KAPITEL 3

VEKTORRÄUME

3.1 Gruppen, Ringe und Körper

Definition 3.1.1
Es sei G eine nichtleere Menge. Eine Gruppe ist ein Paar $(G, *)$, wobei $*$ eine Abbildung

$$\begin{array}{rccc} *\colon & G \times G & \to & G \\ & (g_1, g_2) & \mapsto & g_1 * g_2 \end{array}$$

ist, sodass gilt:

1. (*Assoziativität von* $*$)
   Die Abbildung $*$ erfüllt
   $$g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3$$
2. (*Existenz des neutralen Elements*)
   Es gibt ein Element $e \in G$, sodass
   $$g * e = e * g = g \quad \text{für alle } g \in G\,. \tag{3.1.1}$$
3. (*Existenz des inversen Elements*)
   Für alle $g \in G$, gibt es ein $g' \in G$, sodass
   $$g * g' = g' * g = e\,. \tag{3.1.2}$$

Vorlesung 9 - 17.11.2016

Bemerkung 3.1.1

- Eigenschaft 1. erlaubt uns die Klammern wegzulassen, und wir können definieren
  $$g_1 * g_2 * g_3 \quad \text{als} \quad g_1 * (g_2 * g_3) \quad \text{oder als} \quad (g_1 * g_2) * g_3.$$
  Wenn die Abbildung $*$, die wir benutzt haben, eindeutig ist, bezeichnen wir $g_1 * g_2$ mit $g_1 g_2$.
- Wir können das Produkt $g_1 * g_2 * \cdots * g_N$ von mehreren Elementen definieren, z.B. als
  $$g_1 * g_2 * \cdots g_N := (\cdots((g_1 * g_2) * g_3) * \cdots)\,.$$
  (Sehen Sie Bemerkung 2.1.2.)

Lemma 3.1.1

1. *Das neutrale Element ist eindeutig bestimmt, d. h. wenn e_1 und e_2 existieren, die* (3.1.1) *erfüllen, dann $e_1 = e_2$.*

2. *Für alle $g \in G$ ist das inverse Element von g eindeutig bestimmt, d.h. wenn es g' und g'' gibt, die* (3.1.2) *erfüllen, dann $g' = g''$.*

Beweis. 1. Nehmen wir (3.1.1) mit $g = e_2$ und $e = e_1$ und erhalten $e_2 * e_1 = e_2$. Jetzt benutzen wir (3.1.1) mit $g = e_1$ und $e = e_2$ und erhalten $e_2 * e_1 = e_1$, also $e_1 = e_2$.

Um *2.* zu beweisen, können wir dieselbe Überlegung anstellen, die wir in Satz 2.2.1 (a) benutzt haben. Also, gegeben $g \in G$, seien g' und g'' zwei Elemente von G, die (3.1.2) erfüllen. Also

$$g' = g' * e = g' * (g * g'') = (g' * g) * g'' = e * g'' = g''\,.$$

□

Wir bezeichnen das inverse Element von g mit g^{-1}.

Beispiel 3.1.1
Beispiele und Gegenbeispiele von Gruppen:

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ und $(\mathbb{R}, +)$ sind Gruppen, wobei das neutrale Element (der Addition) 0 ist und das inverse Element von a genau $-a$ ist.

- $(\mathbb{N}_0, +)$ ist keine Gruppe. In der Tat ist die Addition assoziativ, hat ein neutrales Element 0, aber wir können keine Inverse von a finden, für alle $a \neq 0$ (wenn $a \in \mathbb{N}$ dann $-a \notin \mathbb{N}$).

- $(\mathbb{Q}, \cdot)$ (also rationale Zahlen mit Multiplikation) ist keine Gruppe. In der Tat ist die Multiplikation assoziativ, hat ein neutrales Element (das in diesem Fall 1 ist), aber nicht jede rationale Zahl hat eine (multiplikative) Inverse: für das Element 0, können wir keine rationale Zahl a finden, sodass $a \cdot 0 = 1$, weil $a \cdot 0 = 0$ für alle $a \in \mathbb{Q}$.

- $(\mathbb{Q} \setminus \{0\}, \cdot)$ ist eine Gruppe. Wie oben, ist die Multiplikation assoziativ und hat das neutrale Element 1. Dazu, für alle $a \in \mathbb{Q} \setminus \{0\}$, die multiplikative Inverse von a ist $\frac{1}{a}$.

- $(M_n(\mathbb{R}), +)$ ist eine Gruppe (Sehen Sie Proposition 2.1.1, Eigenschaften 1. 3. und 4.).

- $(M_n(\mathbb{R}), \cdot)$ ist keine Gruppe. In der Tat erfüllt die Multiplikation Eigenschaften Axiome 1. und 2. einer Gruppe (Sehen Sie Satz 2.1.3 *(a)* 4. und *(b)*), aber nicht alle Matrizen besitzen eine multplikative Inverse! Nur die invertierbaren Matrizen, also...

- $(GL_n(\mathbb{R}), \cdot)$ (die Menge aller invertierbaren Matrizen mit Multiplikation) ist eine Gruppe, die *allgemeine lineare Gruppe*. Bemerken Sie, um diese Behauptung zu beweisen, sollte man auch beweisen, dass das Produkt von zwei invertierbaren Matrizen auch invertierbar ist (nämlich kann man die Multiplikation auf $GL_n(\mathbb{R})$ beschränken; das ist genau Satz 2.2.1 *(c)*). Dazu sollte man beweisen, dass die Inverse einer Matrix in $GL_n(\mathbb{R})$ auch in $GL_n(\mathbb{R})$ ist (Satz 2.2.1 *(b)*).

Bemerkung 3.1.2
Man sollte die Elemente einer Gruppe immer als *invertierbare Abbildungen* sehen. Zum Beispiel haben wir schon bewiesen, dass jedes Element A in $GL_n(\mathbb{R})$ uns eine invertierbare Abbildung $\mathcal{L}_A\colon M_n(\mathbb{R}) \to M_n(\mathbb{R})$ gibt:

$$A \longrightarrow \mathcal{L}_A.$$

Außerdem können wir die Gruppen $(GL_n(\mathbb{R}), \cdot)$ und $(\mathcal{L}_\cdot, \circ)$ identifizieren (als Gruppen!), d. h.

$$I_n \longrightarrow (\mathcal{L}_{I_n} =)\text{Identität}, \quad A \cdot B \longrightarrow (\mathcal{L}_{A\cdot B} =)\mathcal{L}_A \circ \mathcal{L}_B, \quad A^{-1} \longrightarrow (\mathcal{L}_{A^{-1}} =)\mathcal{L}_A^{-1}.$$

Fragen und Vertiefungen 3.1.1
Es sei K entweder $\mathbb{N}, \mathbb{N}_0, \mathbb{Z}, \mathbb{Q}$ oder $\mathbb{R}$ und $M_n(K)$ die Menge aller $n \times n$-Matrizen mit Koeffizienten in K.

- Für welche K ist $(M_n(K), +)$ eine Gruppe?

- Es sei $\mathcal{G}_n(K)$ die Menge aller $n \times n$-Matrizen mit Koeffizienten in K, die invertierbar sind. Also

  $$\mathcal{G}_n(K) = M_n(K) \cap GL_n(\mathbb{R})\,.$$

  Für welche K ist $(\mathcal{G}_n(K), \cdot)$ eine Gruppe?

Definition 3.1.2
Eine Gruppe $(G, *)$ heißt *abelsch* oder *kommutativ*, falls $g*h = h*g$ für alle $g, h \in G$.

Beispiel 3.1.2
$(\mathbb{Z}, +)$, $(M_n(\mathbb{R}), +)$ und $(\mathbb{Q} \setminus \{0\}, \cdot)$ sind abelsche Gruppen. Die allgemeine lineare Gruppe $(GL_n(\mathbb{R}), \cdot)$ ist nicht abelsch, für alle $n > 1$.

Definition 3.1.3
Es sei R eine nichtleere Menge. Ein *Ring* ist ein Tripel $(R, +, \cdot)$, wobei $+$ (die "Addition") und $\cdot$ (die "Multiplikation") zwei Operationen auf R sind, nämlich

$$+: \begin{array}{ccc} R \times R & \longrightarrow & R \\ (a,b) & \mapsto & a+b \end{array} \quad \text{und} \quad \cdot : \begin{array}{ccc} R \times R & \longrightarrow & R \\ (a,b) & \mapsto & a \cdot b \end{array},$$

sodass gilt:

1. $(R, +)$ ist eine *abelsche Gruppe* mit neutralem Element, bezeichnet mit $0 \in R$ und inversem Element von $a \in R$, bezeichnet mit $-a$.

2. Die Multiplikation $\cdot$ ist *assoziativ* (also $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ für alle $a, b, c \in R$) und *besitzt ein neutrales Element*, das wir mit 1 bezeichnen (also $1 \cdot a = a \cdot 1 = a$).

