

# 1 Grundlagen

## 1.1 Mengenlehre

### 1.1.1 Erste Definitionen und Beispiele

Die Mengenlehre ist einen nicht trivialen Teil der Mathematik. Wir werden Mengen nicht richtig definieren.

Wir werden mit den folgenden vagen (aber für unseren Zwecke ausreichenden) Definition arbeiten.

**Definition 1.1.1** Eine **Menge**  $M$  ist eine Zusammenfassung von verschiedenen Objekte (die man **Elemente** nennt) zu einem neuen Objekt.

**Axiom 1.1.2 (Extensionalitätsaxiom)** Zwei Mengen  $M$  und  $N$  sind genau dann **gleich**, wenn sie die selbe Elementen enthalten.

**Notation 1.1.3** Wir werden die folgende Symbole benutzen.

$\{ \}$	die Mengenklammern:	z.b. $M = \{0; 1; 2\}$ .
$\in$	ist Element von:	z.b. $1 \in \{0; 1; 2\}$ .
$\notin$	ist nicht Element von:	z.b. $3 \notin \{0; 1; 2\}$ .

$\forall$	alle:	z.b. $\forall n \in \mathbb{N}$ es gilt $n \geq 0$ .
$\exists$	es gibt:	z.b. $\exists n \in \mathbb{N}$ so dass $n \geq 5$ .
$\Rightarrow$	dann:	z.b. $n \geq 1 \Rightarrow n \geq 0$ .

**Bemerkung 1.1.4** Mit Symbole:  $M = N$  genau dann, wenn

$$x \in M \Rightarrow x \in N \text{ und } x \in N \Rightarrow x \in M.$$

**Definition 1.1.5** Sei  $M$  eine Menge.

1. Eine **Teilmenge**  $N$  von einer Menge  $M$  ist eine Menge so dass alle elemente in  $N$  auch in  $M$  enthalten sind. Mit Symbole:  $x \in N \Rightarrow x \in M$ .
2. Eine **echte** Teilmenge  $N$  von einer Menge  $M$  ist eine Teilmenge die nicht gleich  $M$  ist.

**Notation 1.1.6** Hier sind weitere Symbole.

$\subseteq, \subset$  ist Teilmenge von: z.b.  $\{0; 1; 2\} \subseteq \{0; 1; 2\}$  oder  $\mathbb{N} \subseteq \mathbb{Z}$ .  
 $\subsetneq$  ist eine echte Teilmenge von: z.b.  $\{1; 2\} \subsetneq \{0; 1; 2\}$ .

**Bemerkung 1.1.7** Es gilt  $\{0; 1; 2\} = \{2; 0; 1\} = \{0; 0; 1; 2; 2; 2\}$ .

## 1.1.2 Konstruktion in der Mengenlehre

### Aussonderungsaxiom

**Axiom 1.1.8 (Aussonderungsaxiom)** Zu jeder Menge  $M$  und jeder Eigenschaft  $P$  gibt es eine Teilmenge  $N$  von  $M$ , die gerade aus den Elementen von  $M$  mit dieser Eigenschaft besteht.

**Notation 1.1.9** Weitere Symbole.

$|$  mit der Eigenschaft: z.b.  $\{0; 1; 2\} = \{n \in \mathbb{N} \mid n \leq 2\}$ .

**Satz 1.1.10** Es gibt eine Menge, die keine Elemente enthält: Man nennt diese Menge die **leere Menge** und bezeichnet sie mit  $\emptyset$ .  $\square$

*Beweis.* Wir behaupten, dass es mindestens eine Menge  $M$  gibt. Dann kann man, dank dem Aussonderungsaxiom die Menge

$$\emptyset = \{x \in M \mid x \neq x\}$$

definieren. Die Menge  $\emptyset$  enthält keine Elemente.  $\blacksquare$

**Bemerkung 1.1.11** Die leere Menge ist in jede Menge enthalten: für jede Menge  $M$  gilt  $\emptyset \subset M$ .

**Satz 1.1.12** Es gibt keine Menge, die jede Menge als Element enthält  $\square$

*Beweis.* Siehe Tutorium 1.  $\blacksquare$

### Vereinigungsaxiom

**Axiom 1.1.13 (Vereinigungsaxiom)**

1. Seien  $M$  und  $N$  zwei Mengen, dann gibt es eine Menge  $M \cup N$ , die **Vereinigung** von  $M$  und  $N$ , die genau alle Elemente von  $M$  und  $N$  enthält. Mit Symbolen

$$M \cup N = \{x \mid x \in M \text{ oder } x \in N\}.$$

2. Verallgemeinerung. Sei  $I$  eine Indexmenge und  $(M_i)_{i \in I}$  eine Familie von Mengen, dann gibt es eine Menge

$$\bigcup_{i \in I} M_i,$$

die **Vereinigung** von  $(M_i)_{i \in I}$ , die genau alle Elemente von  $M_i$  für alle  $i \in I$  enthält. Mit Symbole

$$\bigcup_{i \in I} M_i = \{x \mid \text{es gibt ein } i \in I \text{ so dass } x \in M_i\}.$$

**Beispiel 1.1.14** Here sind Beispiele von Mengen.

1. Die leere Menge  $\emptyset$ .
2. Zu jedes Element  $x \in M$  kan man die einelementige Menge  $\{x\}$  definieren.
2. Zu zwei Elemente  $x$  und  $y$  kann mann die Paarmenge

$$\{x, y\} = \{x\} \cup \{y\} = \{y\} \cup \{x\} = \{y, x\}$$

definieren. Es ist die Menge, die genau  $x$  und  $y$  enthält.

