unendliche) Teilmenge $M \subseteq V$ heißt **linear unabhängig**, wenn jede endliche injektive Familie in M linear unabhängig ist.

Beispiel: Betrachte $\mathbb{R}$-VR $V = \mathbb{R}^{\mathbb{R}} = \{f: \mathbb{R} \to \mathbb{R}\}$.

1) Darin sind $\sin: \mathbb{R} \to \mathbb{R}$, $\cos: \mathbb{R} \to \mathbb{R}$ linear unabhängig

Vektoren: zu zeigen ist $\alpha \sin + \beta \cos = 0$ (↑ Null-Funktion) d.h.

$\alpha \sin(x) + \beta \cos(x) = 0 \quad \forall x \in \mathbb{R}$.
(↑ reelle Null)

Für $x = 0$ heißt dies $\alpha \cdot 0 + \beta = 0 \Rightarrow \beta = 0$

Für $x = \frac{\pi}{2}$ heißt dies $\alpha + 0 = 0 \Rightarrow \alpha = 0$ ✓

2) Betrachte P, die Menge aller Polynome. Sie sind Vektoren aus $\mathbb{R}^{\mathbb{R}}$. Diese Menge ist linear unabhängig, da z.B.

$p_1(x) = x^2$, $p_2(x) = x^4$, $p_3(x) = x^2 + x^4$ sind mit $\alpha_1 = \alpha_2 = -\alpha_3 = 1$

zum Nullpolynom addiert: $\alpha_1 p_1(x) + \alpha_2 p_2(x) + \alpha_3 p_3(x) = 0$.

3) Betrachte die Menge aller Monome $M = \{p_n: \mathbb{R} \to \mathbb{R},\ x \mapsto x^n$ für $n \in \mathbb{N}_0\}$. $M \subseteq \mathbb{R}^{\mathbb{R}}$ ist linear unabhängige Familie, denn

$\sum_{i=0}^{n} \alpha_i x^i = 0$ für eine beliebige endliche Teilmenge von M

sind wenn die α_i von vornherein Null. Differenziert k-mal:

$0 = \sum_{i=k}^{n} \alpha_i \frac{i!}{(i-k)!} x^{i-k}$, d.h. für $k = n$ gilt: $0 = \alpha_n \cdot n! \cdot 1$

Induktion für $n \mapsto n-1$ führt zu $\alpha_i = 0 \quad \forall i \in \{0, \dots, n\}$.

Lemma 2.12: Es sind äquivalent:

i) $x_1, \dots, x_n$ sind linear unabhängig

ii) Keines der Vektoren x_i ist Linearkombination der anderen

iii) Die Darstellung eines Vektors als Linearkombination der x_i ist eindeutig.

→ Übung: Beweis

Frage: Genügt es für die lineare Unabhängigkeit einer Menge M, dass alle Paare $\{u_1, u_2\} \subseteq M$ linear unabhängig sind? → **Nein!** → Übung

Definition 2.13: Sei V ein K-VR und $M \subseteq V$. M heißt **Basis von V**, falls
- M linear unabhängig,
- $\operatorname{Span} M = V$

Hat man eine Basis M gewählt, dann kann man jeden Vektor $v \in V$ Koordinaten bzgl. dieser Basis bestimmen:
$v = \sum_{x \in M} \alpha_x x$, mit $\alpha_x \in K$. Diese sind eindeutig!

Basisergänzungssatz 2.14: Seien $x_1, \dots, x_n \in V$ linear unabhängig. Weiter seien $y_1, \dots, y_m \in V$ derart, dass
$\operatorname{Span}\{x_1, \dots, x_n, y_1, \dots, y_m\} = V$.
Dann lassen sich $x_1, \dots, x_n$ durch (geeignete) Hinzunahme von Vektoren aus $\{y_1, \dots, y_m\}$ zu einer Basis von V ergänzen.

Basisaustauschsatz 2.15: Seien $\{x_1, \dots, x_n\}$ und $\{y_1, \dots, y_m\}$ Basen von V. Dann gibt es zu jedem $i \in \{1, \dots, n\}$ ein $j \in \{1, \dots, m\}$ sodass aus $\{x_1, \dots, x_n\}$ wieder eine Basis entsteht, wenn man x_i durch y_j ersetzt.
Bemerkung: Es gilt sogar $n = m$, was klar wird aus:

Definition 2.16:
1) Ein K-VR V heißt **endlich erzeugt**, falls es eine endliche Erzeugendenmenge M mit $\operatorname{Span} M = V$ gibt.
2) Für jeden endlich erzeugten VR V besitzen alle Basen die gleiche Anzahl von Elementen. Diese heißt **Dimension** von V.

Beispiel: 1) $\mathbb{R}$-VR $V = \mathbb{R}^n \Rightarrow \dim \mathbb{R} = n$