3. Die Multiplikation $\cdot$ ist *distributiv* über die Addition $+$, nämlich

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c),$$

und

$$(b + c) \cdot a = (b \cdot a) + (c \cdot a).$$

Bemerkung 3.1.3
Manche Autoren verzichten auf die Existenz des neutralen Elements 1 in R.

Fragen und Vertiefungen 3.1.2
Beweisen Sie, dass das neutrale Element der Multiplikation eindeutig bestimmt ist.

Definition 3.1.4
Ein Ring $(R, +, \cdot)$ heißt *kommutativ*, falls $a \cdot b = b \cdot a$ für alle $a, b \in R$.

Beispiel 3.1.3

- Die Tripel $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ sind kommutative Ringe.

- Das Tripel $(M_n(\mathbb{R}), +, \cdot)$ ist ein Ring, der für alle $n > 1$ nicht kommutativ ist.

- Der *Polynomring* $R[x]$. Es sei $(R, +, \cdot)$ ein Ring. Wir können wie folgt einen neuen Ring $(R[x], +, \cdot)$ definieren, der Polynomring genannt wird. Per definitionem ist $R[x]$ die Menge aller endlichen Folgen

$$R[x] := \{(a_k)_{k \in \mathbb{N}_0} \mid a_k \in R, \;\; a_i = 0 \text{ für alle bis auf endlich viele } i \in \mathbb{N}_0\}.$$

Also, ein Element von $R[x]$ sieht

$$a = (a_0, a_1, \ldots, a_n, 0, 0, \ldots, 0, \ldots)$$

aus. Äquivalent gesagt, ein Element $a \in R[x]$ kann als

$$a = \sum_{i=0}^{n} a_i x^i$$

dargestellt werden, für ein $n \in \mathbb{N}_0$, das von der Folge a abhängt. Also ist $a \in R[x]$ ein *Polynom* mit Koeffizienten in R und Variable x.

Man kann eine Addition $+$ und Multiplikation $\cdot$ auf $R[x]$ definieren als

$$(a_k)_{k\in\mathbb{N}_0} + (b_k)_{k\in\mathbb{N}_0} := (a_k + b_k)_{k\in\mathbb{N}_0}, \quad (a_k)_{k\in\mathbb{N}_0} \cdot (b_k)_{k\in\mathbb{N}_0} = \left(\sum_{i+j=k} a_i \cdot b_j \right)_{k\in\mathbb{N}_0}.$$

Es ist einfach zu beweisen, dass $(R[x], +, \cdot)$ ein Ring ist, mit $0 = (0, 0, \dots, 0, \dots)$, $1 = (1, 0, 0, \dots, 0, \dots)$ und $-(a_k)_{k\in\mathbb{N}_0} = (-a_k)_{k\in\mathbb{N}_0}$. Wenn $(R, +, \cdot)$ ein kommutativer Ring ist, dann ist auch $(R[x], +, \cdot)$ kommutativ.

Fragen und Vertiefungen 3.1.3
Es sei I eine nichtleere Menge und $\mathcal{A}$ die Menge aller Abbildungen von I nach R, wobei $(R, +, \cdot)$ ein Ring ist. Definieren wir

$$+ : \begin{array}{ccc} \mathcal{A} \times \mathcal{A} & \longrightarrow & \mathcal{A} \\ (f, g) & \mapsto & f + g \end{array} \quad \text{und} \quad \cdot : \begin{array}{ccc} \mathcal{A} \times \mathcal{A} & \longrightarrow & \mathcal{A} \\ (f, g) & \mapsto & f \cdot g \end{array}$$

als $(f + g)(x) := f(x) + g(x)$ und $(f \cdot g)(x) := f(x) \cdot g(x)$ für alle $x \in I$.

Ist $(\mathcal{A}, +, \cdot)$ ein Ring? Wenn Ja, was ist das additive neutrale Element $0 \in \mathcal{A}$? Was ist das multiplikative neutrale Element $1 \in \mathcal{A}$? Und was ist $-f$?

Lemma 3.1.2
Es sei $(R, +, \cdot)$ ein Ring. Dann

$$0 \cdot a = 0 \quad \textit{für alle } a \in R\,.$$

Beweis. Weil 0 das neutrale Element der Gruppe $(R, +)$ ist, und nach dem Distributivgesetz folgt, dass

$$0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a.$$

Es sei $b = 0 \cdot a$ und $-b$ seine (additive) Inverse. Nach der obigen Gleichung $b = b + b$ folgt dass

$$0 = b - b = b + b - b = b + 0 = b$$

und die Behauptung folgt. □

Bemerkung 3.1.4
Es sei $(R, +, \cdot)$ ein Ring. Nehmen wir an, dass $0 = 1$ (also, ist das additive neutrale Element gleich das multiplikative neutrale Element). Dann $R = \{0\}$. In der Tat sei $a \in R$ ein beliebiges Element in R. Dann, nach Lemma 3.1.2 und nach der Voraussetzung $0 = 1$, folgt, dass

$$0 = 0 \cdot a = 1 \cdot a = a\,.$$

Künftig nehmen wir an, dass $0 \neq 1$ im Ring R (also, hat R mindestens zwei Elemente).

Definition 3.1.5
Es sei $a \in R$ ein Element, das eine multiplikative Inverse hat, d. h. es gibt $b \in R$ sodass $a \cdot b = b \cdot a = 1$. Dann heißt a eine *Einheit* des Rings $(R, +, \cdot)$. Die Menge aller Einheiten wird mit R^* bezeichnet.

Bemerkung 3.1.5

- Bemerken Sie, dass wenn $0 \neq 1$ in R, dann $R^* \subsetneq R$, weil 0 keine Einheit ist! (Sehen Sie Lemma 3.1.2). Also $R^* \subseteq R \setminus \{0\}$.
- Wenn $a \in R^*$, dann ist die multiplikative Inverse b eindeutig bestimmt. In der Tat, es seien $b, b' \in R$, sodass $a \cdot b = b \cdot a = 1$ und $a \cdot b' = b' \cdot a = 1$. Dann

  $$b = b \cdot 1 = b \cdot (a \cdot b') = (b \cdot a) \cdot b' = 1 \cdot b' = b'.$$

  Die multiplikative Inverse von a bezeichnen wir mit a^{-1}.

Vorlesung 10 - 21.11.2016

Lemma 3.1.3
Das Paar $(R^*, \cdot)$ ist eine Gruppe.

Beweis. Das Produkt $a \cdot b$ von zwei Einheiten a und b ist noch eine Einheit mit $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$. Also können wir die Multiplikation auf R^* einschränken

$$\cdot \ : R^* \times R^* \to R^*.$$

Weil $R^* \subset R$, ist die Assoziativität von $\cdot$ eine Folgerung der Assoziativität der Multiplikation $\cdot$ im Ring R.

Das neutrale multiplikative Element 1 ist natürlich eine Einheit, weil $1 \cdot 1 = 1$. Also $1^{-1} = 1$, und das inverse Element a^{-1} von a ist eine Einheit, mit $(a^{-1})^{-1} = a$. □

Definition 3.1.6

- Es sei $(R, +, \cdot)$ ein Ring. Wenn R^* genau $R \setminus \{0\}$ ist, nennen wir $(R, +, \cdot)$ einen *Schiefkörper*. Mit anderen Worten, ein Ring $(R, +, \cdot)$ ist ein Schiefkörper, falls $(R \setminus \{0\}, \cdot)$ eine Gruppe ist.
- Ein Schiefkörper $(R, +, \cdot)$, falls R ein kommutativer Ring ist, heißt *Körper*. Mit anderen Worten, ist ein Ring $(R, +, \cdot)$ ein Körper, falls $(R \setminus \{0\}, \cdot)$ eine kommutative Gruppe ist.

  Wir bezeichnen einen Körper mit $\mathbb{K}$.