Aus dem Vereinigungsaxiom und dem Aussonderungsaxiom ergibt sich die Existenz des Durchschnitts von Mengen.

**Satz 1.1.15 (Durchschnitt)**

1. Seien  $M$  und  $N$  zwei Mengen, dann gibt es genau eine Menge  $M \cap N$ , der **Durchschnitt** von  $M$  und  $N$ , die genau die Elementen von  $M$  und  $N$  enthält. Mit Symbole

$$M \cap N = \{x \in M \cup N \mid x \in M \text{ und } x \in N\}.$$

2. Verallgemeinerung. Sei  $I$  eine Indexmenge und  $(M_i)_{i \in I}$  eine Familie von Mengen, dann gibt es genau eine Menge

$$\bigcap_{i \in I} M_i,$$

der **Durchschnitt** von  $(M_i)_{i \in I}$ , welche genau die Elemente, die in jeder Menge  $M_i$  für all  $i \in I$  enthalten sind. Mit Symbole

$$\bigcap_{i \in I} M_i = \left\{ x \in \bigcup_{i \in I} M_i \mid \text{für alle } i \in I \text{ gilt } x \in M_i \right\}.$$

**Satz 1.1.16** Seien  $M$ ,  $N$  und  $O$  drei Mengen. Dann gilt.

1.  $M \cup M = M$  und  $M \cap M = M$ .
2.  $M \cup N = N \cup M$  und  $M \cap N = N \cap M$ .
3.  $M \cup (N \cup O) = (M \cup N) \cup O$  und  $M \cap (N \cap O) = (M \cap N) \cap O$

□

*Beweis.* Übung ■

**Satz 1.1.17** Seien  $M$ ,  $N$  und  $O$  drei Mengen. Dann gilt.

$$1. M \cap (N \cup O) = (M \cap N) \cup (M \cap O).$$

$$2. M \cup (N \cap O) = (M \cup N) \cap (M \cup O).$$

□

*Beweis.* Siehe Übungsblatt 0. ■

**Definition 1.1.18** Das **Komplement** von  $N$  in  $M$  ist die Menge  $M \setminus N$  von elemente die in  $M$  und nicht in  $N$  enthalten sind. Mit Symbole:

$$M \setminus N = \{x \in M \mid x \notin N\}.$$

**Satz 1.1.19** Seien  $M$ ,  $N$  und  $O$  drei Mengen. Dann gilt.

$$1. M \setminus (N \cup O) = (M \setminus N) \cap (M \setminus O).$$

$$2. M \setminus (N \cap O) = (M \setminus N) \cup (M \setminus O).$$

□

*Beweis.* Siehe Übungsblatt 0. ■

## Potenzmengensaxiom

**Axiom 1.1.20** Sei  $M$  eine Menge, dann gibt es genau eine Menge, die **Potenzmenge**  $\mathfrak{P}(M)$  von  $M$ , welche Elemente genau alle Teilmenge von  $M$  sind.

**Beispiel 1.1.21**

$$1. \mathfrak{P}(\emptyset) = \{\emptyset\}.$$

$$2. \mathfrak{P}(\{\emptyset\}) = \{\emptyset; \{\emptyset\}\}.$$

$$3. \mathfrak{P}(\{0; 1; 2\}) = \{\emptyset; \{0\}; \{1\}; \{2\}; \{0; 1\}; \{0; 2\}; \{1; 2\}; \{0; 1; 2\}\}.$$

## Kartesische Produkt

**Definition 1.1.22 (Kartesische Produkt)** Seien  $M$  und  $N$  zwei Mengen.

1. Ein **geordnetes Paar** von Elementen  $x \in M$  und  $y \in N$  besteht aus der Angabe eines ersten Elements  $x \in M$  und eines zweiten Elements  $y \in N$ . Paaren werden als  $(x, y)$  geschrieben.

2. Die Menge aller geordneten Paare von Elementen aus  $M$  und  $N$  heißt das **Kartesische Produkt** und ist durch  $M \times N = \{(x, y) \mid x \in M, y \in N\}$  bezeichnet.

**Satz 1.1.23** Es gilt  $(x, y) = (y, x)$  genau dann wenn  $x = y$ . □

**Beispiel 1.1.24** Sei  $M = \{0; 1; 2\}$  und  $N = \{A, B\}$  dann gilt

$$M \times N = \{(0, A); (0, B); (1, A); (1, B); (2, A); (2, B)\}.$$

## 1.2 Natürliche Zahlen

### 1.2.1 Definition

Wir haben noch keine unendliche Menge, *i. e.* Menge mit unendlichen vielen Elementen, gesehen. Wir brauchen eigentlich ein neues Axiom dafür.

**Axiom 1.2.1 (Peano Axiome)** Es gibt eine Menge  $\mathbb{N}$ , die Meger der natürlichen Zahlen mit den folgenden Eigenschaften:

- zu jeder  $n \in \mathbb{N}$ , gibt es genau einen Nachfolger  $N(n) \in \mathbb{N}$  (später  $N(n) = n+1$ ).
- Es gibt ein Element  $0 \in \mathbb{N}$ , so dass für alle  $n \in \mathbb{N}$  gilt  $N(n) \neq 0$ .
- Jede  $n \in \mathbb{N}$  ist Nachfolger höchstens einer natürlichen Zahlen.
- Sei  $M$  eine Teilmenge von  $\mathbb{N}$ , so dass

$$- 0 \in M$$

$$- n \in M \Rightarrow N(n) \in M$$

dann gilt  $M = \mathbb{N}$  (**Induktionseigenschaftaxiom**).

**Notation 1.2.2** Konkret kann man die natürliche Zahlen wie folgt definieren:  $0$ ,  $1 = N(0)$ ,  $2 = N(1)$ ,  $3 = N(2)$  ...  $n+1 = N(n)$ .

Man kann mit dieser Definiton die klassische arthmetische Eigenschaften von  $\mathbb{N}$  zurück finden.

**Beispiel 1.2.3** Here sind weitere Beispiele von unendliche Mengen die man dank der Existenz von  $\mathbb{N}$  konstruieren kann.

Die Menge der ganzen Zahlen ist  $\mathbb{Z}$ .

Die Mende der rationale Zahlen ist  $\mathbb{Q}$ .

Die Mende der reelen Zahlen ist  $\mathbb{R}$ .

Die Mende der komplexen Zahlen ist  $\mathbb{C}$ .

### 1.2.2 Induktion

**Satz 1.2.4** Sei  $P$  eine eigenschaft die eine natürliche Zahl haben kann. Wenn  $P(0)$  und  $P(n) \Rightarrow P(n+1)$  wahr sind, dann ist  $P(n)$  wahr für jede  $n \in \mathbb{N}$ .  $\square$

*Beweis.* Sei  $M = \{n \in \mathbb{N} \mid P(n) \text{ ist wahr}\}$ , dann gilt  $0 \in M$  und  $n \in M \Rightarrow N(n) \in M$ . Vom Induktionseigenschaftaxiom folgt  $M = \mathbb{N}$ .  $\blacksquare$

### Beispiel 1.2.5

1. Für alle  $n \in \mathbb{N}$  gilt  $0 + 1 + 2 + \dots + n = \frac{n(n+1)}{2}$ .
2. Für alle  $n \in \mathbb{N}$  gilt  $0^2 + 1^2 + 2^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}$ .
3. Für alle  $n \in \mathbb{N}$  gilt  $0^3 + 1^3 + 2^3 + \dots + n^3 = \frac{n^2(n+1)^2}{4}$ .

*Beweis.* 1. Sei  $P(n)$  die Eigenschaft

$$0 + 1 + 2 + \dots + n = \frac{n(n+1)}{2}.$$

Dann gilt  $P(0)$ . Angenommen, dass  $P(n)$  gilt, dann gilt

$$0 + 1 + 2 + \dots + n + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{n^2 + n + 2n + 2}{2} = \frac{(n+1)(n+2)}{2}.$$

2. und 3. Siehe Übungsblatt 0. ■

## 1.3 Auswahlaxiom

Wir geben noch ein Axiom, das nicht von den Anderen abhängt.

**Axiom 1.3.1 (Auswahlaxiom)** Sei  $(M_i)_{i \in I}$  ein Mengensystem so dass für jedes  $i \in I$ , gilt  $M_i \neq \emptyset$  und für jede  $i, j \in I$ , gilt  $M_i \cap M_j = \emptyset$ . Dann gibt es eine Menge  $M$ , so dass für jedes  $i \in I$  die Menge  $M_i \cap M$  genau ein Element enthält.

Dieses Axiom wird später benutzt, um zu beweisen, dass jeder Vektorraum eine Basis enthält.

## 1.4 Abbildungen

**Definition 1.4.1** Seien  $M$  und  $N$  zwei Mengen. Eine **Abbildung**  $f$  von  $M$  nach  $N$  ist eine Vorschrift, durch die jede Elemente  $x \in M$  genau ein Element  $f(x) \in N$  zugeordnet wird. In Symbol man schreibt:

$$\begin{aligned} f: M &\rightarrow N \\ x &\mapsto f(x). \end{aligned}$$

Die Menge  $M$  heißt **Definitionsbereich** und  $N$  heißt **Wertebereich** der Abbildung  $f$ .

**Beispiel 1.4.2**

1. Sei  $M$  eine Menge, es gibt die **identische Abbildung**  $\text{Id}_M : M \rightarrow M, x \mapsto x$ .
2. Sei  $f : \mathbb{R} \rightarrow \mathbb{R}, x \mapsto x^2$ .

**Definition 1.4.3** Seien  $f : M \rightarrow N$  und  $g : N \rightarrow O$ , dann kann man  $f$  mit  $g$  **componieren**. Als Resultat erhält man eine Abbildung  $g \circ f : M \rightarrow O$  definiert durch  $x \mapsto g(f(x))$ .

**Definition 1.4.4** Sei  $f : M \rightarrow N$  eine Abbildung und seien  $X \subset M$  und  $Y \subset N$  Teilmengen von  $M$  und  $N$ . Das **Bild** von  $X$  unter  $f$  ist die Teilmenge von  $N$  definiert durch

$$f(X) = \{y \in N \mid \exists x \in X \text{ mit } y = f(x)\} = \{f(x) \mid x \in X\}.$$

Das **Urbild** von  $Y$  ist die Teilmenge von  $M$  definiert durch

$$f^{-1}(Y) = \{x \in M \mid f(x) \in Y\}.$$

Für eine Teilmenge  $\{y\}$  mit einem einzigen Element schreibt man  $f^{-1}(y) = f^{-1}(\{y\})$ .

**Beispiel 1.4.5** Sei  $f : \mathbb{Z} \rightarrow \mathbb{Z}$  die Abbildung definiert durch  $x \mapsto x^2$ . Dann gilt  $f(\{-1; 1\}) = \{1\}$  und  $f^{-1}(1) = \{-1; 1\}$ .