Beispiel 3.1.4

1. $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring, aber kein Körper, weil $\mathbb{Z}^* = \{1, -1\}$.
2. $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ sind Körper.
3. $(M_n(\mathbb{R}), +, \cdot)$ ist kein Schiefkörper für alle $n > 1$, weil $M_n(\mathbb{R})^* = GL_n(\mathbb{R}) \subsetneq M_n(\mathbb{R}) \setminus \{0\}$ für alle $n > 1$.
4. *Körper der komplexen Zahlen*: Definieren wir die Menge
$$\mathbb{C} := \{x + \mathrm{i}y \mid x, y \in \mathbb{R}\}$$
mit Addition und Multiplikation gegeben durch
$$\begin{aligned}(x_1 + \mathrm{i}y_1) + (x_2 + \mathrm{i}y_2) &:= (x_1 + x_2) + \mathrm{i}(y_1 + y_2),\\ (x_1 + \mathrm{i}y_1) \cdot (x_2 + \mathrm{i}y_2) &:= (x_1x_2 - y_1y_2) + \mathrm{i}(x_1y_2 + x_2y_1).\end{aligned}$$
Also, $\mathrm{i}^2 = -1$, und i heißt *imaginäre Einheit*. Dann ist $(\mathbb{C}, +, \cdot)$ ein Körper. In der Tat ist es einfach nachzuprüfen, dass $(\mathbb{C}, +)$ eine abelsche Gruppe ist, mit $0 = 0 + \mathrm{i}0$ und $-(x + \mathrm{i}y) = -x - \mathrm{i}y$. Ferner ist $(\mathbb{C} \setminus \{0\}, \cdot)$ eine abelsche Gruppe mit
$$(x + \mathrm{i}y)^{-1} = \frac{x}{x^2 + y^2} - \mathrm{i}\frac{y}{x^2 + y^2}\,.$$

Fragen und Vertiefungen 3.1.4

- Es sei $(R[x], +, \cdot)$ der Polynomring in Beispiel 3.1.3, wobei $R = \mathbb{Q}$ oder $\mathbb{R}$. Was ist $R[x]^*$? Ist $R[x]$ ein Schiefkörper?
- Es sei $(\mathcal{A}, +, \cdot)$ wie in Beispiel 3.1.3. Was ist $\mathcal{A}^*$? Ist $\mathcal{A}$ ein Schiefkörper?

3.2 Vektorräume

Definition 3.2.1
Es sei V eine nichtleere Menge. Das Tripel $(V, +, \cdot)$ ist ein *Vektorraum* über einem Körper $\mathbb{K}$ (oder $\mathbb{K}$-Vektorraum), falls wir Operationen $+$ ("*Vektoraddition*") und $\cdot$ ("*Skalarmultiplikation*")

$$+\colon \begin{array}{ccc} V \times V & \to & V \\ (v, w) & \mapsto & v + w \end{array} \qquad \cdot\colon \begin{array}{ccc} \mathbb{K} \times V & \to & V \\ (k, v) & \mapsto & k \cdot v \end{array}$$

definieren können, sodass folgende Eigenschaften gelten:

1. $(V, +)$ ist eine abelsche Gruppe. Wir bezeichnen mit $\mathbf{0}$ das neutrale Element, und mit $-v$ die (additive) Inverse von $v \in V$.

2. Für alle $u, v \in V$ und $k \in \mathbb{K}$ gilt
$$k \cdot (u + v) = k \cdot u + k \cdot v.$$
3. Für alle $h, k \in \mathbb{K}$ und $v \in V$ gilt
$$(h + k) \cdot v = h \cdot v + k \cdot v.$$
4. Für alle $h, k \in \mathbb{K}$ und $v \in V$ gilt
$$(hk) \cdot v = h \cdot (k \cdot v)$$
5. Für alle $v \in V$
$$1 \cdot v = v\,.$$

Die Elemente von V werden *Vektoren* genannt, und diejenigen von $\mathbb{K}$ *Skalare*. Wir bezeichnen $k \cdot v$ mit kv, wobei $k \in \mathbb{K}$ und $v \in V$.

Bemerkung 3.2.1
Bemerken Sie, dass das neutrale Element $\mathbf{0}$ und das inverse Element $-v$ von v eindeutig bestimmt sind, weil $(V, +)$ eine (abelsche) Gruppe ist (Sehen Sie Lemma 3.1.1).

Lemma 3.2.1
Es sei $0 \in \mathbb{K}$, $v \in V$ ein beliebiger Vektor und $k \in \mathbb{K}$. Dann gilt
$$0\,v = \mathbf{0} \tag{3.2.1}$$
$$k\,\mathbf{0} = \mathbf{0} \tag{3.2.2}$$
$$(-1)v = -v \tag{3.2.3}$$
wobei $-1 \in \mathbb{K}$ die additive Inverse des multiplikativen neutralen Element $1 \in \mathbb{K}$ ist.

Beweis. Übung. □

Beispiel 3.2.1

- Es sei $n \in \mathbb{N}$ und $\mathbb{K}^n$ definiert als
$$\mathbb{K}^n := \{(k_1, \ldots, k_n) \mid k_i \in \mathbb{K}\}.$$
Definieren wir zwei Operationen $+$ und $\cdot$ auf $\mathbb{K}^n$ wie folgt
$$\begin{array}{cccc} +: & \mathbb{K}^n \times \mathbb{K}^n & \to & \mathbb{K}^n \\ & ((k_1, \ldots, k_n), (h_1, \ldots, h_n)) & \mapsto & (k_1 + h_1, \ldots, k_n + h_n) \end{array}$$
und
$$\begin{array}{cccc} \cdot\ : & \mathbb{K} \times \mathbb{K}^n & \to & \mathbb{K}^n \\ & (k, (k_1, \ldots, k_n)) & \mapsto & (kk_1, \ldots, kk_n). \end{array}$$
Es ist einfach zu beweisen, dass $\mathbb{K}^n$ ein $\mathbb{K}$-Vektorraum ist.

- Die Menge aller Matrizen $M_{m,n}(\mathbb{K})$ mit Addition $+$ und Skalarmultiplikation $\cdot$ ist ein $\mathbb{K}$-Vektorraum.

- Es sei V ein $\mathbb{K}$-Vektorraum und I eine nichtleere Menge. Es sei $\mathcal{A}(I, V)$ die Menge aller Abbildungen $f\colon I \to V$ mit Addition und Skalarmultiplikation punktweise definiert, also: $(f+g)(x) := f(x) + g(x)$ und $(k \cdot f)(x) := k \cdot f(x)$, für alle $x \in I$ und $k \in \mathbb{K}$. Es ist einfach zu beweisen, dass mit dieser Addition und Skalarmultiplikation $\mathcal{A}(I, V)$ ein $\mathbb{K}$-Vektorraum ist.

- (*Polynomräume*) Die Menge aller Polynome $\mathbb{K}[x]$ mit Koeffizienten in einem Körper $\mathbb{K}$, mit Addition definiert wie in Beispiel 3.1.3 und Skalarmultiplikation, definiert als
$$k \cdot \sum_{i=0}^{n} a_i x^i := \sum_{i=0}^{n} k a_i x^i$$
ist ein $\mathbb{K}$-Vektorraum.

  Es sei $\mathbb{K}[x]_n \subset \mathbb{K}[x]$ die Menge der Polynome, deren Grad durch ein $n \in \mathbb{N}$ nach oben beschränkt ist, d. h. ein beliebiges Element $a \in \mathbb{K}[x]_n$ ist der Gestalt $a = \sum_{i=0}^{n} a_i x^i$ (also, $a_k = 0$ für alle $k > n$). Dann ist $\mathbb{K}[x]_n$, mit Addition und Skalarmultiplikation definiert wie in $\mathbb{K}[x]$, ein $\mathbb{K}$-Vektorraum.

Vorlesung 11 - 24.11.2016

Definition 3.2.2
Es sei V ein $\mathbb{K}$-Vektorraum und $U \subset V$ eine nichtleere Teilmenge. Dann sagen wir, dass U ein *Untervektorraum* (oder *Unterraum*) von V ist, falls

1. Für alle $v, w \in U$ ist $v + w$ in U (U ist abgeschlossen bezüglich Addition).

2. Für alle $k \in \mathbb{K}$ und $v \in U$ ist kv in U (U ist abgeschlossen bezüglich Skalarmultiplikation).

Die obigen Bedingungen sagen uns, dass wir die Addition $+$ und Skalarmultiplikation $\cdot$, die auf V definiert sind, auf U definieren können.

Lemma 3.2.2
Ein Untervektorraum U eines $\mathbb{K}$-Vektorraums $(V, +, \cdot)$, mit Operationen $+$ und $\cdot$, ist selbst ein $\mathbb{K}$-Vektorraum $(U, +, \cdot)$.

Beweis. Zuerst beweisen wir, dass $(U, +)$ eine abelsche Gruppe ist. Die Addition $+$ ist assoziativ und kommutativ, weil sie assoziativ und kommutativ auf V ist.

Das neutrale Element $\mathbf{0} \in V$ ist ein Element von U. In der Tat, nach Voraussetzung (Eigenschaft 2. in Definition 3.2.2) haben wir, dass $0\,v \in U$ für alle $v \in U$, und nach Lemma 3.2.1, $0\,v = \mathbf{0}$.

Falls $v \in U$, dann ist auch $-v$ ein Element von U. In der Tat, nach Lemma 3.2.1, haben wir, dass $-v = (-1)v$, und $(-1)v$ in U sein muss (Eigenschaft 2. in Definition 3.2.2).

Eigenschaften 2., 3., 4., und 5. der Definition 3.2.1 sind erfüllt, weil sie für den Vektorraum $(V, +, \cdot)$ erfüllt sind. □

Beispiel 3.2.2

- Es sei U_i die Teilmenge von $\mathbb{K}^n$ gegeben durch

$$U_i := \{(k_1, \dots, k_n) \in \mathbb{K}^n \mid k_i = 0\}, \text{ für ein } 1 \leq i \leq n.$$

  Also ist U_i ein Untervektorraum von $\mathbb{K}^n$.