**Definition 1.4.6** Sei  $f : M \rightarrow N$  eine Abbildung.

1. Die Abbildung  $f$  heißt **injektiv** wenn, für alle  $x, x' \in M$  gilt die Implikation  $f(x) = f(x') \Rightarrow x = x'$  (oder  $x \neq x' \Rightarrow f(x) \neq f(x')$ ).
2. Die Abbildung  $f$  heißt **surjektiv** wenn,  $f(M) = N$ .
3. Die Abbildung  $f$  heißt **bijektiv** wenn sie injektiv und surjektiv ist.

**Satz 1.4.7** Sei  $f : M \rightarrow N$  eine Abbildung. Die Abbildung  $f$  ist bijektiv genau dann wenn existiert eine Abbildung  $g : N \rightarrow M$  mit  $g \circ f = \text{Id}_M$  und  $f \circ g = \text{Id}_N$ .

Für  $f$  bijektiv ist die Abbildung  $g$  eindeutig definiert. □

*Beweis.* Angenommen  $f$  sei bijektiv. Sei  $y \in N$ . Als  $f$  surjektiv ist, existiert ein Element  $x \in M$  mit  $f(x) = y$ . Das Element  $x$  ist von  $y$  eindeutig definiert weil für  $x' \in M$  mit  $f(x) = f(x')$  gilt  $x = x'$ . Man definiert  $g : N \rightarrow M$  mit  $g(y) = x$ . Dann gilt  $f \circ g(y) = f(g(y)) = f(x) = y$  und  $g \circ f(x) = g(f(x)) = g(y) = x$ .

Die Abbildung  $g$  ist eindeutig: sei  $h : N \rightarrow M$  mit  $h \circ f = \text{Id}_M$  und  $f \circ h = \text{Id}_N$ , dann gilt für  $y = f(x) \in N$ :  $h(y) = g(f(x)) = x = g(y)$ . Da  $f$  surjetiv gilt die Gleichheit  $h(y) = g(y)$  für alle  $y \in N$ .

Angenommen es gibt  $g$ , dann für  $x, y \in M$  mit  $f(x) = f(y)$  gilt  $x = g(f(x)) = g(f(y)) = y$ , so dass  $f$  injektiv ist. Sei  $y \in N$  dann gilt  $y = f(g(y))$  und  $f$  ist surjektiv. ■

**Definition 1.4.8** Sei  $f : M \rightarrow N$  eine bijektive Abbildung, dann ist die einzige Abbildung  $g$  so dass  $g \circ f = \text{Id}_M$  und  $f \circ g = \text{Id}_N$  die **Umkehrabbildung** genannt und wird mit  $f^{-1} : N \rightarrow M$  geschrieben.

**Bemerkung 1.4.9** Sei  $f : M \rightarrow N$  eine Abbildung und  $Y$  eine Teilmenge von  $N$ . Die Urbild  $f^{-1}(Y)$  ist für jede (auch nicht bijektive) Abbildung definiert und für  $y \in N$  ist die Urbild  $f^{-1}(y)$  für jede (auch nicht bijektive) Abbildung definiert.

**Satz 1.4.10** Seien  $f : M \rightarrow N$  und  $g : N \rightarrow O$  zwei Abbildungen. Dann gilt.

1.  $f$  und  $g$  injektiv  $\Rightarrow g \circ f$  injektiv.

2.  $f$  und  $g$  surjektiv  $\Rightarrow g \circ f$  surjektiv.

3.  $f$  und  $g$  bijektiv  $\Rightarrow g \circ f$  bijektiv. □

*Beweis.* 1. Seien  $x, y \in M$ , so dass  $g \circ f(x) = g \circ f(y)$ , dann gilt  $g(f(x)) = g(f(y))$  und als  $g$  injektiv ist, gilt  $f(x) = f(y)$ . Als  $f$  injektiv ist, gilt  $x = y$  so dass  $g \circ f$  injektiv ist.

2. Sei  $z \in O$ . Als  $g$  surjektiv ist, gibt es  $y \in N$  mit  $g(y) = z$ . Als  $f$  surjektiv ist, gibt es  $x \in M$  mit  $f(x) = y$ . Dann gilt  $g \circ f(x) = g(f(x)) = g(y) = z$  und  $g \circ f$  ist surjektiv.

3. Folgt aus 1. und 2. ■

**Satz 1.4.11** Sei  $f : M \rightarrow N$  eine Abbildung zwischen nicht leere Mengen.

1. Die Abbildung  $f$  ist injektiv genau dann wenn, es eine Abbildung  $g : N \rightarrow M$  mit  $g \circ f = \text{Id}_M$  gibt.

2. Die Abbildung  $f$  ist surjektiv genau dann wenn, es eine Abbildung  $h : N \rightarrow M$  mit  $f \circ h = \text{Id}_N$  gibt.

3. Wenn  $f$  bijektiv ist dann sind die beide Abbildungen  $g : N \rightarrow M$  und  $h : N \rightarrow M$  gleich die Umkehrabbildung  $f^{-1}$ . □

*Beweis.* Siehe Tutorium 2. ■

**Definition 1.4.12** Sei  $f : M \rightarrow N$  eine Abbildung, der **Graph** von  $f$  ist die Teilmenge  $\Gamma(f) \subset M \times N$  von  $M \times N$  definiert durch

$$\Gamma(f) = \{(x, y) \in M \times N \mid y = f(x)\} = \{(x, f(x)) \mid x \in M\}.$$

**Definition 1.4.13** Seien  $M$  und  $N$  zwei Mengen, dann ist  $N^M$  die **Menge aller Abbildungen** von  $M$  nach  $N$ .