- Es sei U_{hk} die Teilmenge aller Matrizen von $M_n(\mathbb{K}) = \{(a_{ij})_{1\leq i,j\leq n}\}$ mit $a_{hk} = 0$ für ein $1 \leq h \leq n$ und ein $1 \leq k \leq n$. Man kann nachprüfen, dass U_{hk} ein Untervektorraum von $M_n(\mathbb{K})$ ist.

- Es sei $y \in I$ und $\mathcal{A}(I, V)_y$ die Teilmenge aller Abbildungen in $\mathcal{A}(I, V)$, sodass $f(y) = \mathbf{0}$. Dann kann man beweisen, dass $\mathcal{A}(I, V)_y$ ein Untervektorraum von $\mathcal{A}(I, V)$ ist.

- Es sei S_n die Teilmenge aller $n \times n$-symmetrischen Matrizen mit Koeffizienten in $\mathbb{K}$, d.h. $S_n = \{A \in M_n(\mathbb{K}) \mid A = A^T\}$. Dann S_n ein Untervektorraum von $M_n(\mathbb{K})$ ist. In der Tat haben wir, dass gegeben $A, B \in S_n$, dann gilt $(A + B)^T = A^T + B^T = A + B$, und gegeben $k \in \mathbb{K}$, $(kA)^T = kA^T = kA$.

- Es sei $\mathbb{K}[x]_n$ die Teilmenge aller Polynome in $\mathbb{K}[x]$, deren Grad höchstens $n \in \mathbb{N}$ ist. Dann ist $\mathbb{K}[x]_n$ ein Untervektorraum von $\mathbb{K}[x]$.

3.2.1 Linearkombinationen und lineare (Un)abhängigkeit

Künftig bezeichnen wir einen $\mathbb{K}$-Vektorraum $(V, +, \cdot)$ nur V, wenn die Addition $+$ und Skalarmultiplikation $\cdot$ in V klar sind.

Definition 3.2.3

- Es sei V ein Vektorraum über $\mathbb{K}$. Dann nennen wir jeden Vektor $v \in V$ der Gestalt

$$v = k_1 v_1 + \cdots + k_n v_n, \quad \text{wobei } k_1, \dots, k_n \in \mathbb{K} \text{ und } v_1, \dots, v_n \in V,$$

  eine *Linearkombination* von $v_1, \dots, v_n$ mit Koeffizienten $k_1, \dots, k_n$.

- Wir bezeichnen die Menge aller Linearkombinationen von $v_1, \dots, v_n$ mit $\mathrm{span}_{\mathbb{K}}\{v_1, \dots, v_n\}$, also

$$\mathrm{span}_{\mathbb{K}}\{v_1, \dots, v_n\} := \{k_1 v_1 + \dots + k_n v_n \mid k_1, \dots, k_n \in \mathbb{K}\}\,,$$

  und wir sagen, dass $\mathrm{span}_{\mathbb{K}}\{v_1, \dots, v_n\}$ der *lineare Spann* von $v_1, \dots, v_n$ ist.

Lemma 3.2.3
Es seien $v_1, \dots, v_n$ Vektoren eines Vektorraumes V über $\mathbb{K}$. Dann ist $U := span_{\mathbb{K}}\{v_1, \dots, v_n\}$ ein Untervektorraum von V.

Beweis. Zuerst bemerken wir, dass U eine nichtleere Menge ist. Um zu beweisen, dass U ein Untervektorraum von V ist, sollen wir beweisen, dass U abgeschlossen unter Addition und Skalarmultiplikation ist. Es seien $v = k_1 v_1 + \dots + k_n v_n$, mit $k_1, \dots, k_n \in \mathbb{K}$, und $w = l_1 v_1 + \cdots l_n v_n$, mit $l_1, \dots, l_n \in \mathbb{K}$, also $v, w \in U$. Weil $(V, +)$ eine abelsche Gruppe ist, erhalten wir, dass

$$\begin{aligned} v + w = k_1 v_1 + \dots + k_n v_n + l_1 v_1 + \cdots l_n v_n = k_1 v_1 + l_1 v_1 + \dots + k_n v_n + l_n v_n = \\ = (k_1 + l_1) v_1 + \dots + (k_n + l_n) v_n \in U\,, \end{aligned} \tag{3.2.4}$$

wobei die letzte Gleichung eine Folgerung von Eigenschaft 3. der Definition 3.2.1 ist. Außerdem haben wir, dass

$$kv = k(k_1 v_1 + \cdots k_n v_n) = (kk_1) v_1 + \dots + (kk_n) v_n \in U\,,$$

wobei die zweite Gleichung eine Folgerung von Eigenschaft 4. der Definition 3.2.1 ist. □

Definition 3.2.4
Es sei V ein $\mathbb{K}$-Vektorraum und $v_1, \dots, v_n$ Vektoren in V. Dann sagen wir, dass die Teilmenge $\{v_1, \dots, v_n\}$ ein *endliches Erzeugendensystem* von V ist, falls

$$\mathrm{span}_{\mathbb{K}}\{v_1, \dots, v_n\} = V\,.$$

Also, für jeden Vektor $v \in V$, existieren $k_1, \dots, k_n \in \mathbb{K}$, sodass v als Linearkombination von $v_1, \dots, v_n$ mit Koeffizienten $k_1, \dots, k_n$ geschrieben werden kann, d.h.

$$v = k_1 v_1 + \dots + k_n v_n\,.$$

Beispiel 3.2.3
Es sei $V = \mathbb{K}^n$, dann ist ein Erzeugendensystem gegeben durch

$$\{e_1 := (1, 0, \dots, 0), e_2 := (0, 1, 0, \dots, 0), \dots, e_n := (0, 0, \dots, 0, 1)\}.$$

In der Tat sei $v = (k_1, \dots, k_n) \in \mathbb{K}^n$, dann $v = k_1 e_1 + k_2 e_2 + \dots + k_n e_n$.

Bemerkung 3.2.2

- Nicht jeder Vektorraum V besitzt ein endliches Erzeugendensystem. Zum Beispiel, es sei $V = \mathbb{K}[x]$. Nehmen wir an, dass $K[x]$ ein endliches Erzeugendensystem $\{p_1, \ldots, p_n\}$ hätte. Wir sollen einen Widerspruch erhalten. Es sei m das Maximum des Grads der Polynome $p_1, \ldots, p_n$. Bemerken wir, dass

  $$\mathrm{Grad}(k_1p_1 + k_2p_2 + \cdots k_np_n) \leq \max\{\mathrm{Grad}(p_1), \mathrm{Grad}(p_2), \ldots, \mathrm{Grad}(p_n)\} = m\,.$$

  Also kann der Polynom x^{m+1} als Linearkombination von $p_1, \ldots, p_n$ nicht geschrieben werden.

- Der Untervektorraum $\mathbb{K}[x]_n$ besitzt ein endliches Erzeugendensystem (Übung).

Definition 3.2.5
Es sei V ein $\mathbb{K}$-Vektorraum. Die Vektoren $v_1, \ldots, v_n$ sind *linear unabhängig*, wenn die Gleichung

$$k_1v_1 + \cdots + k_nv_n = \mathbf{0}$$

nur die triviale Lösung $k_1 = k_2 = \ldots = k_n = 0 \in \mathbb{K}$ hat.

Falls es auch nicht nur triviale Lösungen gibt, nennt man die Vektoren $v_1, \ldots, v_n$ *linear abhängig*.

Beispiel 3.2.4

- Der Null-Vektor $\mathbf{0} \in V$ ist linear abhängig. In der Tat, nach Lemma 3.2.1, haben wir, dass

  $$k\,\mathbf{0} = \mathbf{0} \quad \text{für alle } k \in \mathbb{K}.$$

- Die Vektoren $e_1, \ldots, e_n \in \mathbb{K}^n$ in Beispiel 3.2.3 sind linear unabhängig. In der Tat

  $$k_1e_1 + \cdots + k_ne_n = (k_1, \ldots, k_n) = \mathbf{0} = (0, \ldots, 0)$$

  genau dann, wenn $k_1 = \cdots = k_n = 0$.

- Es seien $v_1 = (1, 1, 2)$, $v_2 = (3, 3, 2)$, $v_3 = (0, 0, 4)$ und $v_4 = (1, 2, 1)$ Vektoren in $\mathbb{R}^3$. Es gilt $-3v_1 + v_2 + v_3 = (0, 0, 0) = \mathbf{0}$, also sind v_1, v_2, v_3 linear abhängig.

  Prüfen Sie nach, dass v_1, v_2 und v_4 linear unabhängig sind (Sie sollten ein lineares Gleichungssystem lösen!).