### 1.4.1 Abbildungen und Mengenoperationen

**Satz 1.4.14** Seien  $f : M \rightarrow N$  eine Abbildung,  $M_1, M_2 \subset M$  und  $N_1, N_2 \subset N$  dann gilt:

1.  $M_1 \subset M_2 \Rightarrow f(M_1) \subset f(M_2)$  und  $N_1 \subset N_2 \Rightarrow f^{-1}(N_1) \subset f^{-1}(N_2)$ .
2.  $f(M_1 \cup M_2) = f(M_1) \cup f(M_2)$  und  $f^{-1}(N_1 \cup N_2) = f^{-1}(N_1) \cup f^{-1}(N_2)$ .
3.  $f(M_1 \cap M_2) \subset f(M_1) \cap f(M_2)$  und  $f^{-1}(N_1 \cap N_2) = f^{-1}(N_1) \cap f^{-1}(N_2)$ .
4.  $f(M_1) \setminus f(M_2) \subset f(M_1 \setminus M_2)$  und  $f^{-1}(N_1 \setminus N_2) = f^{-1}(N_1) \setminus f^{-1}(N_2)$ . □

*Beweis.* Siehe Übungsblatt 2. ■

## 1.5 Relationen

### 1.5.1 Erste Definition

**Definition 1.5.1** Sei  $M$  eine Menge. Eine **Relation** auf der Menge  $M$  ist eine Teilmenge  $R$  von  $M \times M$ . Seien  $x, y$  zwei Elemente in  $M$ , für  $(x, y) \in R$  schreibt man  $x \sim_R y$ .

**Beispiel 1.5.2** 1. Sei  $M$  eine Menge, die Relation  $R = \{(x, y) \in M \times M \mid x = y\}$  ist die Gleichheitsrelation. Es gilt  $x \sim_R y \Leftrightarrow x = y$ .

2. Sei  $M = \mathbb{N}$  und  $R = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid x \leq y\}$ . Dann ist  $R$  eine Relation auf  $\mathbb{N}$ .

3. Sei  $M$  eine Menge und  $R = \{(A, B) \in \mathfrak{P}(M) \mid A \cap B = \emptyset\}$ . Dann ist  $R$  eine Relation auf  $M$ .

**Definition 1.5.3** Sei  $R$  eine Relation auf einer Menge  $M$ .

1.  $R$  heißt **reflexiv**, wenn  $x \sim_R x$  für alle  $x \in M$ .
2.  $R$  heißt **symmetrisch**, wenn  $x \sim_R y \Rightarrow y \sim_R x$ .
3.  $R$  heißt **antisymmetrisch**, wenn  $(x \sim_R y \text{ und } y \sim_R x) \Rightarrow x = y$ .
4.  $R$  heißt **transitiv**, wenn  $(x \sim_R y \text{ und } y \sim_R z) \Rightarrow x \sim_R z$ .

**Beispiel 1.5.4** 1. Sei  $M$  eine Menge, die Gleichheitsrelation  $R = \{(x, y) \in M \times M \mid x = y\}$  ist reflexiv, symmetrisch, antisymmetrisch und transitiv.

2. Sei  $M = \mathbb{N}$  die Relation  $R = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid x \leq y\}$  ist reflexiv, antisymmetrisch und transitiv aber nicht symmetrisch.

3. Sei  $M$  eine nichtleere Menge. Die Relation  $R = \{(A, B) \in \mathfrak{P}(M) \mid A \cap B = \emptyset\}$  auf der Menge  $M$  ist nicht reflexiv, symmetrisch, nicht antisymmetrisch und nicht transitiv.

## 1.5.2 Ordnungsrelationen

**Definition 1.5.5** Sei  $M$  eine Menge und  $R$  eine Relation auf  $M$ . Die Relation  $R$  heißt **Ordnungsrelation**, wenn  $R$  reflexiv, antisymmetrisch und transitiv ist.

**Beispiel 1.5.6** 1. Sei  $M$  eine Menge, die Gleichheitsrelation ist eine Ordnungsrelation.

2. Sei  $M = \mathbb{N}$  die Relation  $R = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid x \leq y\}$  ist eine Ordnungsrelation.

3. Sei  $M$  eine nichtleere Menge. Die Relation  $R = \{(A, B) \in \mathfrak{P}(M) \mid A \cap B = \emptyset\}$  ist nicht eine Ordnungsrelation.

## 1.5.3 Äquivalenzrelationen

**Definition 1.5.7** Sei  $R$  eine Relation auf einer Menge  $M$ . 4.  $R$  heißt **Äquivalenzrelation**, wenn  $R$  reflexiv, symmetrisch und transitiv ist.

**Beispiel 1.5.8** 1. Sei  $M$  eine Menge, die Gleichheitsrelation ist eine Äquivalenzrelation.

2. Sei  $M = \mathbb{N}$  die Relation  $R = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid x \leq y\}$  ist keine Äquivalenzrelation.

3. Sei  $M$  eine nichtleere Menge. Die Relation  $R = \{(A, B) \in \mathfrak{P}(M) \mid A \cap B = \emptyset\}$  ist keine Äquivalenzrelation.