3.2.2 Basis eines Vektorraums

Definition 3.2.6
Es sei V ein $\mathbb{K}$-Vektorraum. Eine *(endliche) Basis* von V ist ein endliches Erzeugendensystem $\{v_1, \ldots, v_n\} \subset V$ so dass $v_1, \ldots, v_n$ linear unabhängig sind.

Beispiel 3.2.5

- Die Menge $\{e_1, \ldots, e_n\}$ ist eine Basis von $\mathbb{K}^n$.

- Die Menge der Vektoren $v_1 = (1,0)$, $v_2 = (0,1)$ und $v_3 = (1,1)$ ist ein Erzeugendensystem von $\mathbb{R}^2$ (warum?), aber sie sind keine Basis, weil
$$v_1 + v_2 - v_3 = \mathbf{0}\,,$$
also v_1, v_2, v_3 linear abhängig sind.
- Die Vektoren $v_1 = (1,0,0)$ und $v_2 = (0,1,0)$ sind keine Basis von $\mathbb{R}^3$, weil $(0,0,1) \notin \operatorname{span}_{\mathbb{R}}\{v_1, v_2\}$.

Bemerkung 3.2.3
Die Teilmenge $U = \{\mathbf{0}\}$ eines Vektorraums V mit Null-Vektor $\mathbf{0}$ ist selbst ein Vektorraum, weil U ein Untervektorraum von V ist. Bemerken Sie, dass U keine Basis besitzt, weil $\mathbf{0}$ linear abhängig ist.

Wegen Bemerkung 3.2.3 nehmen wir künftig an, dass $V \neq \{\mathbf{0}\}$, sofern nicht anders angegeben.

Fragen und Vertiefungen 3.2.1
Es sei $L_0 := \{(x_1, x_2, x_3) \in \mathbb{R}^3 \mid x_1 + x_2 + x_3 = 0\}$. Ist L_0 ein Untervektorraum von $\mathbb{R}^3$? Wenn Ja, ist $(1,-1,0)$, $(1,0,-1)$ eine Basis von L_0?

Lemma 3.2.4
Es sei $v_1, \ldots, v_n$ eine Basis eines Vektorraums V über $\mathbb{K}$ und $v \in V$. Dann gibt es eindeutige Skalare $k_1, \ldots, k_n \in \mathbb{K}$, sodass $v = k_1v_1 + \cdots + k_nv_n$.

Die Skalare $k_1, \ldots, k_n$ heißen *Koeffizienten* von v bezüglich der Basis $v_1, \ldots, v_n$.

Beweis. Da $v_1, \ldots, v_n$ den Vektorraum erzeugen, existieren $k_1, \ldots, k_n \in \mathbb{K}$, sodass $v = k_1v_1 + \cdots + k_nv_n$. Um zu beweisen, dass $k_1, \ldots, k_n$ eindeutig bestimmt sind, seien $l_1, \ldots, l_n \in \mathbb{K}$, sodass $v = l_1v_1 + \cdots + l_nv_n$. Wie müssen beweisen, dass $k_i = l_i$ für alle $i = 1, \ldots, n$. Nach
$$k_1v_1 + \cdots + k_nv_n = l_1v_1 + \cdots + l_nv_n$$
erhalten wir, dass
$$(k_1 - l_1)v_1 + \cdots + (k_n - l_n)v_n = \mathbf{0}\,.$$
Da $v_1, \ldots, v_n$ linear unabhängig sind, haben wir, dass $k_i - l_i = 0$ für alle $i = 1, \ldots, n$, und die Behauptung folgt. □

Satz 3.2.5
Es sei $V \neq \{\mathbf{0}\}$ ein $\mathbb{K}$-Vektorraum, der ein endliches Erzeugendensystem besitzt. Dann besitzt V eine Basis.

Beweis. Es sei $\{v_1, \ldots, v_n\}$ ein (endliches) Erzeugendensystem. Wenn $v_1, \ldots, v_n$ linear unabhängig sind, dann ist $v_1, \ldots, v_n$ eine Basis von V. Andernfalls, gibt es $(k_1, \ldots, k_n) \neq \mathbf{0} \in \mathbb{K}^n$, sodass

$$k_1 v_1 + \cdots + k_n v_n = \mathbf{0}.$$

Weil $(k_1, \ldots, k_n) \neq \mathbf{0}$ ist, gibt es ein $j \in \{1, \ldots, n\}$, sodass $k_j \neq 0$. Nach der Gleichung oben folgt, dass

$$v_j = -k_j^{-1}(k_1 v_1 + \cdots + k_{j-1} v_{j-1} + k_{j+1} v_{j+1} + \cdots + k_n v_n)\,.$$

Also, $v_j \in \operatorname{span}_{\mathbb{K}}\{v_1, \ldots, v_{j-1}, v_{j+1}, \ldots, v_n\}$ und wir erhalten, dass

$$\operatorname{span}_{\mathbb{K}}\{v_1, \ldots, v_{j-1}, v_{j+1}, \ldots, v_n\} = \operatorname{span}_{\mathbb{K}}\{v_1, \ldots, v_{j-1}, v_j, v_{j+1}, \ldots, v_n\} = V\,.$$

Wenn die Vektoren $v_1, \ldots, v_{j-1}, v_{j+1}, \ldots, v_n$ linear unabhängig sind, dann ist eine Basis von V genau gegeben durch $v_1, \ldots, v_{j-1}, v_{j+1}, \ldots, v_n$. Wenn $v_1, \ldots, v_{j-1}, v_{j+1}, \ldots, v_n$ linear abhängig sind, dann können wir den obigen Schritt wiederholen, und nach endlichen vielen Schritten finden wir eine Basis. □

Vorlesung 12 - 28.11.2016

Fragen und Vertiefungen 3.2.2
Die folgenden Behauptungen sind leicht zu beweisen, und der Beweis ist eine Übung:

1. Der Null-Vektor $\mathbf{0}$ ist der einzige Vektor, der linear abhängig ist.

2. Es seien $v_1, \ldots, v_n$ linear unabhängige Vektoren. Dann ist $v_i \neq \mathbf{0}$ für alle $1 \leq i \leq n$.

3. Es sei $\{w_1, \ldots, w_k\} \subseteq \operatorname{span}_{\mathbb{K}}\{v_1, \ldots, v_n\}$. Dann ist $\operatorname{span}_{\mathbb{K}}\{w_1, \ldots, w_k\} \subseteq \operatorname{span}_{\mathbb{K}}\{v_1, \ldots, v_n\}$.

4. Die folgenden Bedingungen sind äquivalent:
   "$v_1, \ldots, v_n$ sind linear abhängige Vektoren, mit $n \geq 2$", und
   "existiert $j \in \{1, \ldots, n\}$, sodass $v_j \in \operatorname{span}_{\mathbb{K}}\{v_1, \ldots, v_{j-1}, v_{j+1}, \ldots, v_n\}$".

Proposition 3.2.6
Es seien $v_1, \ldots, v_n$ linear unabhängige Vektoren eines Vektorraums V. Dann sind die Vektoren $v_1, \ldots, v_m$ linear unabhängig für alle $1 \leq m \leq n$. Äquivalent gesagt, wenn $v_1, \ldots, v_m$ linear abhängig sind, dann sind auch $v_1, \ldots, v_n$ linear abhängig.

Beweis. Wir beweisen die zweite Behauptung. Wenn $v_1, \dots, v_m$ linear abhängig sind, dann existieren $k_1, \dots, k_m \in \mathbb{K}$ sodass

$$k_1 v_1 + \cdots + k_m v_m = \mathbf{0}$$

wobei nicht alle Koeffizienten k_i Null sind. Es folgt, dass

$$k_1 v_1 + \cdots + k_m v_m + 0\, v_{m+1} + \cdots + 0\, v_n = k_1 v_1 + \cdots + k_m v_m + \mathbf{0} = \mathbf{0}$$

wobei nicht alle Koeffizienten der obigen Linearkombination null sind. Es folgt, dass $v_1, \dots, v_n$ linear abhängig sind. □

Das Ziel der nächsten Sätze ist zu beweisen, dass für jeden Vektorraum das Konzept von Dimension definiert werden kann. Wir beginnen mit folgenden:

Satz 3.2.7
Es sei $v_1, \dots, v_n$ ein endliches Erzeugendensystem von einem Vektorraum V und $w_1, \dots, w_m$ Vektoren in V. Falls $m > n$, sind $w_1, \dots, w_m$ linear abhängig.