**Lemma 1.5.9** Sei  $R = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid x - y \text{ ist gerade}\}$ . Dann ist  $R$  eine Äquivalenzrelation auf  $\mathbb{N}$ . □

*Beweis.* Siehe Übungsblatt 2. ■

**Satz 1.5.10** Sei  $f : M \rightarrow N$  eine Abbildung. Dann ist  $R = \{(x, y) \in M \mid f(x) = f(y)\}$  eine Äquivalenzrelation. □

*Beweis.* Als  $f(x) = f(x)$ , gilt  $x \sim_R x$ . Für  $x \sim_R y$ , gilt  $f(x) = f(y)$  und  $f(y) = f(x)$ , so dass  $y \sim_R x$  gilt. Für  $x \sim_R y$  und  $y \sim_R z$ , gilt  $f(x) = f(y)$  und  $f(y) = f(z)$ , so dass  $f(x) = f(z)$  und  $x \sim_R z$  gilt. ■

### 1.5.4 Quotient

**Definition 1.5.11** Sei  $R$  eine Äquivalenzrelation auf einer Menge  $M$ .

1. Die **Äquivalenzklasse**  $[x]$  von  $x$  ist die Menge aller Elemente  $y$  mit  $x \sim_R y$ . Mit Symbol:

$$[x] = \{y \in M \mid x \sim_R y\}.$$

2. Die Gesamtheit der Äquivalenzklassen bildet eine Teilmenge der Potenzmenge  $\mathfrak{P}(M)$  die man  $M/R$  bezeichnet und **Quotientenmenge von  $M$  nach  $R$** . Mit Symbol

$$\begin{aligned} M/R &= \{N \in \mathfrak{P}(M) \mid \exists x \in M \text{ mit } N = [x]\} \\ &= \{[x] \in \mathfrak{P}(M) \mid x \in M\}. \end{aligned}$$

**Lemma 1.5.12** Sei  $R$  eine Äquivalenzrelation auf einer Menge  $M$  und sei  $x, y \in M$ . Dann sind die folgende Aussagen äquivalent:

1.  $[x] = [y]$ ;

2.  $[x] \cap [y] \neq \emptyset$ ;

3.  $x \sim_R y$ . □

*Beweis.* 1.  $\Rightarrow$  2. Trivial:  $x \in [x] = [y]$  also  $x \in [x] \cap [y]$ .

2.  $\Rightarrow$  3. Sei  $z \in [x] \cap [y]$ . Dann gilt  $x \sim_R z$  und  $y \sim_R z$ . Als  $R$  symmetrisch ist gilt  $z \sim_R y$  und von der transitivität gilt  $x \sim_R y$ .

3.  $\Rightarrow$  1. Sei  $z \in [x]$ , dann gilt  $x \sim_R z$ . Als  $R$  symmetrisch und transitiv ist gilt  $y \sim_R z$  i. e.  $z \in [y]$  und  $[x] \subset [y]$ . Die Inklusion  $[y] \subset [x]$  kann man mit der selben Methode beweisen. ■

**Korollar 1.5.13** Sei  $O \in M/R$  eine Äquivalenzklasse dann gilt  $x \in O \Leftrightarrow [x] = O$ .

**Definition 1.5.14** Sei  $M$  eine Menge, eine **Partition** von  $M$  ist eine Familie  $(M_i)_{i \in I}$  von Teilmengen  $M_i \subset M$  so dass

- $M_i \cap M_j = \emptyset$  für  $i \neq j$ ,

- $\bigcup_{i \in I} M_i = M$ .

**Satz 1.5.15** Sei  $R$  eine Äquivalenzrelation auf einer Menge  $M$ . Dann bildet die Familie von Äquivalenzklassen eine Partition von  $M$ . □

*Beweis.* Aus Lemma 1.5.12 gilt  $[x] \cap [y] = \emptyset$  für  $[x] \neq [y]$ . Außerdem, gibt es für jedes Element  $x \in M$  eine Klasse:  $[x]$  so dass  $x \in [x]$ . Es gilt daher

$$M \subset \bigcup_{[x] \in M/R} [x].$$

Die umgekehrte Inklusion gilt auch da  $[x] \subset M$  für alle  $[x]$ . ■

**Definition 1.5.16** Sei  $R$  eine Äquivalenzrelation auf einer Menge  $M$ . Die Abbildung  $p_R : M \rightarrow M/R$  definiert durch  $x \mapsto [x]$  heißt die **kanonische Projektion**.

**Lemma 1.5.17** Sei  $R$  eine Äquivalenzrelation auf einer Menge  $M$ .

1. Die kanonische Projektion  $p_R$  ist surjektiv.
2. Es gilt für  $x, y \in M$ :  $[x] = [y] \Leftrightarrow p_R(x) = p_R(y)$ . □

*Beweis.* 1. Sei  $[x] \in M/R$ , dann gilt  $[x] = p_R(x)$ .

2. Trivial aus der Definition. ■

**Satz 1.5.18** Sei  $R$  eine Äquivalenzrelation auf einer Menge  $M$ . Sei  $f : M \rightarrow N$  eine Abbildung, so dass  $[x] = [y] \Rightarrow f(x) = f(y)$ . Dann gibt es eine Abbildung  $\bar{f} : M/R \rightarrow N$ , so dass  $f = \bar{f} \circ p_R$ .

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ p_R \downarrow & \nearrow \bar{f} & \\ M/R & & \end{array}$$

*Beweis.*  $M/R$  ist eine Menge von Teilmengen von  $M$ . Sei  $O \in M/R$  (z.b.  $O = [z]$  für  $z \in M$ ). Wenn die Abbildung  $\bar{f}$  existiert, dann gilt für  $x \in O$ :  $f(x) = \bar{f}(p_R(x)) = \bar{f}([x]) = \bar{f}(O)$  i.e.  $\bar{f}(O) = f(x)$ .

Seien  $x, y \in O$ , dann gilt aus Lemma 1.5.17:  $[x] = O = [y]$  und  $f(x) = f(y)$ . Die Abbildung  $O \rightarrow N$  definiert durch  $x \mapsto f(x)$  ist konstant gleich  $n \in N$ . Wir definieren  $\bar{f}(O) = n$ . Es gilt  $n = f(x)$  für jeder  $x \in O$ .

Es gilt  $\bar{f} \circ p_R(x) = \bar{f}([x]) = f(x)$ . ■

## 2 Gruppen, Körper und Ringe

### 2.1 Gruppen

#### 2.1.1 Definition und Beispiele

**Definition 2.1.1** Eine **Gruppe** ist ein geordnetes Paar  $(G, m)$  mit  $G$  einer Menge und  $m$  einer Abbildung  $m : G \times G \rightarrow G$  (auch **Verknüpfung** genannt) so dass die folgenden Eigenschaften erfüllt sind:

- Es existiert ein **neutrales Element**  $e$  in  $G$  mit  $m(e, x) = m(x, e) = x$  für alle  $x \in G$ .
- Die Verknüpfung  $m$  ist **assoziativ**, dass heißt  $m(x, m(y, z)) = m(m(x, y), z)$  für alle  $x, y, z \in G$ .
- Für jedem  $x \in G$  gibt es ein **inverses Element**, dass heißt eine Element  $y \in G$  mit  $m(x, y) = m(y, x) = e$ .

**Definition 2.1.2** Eine Gruppe  $(G, m)$  heißt **kommutativ** oder **abelsch** falls gilt:  $m(x, y) = m(y, x)$  für alle  $x, y \in G$ .

**Notation 2.1.3** Wir werden oft die Verknüpfung  $m : G \times G \rightarrow G$  mit einem multiplikativen Symbol schreiben:  $m(x, y) = x \cdot y$ . Die Axiome für die Definition einer Gruppen sehen wie folgt aus:

- **Neutrales Element:**  $e \in G$  mit  $e \cdot x = x \cdot e = x$  für alle  $x \in G$ .
- **Assoziativität:**  $x \cdot (y \cdot z) = (x \cdot y) \cdot z$  für alle  $x, y, z \in G$ .
- **Inverses Element:** für jedem  $x \in G$  existiert  $y \in G$  mit  $x \cdot y = y \cdot x = e$ .

Die **Kommutativität** sieht wie folgt aus:

$$x \cdot y = y \cdot x.$$

**Beispiel 2.1.4** Hier sind Beispiele von Gruppen:

- $(\mathbb{Z}, +)$ , wo  $+$  :  $\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$  durch  $(x, y) \mapsto x + y$  definiert ist, ist eine abelsche Gruppe.

- $(\mathbb{Q}, +)$ , wo  $+: \mathbb{Q} \times \mathbb{Q} \rightarrow \mathbb{Q}$  durch  $(x, y) \mapsto x + y$  definiert ist, ist eine abelsche Gruppe.
- $(\mathbb{R}, +)$ , wo  $+: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$  durch  $(x, y) \mapsto x + y$  definiert ist, ist eine abelsche Gruppe.
- $(\mathbb{C}, +)$ , wo  $+: \mathbb{C} \times \mathbb{C} \rightarrow \mathbb{C}$  durch  $(x, y) \mapsto x + y$  definiert ist, ist eine abelsche Gruppe.
- $(\mathbb{Q} \setminus \{0\}, \times)$ , wo  $\times: \mathbb{Q} \setminus \{0\} \times \mathbb{Q} \setminus \{0\} \rightarrow \mathbb{Q} \setminus \{0\}$  durch  $(x, y) \mapsto x \times y$  definiert ist, ist eine abelsche Gruppe.
- Für eine Menge  $M$ , die Menge  $\text{Bij}(M)$  der bijektiven Selbstabbildungen  $f: M \rightarrow M$  mit der Verknüpfung  $\text{Bij}(M) \times \text{Bij}(M) \rightarrow \text{Bij}(M)$  gegeben durch Komposition von Abbildungen:  $(f, g) \mapsto f \circ g$  ist eine Gruppe. Die Gruppe  $(\text{Bij}(M), \circ)$  ist nicht kommutativ sofern  $M$  mindestens drei paarweise verschiedene Elemente enthält.
- $(\mathbb{N}, +)$  ist keine Gruppe: 1 hat kein inverses Element.

**Satz 2.1.5** Sei  $(G, \cdot)$  eine Gruppe.

1. Das neutral Element ist eindeutig bestimmt.

2. Sei  $x \in G$ , das inverse Element von  $x$  ist eindeutig bestimmt. □

*Beweis.* 1. Seien  $e$  und  $e'$  zwei neutrale Elemente. Dann gilt  $e' = e \cdot e'$  weil  $e'$  neutral ist und  $e \cdot e' = e'$  weil  $e$  neutral ist. Es folgt  $e' = e \cdot e' = e$ .

2. Seien  $y$  und  $y'$  zwei inverse Elemente von  $x$ . Dann gilt

$$y = e \cdot y = (y' \cdot x) \cdot y = y' \cdot (x \cdot y) = y'.$$

**Beispiel 2.1.6** Wir beschreiben das neutral Element und das inverse von einem Element  $x$  in den obigen Beispielen von Gruppen.

- $(\mathbb{Z}, +)$ : neutral Element 0. Inverse von  $x$ :  $-x$ .
- $(\mathbb{Q}, +)$ : neutral Element 0. Inverse von  $x$ :  $-x$ .
- $(\mathbb{R}, +)$ : neutral Element 0. Inverse von  $x$ :  $-x$ .
- $(\mathbb{C}, +)$ : neutral Element 0. Inverse von  $x$ :  $-x$ .
- $(\mathbb{Q} \setminus \{0\}, \times)$ : neutral Element 1. Inverse von  $x$ :  $\frac{1}{x} = x^{-1}$ .
- $(\text{Bij}(M), \circ)$ : neutral Element  $\text{Id}_M$ . Inverse von  $f$ :  $f^{-1}$ .