Beweis. Es seien $w_1, \dots, w_n$ die ersten n Vektoren von $w_1, \dots, w_m$. Wenn $w_1, \dots, w_n$ linear abhängig sind, dann nach Proposition 3.2.6 sind auch $w_1, \dots, w_m$ linear abhängig und wir können den Beweis schließen. Also nehmen wir an, dass $w_1, \dots, w_n$ linear unabhängig sind. Um die Behauptung zu beweisen, genügt es zu beweisen, dass $\operatorname{span}_{\mathbb{K}}\{w_1, \dots, w_n\} = V$. In der Tat, in diesem Fall haben wir

$$w_m = \alpha_1 w_1 + \cdots + \alpha_n w_n\,,$$

und die Gleichung $\alpha_1 w_1 + \cdots + \alpha_n w_n + 0 w_{n+1} + \cdots + 0 w_{m-1} - w_m = \mathbf{0}$ hat eine nicht triviale Lösung (der Koeffizient von w_m ist gleich -1), und $w_1, \dots, w_m$ sind linear abhängig. Im Folgenden beweisen wir, dass

$$\operatorname{span}_{\mathbb{K}}\{w_1, \dots, w_n\} = V. \tag{3.2.5}$$

Nach Voraussetzung $\operatorname{span}_{\mathbb{K}}\{v_1, \dots, v_n\} = V$, also existieren $k_1, \dots, k_n$, sodass

$$w_1 = k_1 v_1 + \cdots + k_n v_n\,.$$

Weil wir angenommen haben, dass $w_1, \dots, w_n$ linear unabhängig sind, $w_1 \neq \mathbf{0}$ (Fragen und Vertiefungen 3.2.2, 2.), können nicht alle Koeffizienten $k_1, \dots, k_n$ Null sein. Nehmen wir an, dass $k_1 \neq 0$ und erhalten

$$v_1 = k_1^{-1}(w_1 - k_2 v_2 - \cdots - k_n v_n).$$

Deshalb $v_1 \in \operatorname{span}_{\mathbb{K}}\{w_1, v_2, \dots, v_n\}$. Weil $v_2, \dots, v_n \in \operatorname{span}_{\mathbb{K}}\{w_1, v_2, \dots, v_n\}$, erhalten wir, dass $\operatorname{span}_{\mathbb{K}}\{v_1, v_2, \dots, v_n\} \subseteq \operatorname{span}_{\mathbb{K}}\{w_1, v_2, \dots, v_n\}$. Nach Voraussetzung $\operatorname{span}_{\mathbb{K}}\{v_1, v_2, \dots, v_n\} = V$ (Fragen und Vertiefungen 3.2.2, 3.), also

$$\operatorname{span}_{\mathbb{K}}\{w_1, v_2, \dots, v_n\} = V\,. \tag{3.2.6}$$

Jetzt beweisen wir, dass

$$\mathrm{span}_{\mathbb{K}}\{w_1, \ldots, w_s, v_{s+1}, \ldots, v_n\} = V \ \text{ für ein } \ 1 \leq s \leq n-1 \implies \mathrm{span}_{\mathbb{K}}\{w_1, \ldots, w_s, w_{s+1}, v_{s+2}, \ldots, v_n\} = V, \tag{3.2.7}$$

und die Behauptung (3.2.5) folgt nach Induktion; (3.2.6) ist genau der Induktionsanfang und (3.2.7) der Induktionsschritt.

Angenommen, dass $\mathrm{span}_{\mathbb{K}}\{w_1, \ldots, w_s, v_{s+1}, \ldots, v_n\} = V$ für ein $1 \leq s \leq n-1$, existieren $h_1, \ldots, h_s, h_{s+1}, \ldots, h_n$ sodass

$$w_{s+1} = h_1 w_1 + \cdots + h_s w_s + h_{s+1} v_{s+1} + h_{s+2} v_{s+2} + \cdots + h_n v_n \,.$$

Weil $w_1, \ldots, w_n$ nach Voraussetzung linear unabhängig sind, müssen, nach Proposition 3.2.6, die Vektoren $w_1, \ldots, w_s, w_{s+1}$ linear unabhängig sein. Also muss einer der Koeffizienten $h_{s+1}, h_{s+2}, \ldots, h_n$ ungleich Null sein (sonst hätten wir $1 \cdot w_{s+1} - (h_1 w_1 + \cdots + h_s w_s) = \mathbf{0}$). Wir können annehmen, dass $h_{s+1} \neq 0$, und erhalten, dass

$$v_{s+1} = h_{s+1}^{-1}(w_{s+1} - h_1 w_1 - \cdots - h_s w_s - h_{s+2} v_{s+2} - \cdots - h_n v_n) \,.$$

Deshalb erhalten wir, dass $v_{s+1} \in \mathrm{span}_{\mathbb{K}}\{w_1, \ldots, w_s, w_{s+1}, v_{s+2}, \ldots, v_n\}$. Da jeder Vektor in $\{w_1, \ldots, w_s, v_{s+1}, \ldots, v_n\}$ ein Element in $\mathrm{span}_{\mathbb{K}}\{w_1, \ldots, w_s, w_{s+1}, v_{s+2}, \ldots, v_n\}$ ist, erhalten wir, dass

$$V = \mathrm{span}_{\mathbb{K}}\{w_1, \ldots, w_s, v_{s+1}, \ldots, v_n\} \subseteq \mathrm{span}_{\mathbb{K}}\{w_1, \ldots, w_s, w_{s+1}, v_{s+2}, \ldots, v_n\}$$

und (3.2.7) folgt. □

Als Folgerung erhalten wir:

Korollar 3.2.8
Es seien $\{v_1, \ldots, v_n\}$ und $\{w_1, \ldots, w_m\}$ zwei Basen eines Vektorraums V. Dann $n = m$.

Beweis. Weil $\{v_1, \ldots, v_n\}$ eine Basis ist, erzeugen die Vektoren $v_1, \ldots, v_n$ den Vektorraum V. Weil $\{w_1, \ldots, w_m\}$ eine Basis ist, sind die Vektoren $w_1, \ldots, w_m$ linear unabhängig. Also impliziert Satz 3.2.7, dass $m \leq n$. Mit derselben Methode können wir beweisen, dass $n \leq m$, und die Behauptung folgt. □

Vorlesung 13 - 01.12.2016

Dieses Korollar erlaubt uns, folgende Definition zu geben:

Definition 3.2.7
- Es sei V ein Vektorraum, der eine endliche Basis $\{v_1, \dots, v_n\}$ besitzt. Dann nennen wir n die Dimension von V und bezeichnen sie mit $\dim_{\mathbb{K}}(V)$.
- Es sei $V = \{\mathbf{0}\}$, dann setzen wir $\dim_{\mathbb{K}}(V) = 0$.
- Falls $V \neq \{\mathbf{0}\}$ keine endliche Basis besitzt, setzen wir $\dim_{\mathbb{K}}(V) = \infty$.

Beispiel 3.2.6
- Es sei $\mathbb{K}^n = \{(k_1, \dots, k_n) \mid k_i \in \mathbb{K}\}$ und $e_1, \dots, e_n$ wie in Beispiel 3.2.3. Weil $\{e_1, \dots, e_n\}$ eine Basis von $\mathbb{K}^n$ ist, erhalten wir, dass $\dim_{\mathbb{K}}(\mathbb{K}^n) = n$. Bemerken Sie, dass

$$(k_1, \dots, k_n) = k_1 e_1 + \dots + k_n e_n \,.$$

Deshalb sind die Koeffizienten des Vektors $(k_1, \dots, k_n)$ bezüglich der Basis $\{e_1, \dots, e_n\}$ genau die Komponenten $k_1, \dots, k_n$. Wir nennen die Basis $\{e_1, \dots, e_n\}$ die *kanonische Basis* von $\mathbb{K}^n$.

- Der $\mathbb{K}$-Vektorraum aller Matrizen $M_{m,n}(\mathbb{K})$ hat Dimension $m \cdot n$. In der Tat ist eine Basis gegeben durch die Matrizen $\{\Delta_{ij}\}_{\substack{1 \le i \le m \\ 1 \le j \le n}}$, wobei der Koeffizient a_{hk} von Δ_{ij} ist gleich 1 falls $h = i$ und $k = j$, und Null falls $h \neq i$ oder $k \neq j$, und

$$M_{m,n}(\mathbb{K}) \ni A = (a_{ij})_{\substack{1 \le i \le m \\ 1 \le j \le n}} = \sum_{\substack{1 \le i \le m \\ 1 \le j \le n}} a_{ij} \Delta_{ij} \,.$$

- Der Vektorraum $\mathbb{K}[x]$ besitzt keine endliche Basis (Sehen Sie Bemerkung 3.2.2), also $\dim_{\mathbb{K}}(\mathbb{K}[x]) = \infty$. Der (Unter)Vektorraum $\mathbb{K}[x]_n$ der Polynome, deren Grad höchstens $n \in \mathbb{N}$ ist, hat Dimension n (Übung).

Proposition 3.2.9
Es sei V ein Vektorraum, mit $\dim_{\mathbb{K}}(V) = n$. Wenn $v_1, \dots, v_n \in V$ linear unabhängig sind, dann ist $\{v_1, \dots, v_n\}$ eine Basis von V.

Beweis. Wir sollen nur beweisen, dass $\operatorname{span}_{\mathbb{K}}\{v_1, \dots, v_n\} = V$. Es sei $v \in V$ ein beliebiger Vektor. Nach dem Satz 3.2.7 und nach $\dim_{\mathbb{K}}(V) = n$ haben wir, dass $v_1, \dots, v_n, v$ linear abhängig sind. Also existieren $k_1, \dots, k_n, k \in \mathbb{K}$, nicht alle Null, sodass

$$k_1 v_1 + \dots + k_n v_n + kv = \mathbf{0} \,.$$

Weil nach Voraussetzung $v_1, \dots, v_n$ linear unabhängig sind, muss der Koeffizient k nicht Null sein, also

$$v = k^{-1}(-k_1 v_1 - \dots - k_n v_n) \in \operatorname{span}_{\mathbb{K}}\{v_1, \dots, v_n\} \,.$$

Weil v beliebig ist, erhalten wir, dass $\operatorname{span}_{\mathbb{K}}\{v_1, \dots, v_n\} = V$. □

Proposition 3.2.10 (**Basisergänzung**)
Es sei V ein Vektorraum, mit $\dim_{\mathbb{K}}(V) = n$. Wenn $v_1, \ldots, v_k \in V$ linear unabhängig sind, dann existieren $v_{k+1}, \ldots, v_n \in V$, sodass $\{v_1, \ldots, v_k, v_{k+1}, \ldots, v_n\}$ eine Basis ist.

Beweis. Nach dem Satz 3.2.7 und nach der Voraussetzung $\dim_{\mathbb{K}}(V) = n$ haben wir, dass $k \leq n$. Wenn $k = n$, folgt die Behauptung nach Proposition 3.2.9.

Nehmen wir an, dass $k < n$. Bemerken wir, dass $\{v_1, \ldots, v_k\}$ kein Erzeugendensystem sein kann, sonst würden wir eine Basis mit $k < n$ Elementen erhalten und das ist ein Widerspruch (Sehen Sie Korollar 3.2.8). Deshalb können wir einen Vektor $v_{k+1} \in V$ finden, der nicht in $\operatorname{span}_{\mathbb{K}}\{v_1, \ldots, v_k\}$ ist. Wir wollen beweisen, dass $v_1, \ldots, v_k, v_{k+1}$ linear unabhängig sind. Nehmen wir

$$h_1 v_1 + \cdots + h_k v_k + h_{k+1} v_{k+1} = \mathbf{0}\,.$$

Bemerken wir, dass $h_{k+1} = 0$. In der Tat, falls $h_{k+1} \neq 0$, dann könnten wir v_{k+1} als Linearkombination von $v_1, \ldots, v_k$ schreiben:

$$v_{k+1} = h_{k+1}^{-1}(-h_1 v_1 - \cdots - h_k v_k)$$

und würden einen Widerspruch erhalten, weil $v_{k+1} \notin \operatorname{span}_{\mathbb{K}}\{v_1, \ldots, v_k\}$. Weil $h_{k+1} = 0$, müssen wir $h_1 = \ldots = h_k = 0$ haben, weil $v_1, \ldots, v_k$ linear unabhängig sind. Also haben wir bewiesen, dass $v_1, \ldots, v_k, v_{k+1}$ linear unabhängig sind. Falls $k + 1 = n$, nach Proposition 3.2.9 haben wir, dass $\{v_1, \ldots, v_k, v_{k+1}\}$ eine Basis von V ist. Falls $k + 1 < n$ können wir den obigen Schritt wiederholen und einen Vektor $v_{k+2} \notin \operatorname{span}_{\mathbb{K}}\{v_1, \ldots, v_{k+1}\}$ finden, sodass $v_1, \ldots, v_{k+1}, v_{k+2}$ linear unabhängig sind. Falls $k + 2 = n$, Proposition 3.2.9 impliziert, dass $\{v_1, \ldots, v_{k+2}\}$ eine Basis von V ist. Andernfalls wiederholen wir den obigen Schritt $(n - k)$-Male, und finden n linear unabhängige Vektoren $v_1, \ldots, v_n$ die, nach Proposition 3.2.9, eine Basis sind.

□

3.2.3 Untervektorräume und Basen

Eine weitere Folgerung von Satz 3.2.7 ist

Korollar 3.2.11
Es sei V ein $\mathbb{K}$-Vektorraum, mit $\dim_{\mathbb{K}}(V) = n$. *Dann* $\dim_{\mathbb{K}}(U) \leq n$, *für jeden Untervektorraum $U \subseteq V$.*

Beweis. Zuerst nehmen wir an, dass $\dim_{\mathbb{K}}(U) < \infty$, und es sei $\{u_1, \ldots, u_m\}$ eine Basis von U. Weil V ein Erzeugendensystem mit n Elementen besitzt und weil $u_1, \ldots, u_m$ linear unabhängig sind, impliziert Satz 3.2.7, dass $m = \dim_{\mathbb{K}}(U) \leq n$. Was wir noch beweisen sollten ist, dass $\dim_{\mathbb{K}}(U) < \infty$. Wenn nicht, seien $u_1, \ldots, u_m$ linear unabhängige Vektoren. Unsere Voraussetzung ($\dim_{\mathbb{K}}(U) = \infty$) impliziert, dass $\text{span}_{\mathbb{K}}\{u_1, \ldots, u_m\} \neq U$. Also können wir einen Vektor $u_{m+1} \in U$ finden, sodass $u_{m+1} \notin \text{span}_{\mathbb{K}}\{u_1, \ldots, u_m\}$ und sodass $u_1, \ldots, u_m, u_{m+1}$ linear unabhängig sind (Sehen Sie den Beweis der Proposition 3.2.10). Durch Wiederholung dieses Verfahrens könnten wir N linear unabhängige Vektoren in $U \subset V$ finden, für alle $N \in \mathbb{N}$, und Satz 3.2.7 sagt uns, dass das ein Widerspruch ist. □

Es seien U und W zwei Untervektorräume eines Vektorraums V. Nach der Definition folgt, dass der Schnitt $U \cap W$ auch ein Vektorraum ist (Sehen Sie Definition 3.2.2). Bemerken Sie, dass der Schnitt immer eine nicht-leere Menge ist (weil $\mathbf{0} \in U \cap V$). In Allgemeinen, gegeben sei eine Familie $\{U_i\}_{i \in I}$ von Untervektorräumen von V, der Schnitt $\cap_{i \in I} U_i$ ist immer eine nicht-leere Menge und ein Untervektorraum von V.

Die Vereinigung $U \cup W$ von zwei (oder mehreren) Untervektorräumen U und W ist nicht immer ein Untervektorraum. In der Tat, wenn $u \in U$ und $w \in W$, ist die Summe $u+w$ nicht unbedingt in $U \cup W$. Zum Beispiel, es seien $u \neq \mathbf{0}$ und $w \neq \mathbf{0}$ Vektoren in $\mathbb{R}^3$, mit $w \neq \lambda u$ für alle $\lambda \in \mathbb{R}$ (also, u und w sind nicht proportional). Definieren wir $U := \text{span}_{\mathbb{R}}\{u\} = \{k\,u \mid k \in \mathbb{R}\}$; also ist U der Untervektorraum aller Vektoren proportional zu u. Ähnlich sei $W := \text{span}_{\mathbb{R}}\{w\} = \{k\,w \mid k \in \mathbb{R}\}$, der Vektorraum aller Vektoren proportional zu w. Weil u nicht proportional zu w ist folgt, dass $u + w$ nicht proportional ist, weder zu u noch zu w, also $u + w \notin U \cup W$.

Vorlesung 14 - 05.12.2016

Fragen und Vertiefungen 3.2.3
Es seien U und W zwei Untervektorräume eines Vektorraums V. Welche Bedingungen über U und W implizieren, dass $U \cup W$ ein Untervektorraum ist?

Gegeben zwei Untervektorräume U und W, definieren wir

$$U + W := \{u + w \mid u \in U \;\text{ und }\; w \in W\}\,.$$

Bemerken Sie, dass für alle $u_1, u_2 \in U$, $w_1, w_2 \in W$ und $k \in \mathbb{K}$ wir haben

$$(u_1 + w_1) + (u_2 + w_2) = (u_1 + u_2) + (w_1 + w_2) \in U + W$$

$$k(u_1 + w_1) = ku_1 + kw_1 \in U + W\,,$$

also ist $U+W$ ein Untervektorraum. Wir nennen $U+W$ die *Summe zweier Untervektorräume* U und W. Bemerken Sie, dass $U \cup W \subseteq U+W$, weil $U \ni u = u+\mathbf{0} \in U+W$ und $W \ni w = \mathbf{0} + w \in U + W$.

Falls $U \cap W = \{\mathbf{0}\}$, nennen wir $U + W$ die *direkte Summe* von U und W und wir bezeichnen diese Summe mit $U \oplus W$. Wir haben das folgende:

Lemma 3.2.12
Zu jedem $v \in U \oplus W$, gibt es eindeutig bestimmte Vektoren $u \in U$ und $w \in W$ mit $v = u + w$.

Beweis. Es seien $u_1, u_2 \in U$ und $w_1, w_2 \in W$, sodass $v = u_1 + w_1 = u_2 + w_2$. Also $u_1 - u_2 = w_2 - w_1 \in U \cap W$. Weil dieser Schnitt gleich $\mathbf{0}$ ist, erhalten wir, dass $u_1 = u_2$ und $w_1 = w_2$. $\square$

Es seien U und W zwei $\mathbb{K}$-Vektorräume. Das *kartesische Produkt*

$$U \times W := \{(u, w) \mid u \in U \text{ und } w \in W\}$$

von U und W ist ein $\mathbb{K}$-Vektorraum mit Addition und Skalarmultiplikation definiert wie folgt:

$$\begin{aligned} &(u_1, w_1) + (u_2 + w_2) := (u_1 + u_2, w_1 + w_2) \\ &k(u_1, w_1) := (ku_1, kw_1) \end{aligned} \tag{3.2.8}$$

für alle $(u_1, w_1), (u_2, w_2) \in U \times W$ und $k \in \mathbb{K}$. Der Nullvektor ist natürlich $(\mathbf{0}_U, \mathbf{0}_W)$, wobei $\mathbf{0}_U$ der Nullvektor in U und $\mathbf{0}_W$ der Nullvektor in W ist.

Es seien $U' := \{(u, \mathbf{0}_W) \mid u \in U\} \subseteq U \times W$ und $W' := \{(\mathbf{0}_U, w) \mid w \in W\} \subseteq U \times W$. Weil jedes $(u, w) \in U \times W$ gleich $(u, \mathbf{0}_W) + (\mathbf{0}_U, w)$ ist und weil $U' \cap W' = \{(\mathbf{0}_U, \mathbf{0}_W)\}$ erhalten wir, dass

$$U \times W = U' \oplus W' .$$

Satz 3.2.13
Es seien U und W zwei Untervektorräume eines Vektorraums V, mit $\dim_{\mathbb{K}}(U) < \infty$ und $\dim_{\mathbb{K}}(W) < \infty$. Dann haben die Untervektorräume $U \cap W$ und $U + W$ endliche Dimensionen, und die folgende Formel gilt:

$$\dim_{\mathbb{K}}(U) + \dim_{\mathbb{K}}(W) = \dim_{\mathbb{K}}(U + W) + \dim_{\mathbb{K}}(U \cap W) . \tag{3.2.9}$$

Falls $U + W$ die direkte Summe von U und W ist, gilt

$$\dim_{\mathbb{K}}(U) + \dim_{\mathbb{K}}(W) = \dim_{\mathbb{K}}(U + W). \tag{3.2.10}$$

Formel (3.2.9) heißt die *Grassmann Formel.*

Beweis. Zuerst bemerken wir, dass die Dimension von $U \cap W$ endlich ist, weil $U \cap W$ ein Untervektorraum von U ist, und die Behauptung folgt nach der Voraussetzung $\dim_{\mathbb{K}}(U) < \infty$ und Korollar 3.2.11. Es sei $m := \dim_{\mathbb{K}}(U \cap W)$. Wir haben zwei Fälle: $m = 0$ und $m \geq 1$. Der erste Fall ist eine Übung. Wir beweisen den zweiten Fall $m \geq 1$.

Es sei $\{b_1, \dots, b_m\}$ eine Basis von $U \cap W$. Nach Proposition 3.2.10 existieren $u_1, \dots, u_s \in U$ und $w_1, \dots, w_t \in W$, sodass $\{b_1, \dots, b_m, u_1, \dots, u_s\}$ eine Basis von U und $\{b_1, \dots, b_m, w_1, \dots, w_t\}$ eine Basis von W ist. Wir bemerken, dass

$$\dim_{\mathbb{K}}(U) + \dim_{\mathbb{K}}(W) - \dim_{\mathbb{K}}(U \cap W) = m + s + t .$$

Also, um (3.2.9) zu beweisen, genügt es zu beweisen, dass $\{b_1, \ldots, b_m, u_1, \ldots, u_s, w_1, \ldots, w_t\}$ eine Basis von $U + W$ ist. Insbesondere erhalten wir, dass $\dim_{\mathbb{K}}(U + W) < \infty$.

Es sei $u + w \in U + W$. Dann existieren Koeffizienten $\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_s, \alpha'_1, \ldots, \alpha'_m, \gamma_1, \ldots, \gamma_t \in \mathbb{K}$, sodass

$$\begin{aligned} u = \quad & \alpha_1 b_1 + \cdots + \alpha_m b_m + \beta_1 u_1 + \cdots + \beta_s u_s \quad \text{und} \\ w = \quad & \alpha'_1 b_1 + \cdots + \alpha'_m b_m + \gamma_1 w_1 + \cdots + \gamma_t w_t, \quad \text{also} \\ u + w = \quad & (\alpha_1 + \alpha'_1) b_1 + \cdots + (\alpha_m + \alpha'_m) b_m + \beta_1 u_1 + \cdots + \beta_s u_s + \\ & \gamma_1 w_1 + \cdots + \gamma_t w_t\,. \end{aligned}$$

Wir können schließen, dass $\operatorname{span}_{\mathbb{K}}\{b_1, \ldots, b_m, u_1, \ldots, u_s, w_1, \ldots, w_t\} = U + W$. Was wir noch beweisen sollen ist, dass die Vektoren $b_1, \ldots, b_m, u_1, \ldots, u_s, w_1, \ldots, w_t$ linear unabhängig sind.

Nehmen wir die Linearkombination

$$\alpha_1 b_1 + \cdots + \alpha_m b_m + \beta_1 u_1 + \cdots + \beta_s u_s + \gamma_1 w_1 + \cdots + \gamma_t w_t = \mathbf{0}\,, \tag{3.2.11}$$

also

$$\overbrace{\gamma_1 w_1 + \cdots + \gamma_t w_t}^{\in W} = -\left(\overbrace{\alpha_1 b_1 + \cdots + \alpha_m b_m}^{\in U \cap W} + \overbrace{\beta_1 u_1 + \cdots + \beta_s u_s}^{\in U}\right)$$

und die zweite Seite muss in $U \cap W$ sein. Weil $\{b_1, \ldots, b_m\}$ eine Basis von $U \cap W$ ist, existieren $\delta_1, \ldots, \delta_m \in \mathbb{K}$, sodass

$$\alpha_1 b_1 + \cdots + \alpha_m b_m + \beta_1 u_1 + \cdots + \beta_s u_s = \delta_1 b_1 + \cdots + \delta_m b_m$$

also

$$(\alpha_1 - \delta_1) b_1 + \cdots + (\alpha_m - \delta_m) b_m + \beta_1 u_1 + \cdots + \beta_s u_s = \mathbf{0}\,.$$

Weil $\{b_1, \ldots, b_m, u_1, \ldots, u_s\}$ eine Basis von U ist, erhalten wir, dass $\alpha_i = \delta_i$ für alle $i = 1, \ldots, m$ und $\beta_1 = \ldots = \beta_s = 0$. Nach (3.2.11) haben wir, dass

$$\alpha_1 b_1 + \cdots + \alpha_m b_m + \gamma_1 w_1 + \cdots + \gamma_t w_t = \mathbf{0}\,.$$

Weil $\{b_1, \ldots, b_m, w_1, \ldots, w_t\}$ eine Basis von W ist, erhalten wir, dass $\alpha_i = 0$ für alle $i = 1, \ldots, m$ und $\gamma_j = 0$ für alle $j = 1, \ldots, t$. Also können wir schließen, dass alle Koeffizienten in (3.2.11) Null sind, deshalb ist $\{b_1, \ldots, b_m, u_1, \ldots, u_s, w_1, \ldots, w_t\}$ eine Basis von $U + W$.

□

Beispiel 3.2.7
Es sei $V = \mathbb{R}^3$, und $U = \{(x, y, z) \in \mathbb{R}^3 \mid y = 0\}$ und $W = \{(x, y, z) \in \mathbb{R}^3) \mid z = 0\}$. Weil jede (x, y, z) gleich $(x, 0, z) + (0, y, 0)$ ist, erhalten wir, dass $U + W = \mathbb{R}^3$. Man kann nachprüfen, dass $\dim_{\mathbb{R}}(U) = \dim_{\mathbb{R}}(W) = 2$ und $\dim_{\mathbb{R}}(U \cap W) = 1$, weil $U \cap W = \{(x, 0, 0) \mid x \in \mathbb{R}\}$. Also ist $\mathbb{R}^3$ keine direkte Summe von U und W, und (3.2.9) gilt.