**Notation 2.1.7**

1. Oft (aber nicht immer) werden wir allgemeine Verknüpfungen auf  $G$  die eine Gruppe definieren mit  $\cdot$  bezeichnen. In diesem Fall werden wir das neutral Element mit 1 bezeichnen und das inverse Element von  $x$  mit  $x^{-1}$  bezeichnen.
2. Wenn eine Gruppe abelsch ist werden wir oft (aber nicht immer) die Verknüpfung mit  $+$  bezeichnen. Dann werden wir das neutral Element mit 0 bezeichnen und das inverse Element von  $x$  mit  $-x$  bezeichnen.
3. Sei  $(G, \cdot)$  eine Gruppe und seien  $(a_i)_{i \in [1, n]}$   $n$  Elemente in  $G$ . Dann werden wir das Produkt von diesen Elementen mit

$$\prod_{i=1}^n a_i$$

bezeichnen. Falls  $n = 0$  zugelassen ist, dann handelt es sich um die **leere Folge**. Man erklärt das zugehörige leere Produkt durch

$$\prod_{i=1}^0 a_i = 1.$$

4. Sei  $(G, +)$  eine Gruppe und seien  $(a_i)_{i \in [1, n]}$   $n$  Elemente in  $G$ . Dann werden wir die Summe von diesen Elementen mit

$$\sum_{i=1}^n a_i$$

bezeichnen. Falls  $n = 0$  zugelassen ist, dann handelt es sich um die **leere Folge**. Man erklärt das zugehörige leere Summe durch

$$\sum_{i=1}^0 a_i = 0.$$

**2.1.2 Untergruppe**

**Definition 2.1.8** Sei  $(G, \cdot)$  eine Gruppe und  $H \subset G$  eine Teilmenge, dann heißt  $H$  eine **Untergruppe** von  $G$  wenn gilt:

1.  $1 \in H$ ,
2.  $x, y \in H \Rightarrow x \cdot y \in H$ ,
3.  $x \in H \Rightarrow x^{-1} \in H$ .

**Satz 2.1.9** Sei  $H$  eine Untergruppe von  $(G, \cdot)$ , dann ist  $(H, \cdot)$  eine Gruppe. □

*Beweis.* Siehe Übungsblatt 3. ■

**Satz 2.1.10** Sei  $(G, \cdot)$  eine Gruppe und seien  $x, y, z$  Elemente in  $G$ . Dann gilt:

1.  $xy = xz \Rightarrow y = z$ ,
2.  $yx = zx \Rightarrow y = z$ ,
3.  $(x^{-1})^{-1} = x$ ,
4.  $(xy)^{-1} = y^{-1}x^{-1}$ . □

*Beweis.* 1. Es gilt  $y = (x^{-1}x)y = x^{-1}(xy) = x^{-1}(xz) = (x^{-1}x)z = z$ .

2. Es gilt  $y = y(xx^{-1}) = (yx)x^{-1} = (zx)x^{-1} = z(xx^{-1}) = z$ .

3. Es gilt  $xx^{-1} = x^{-1}x = 1$ , das heißt  $x$  ist das inverse Element für  $x^{-1}$ .

3. Es gilt  $(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = xx^{-1} = 1$  und  $(y^{-1}x^{-1})xy = y^{-1}(x^{-1}x)y = y^{-1}y = 1$ , das heißt  $y^{-1}x^{-1}$  ist das inverse Element für  $xy$ . ■

### 2.1.3 Gruppenhomomorphismus

**Definition 2.1.11** Seien  $(G, \cdot)$  und  $(G', \star)$  Gruppen. Eine Abbildung  $f : G \rightarrow G'$  heißt **Gruppenhomomorphismus** wenn für jeden  $x, y \in G$  gilt:

$$f(xy) = f(x) \star f(y).$$

**Satz 2.1.12** Sei  $f : G \rightarrow G'$  ein Gruppenhomomorphismus dann gilt für alle  $x \in G$

$$f(1) = e_{G'} \text{ und } f(x^{-1}) = f(x)^{-1}.$$

wo 1 das neutral Element von  $G$  ist und  $e_{G'}$  das neutral Element von  $G'$  ist. □

*Beweis.* Es gilt  $f(1) \star f(1) = f(1 \cdot 1) = f(1) = f(1) \star e_{G'}$  und von Satz 2.1.10.1 folgt  $f(1) = e_{G'}$ .

Es gilt  $f(x) \star f(x^{-1}) = f(xx^{-1}) = f(1) = e_{G'}$  und  $f(x^{-1}) \star f(x) = f(x^{-1}x) = f(1) = e_{G'}$ , das heißt  $f(x^{-1})$  ist das inverse Element von  $f(x)$ . ■

**Satz 2.1.13** Sei  $f : G \rightarrow G'$  ein Gruppenhomomorphismus, dann ist  $\ker(f) = \{x \in G \mid f(x) = e_{G'}\}$  eine Untergruppe von  $G$ . □

*Beweis.* Es gilt  $1 \in \ker(f)$ . Für  $x, y \in \ker(f)$  gilt  $f(xy) = f(x) \star f(y) = e_{G'} \star e_{G'} = e_{G'}$ , das heißt  $xy \in \ker(f)$  und  $f(x^{-1}) = f(x)^{-1} = e_{G'}^{-1} = e_{G'}$  das heißt  $x \in \ker(f)$ . ■

**Definition 2.1.14** Sei  $f : G \rightarrow G'$  ein Gruppenhomomorphismus, dann heißt die Untergruppe  $\ker(f) = \{x \in G \mid f(x) = e_{G'}\}$  der **Kern** von  $f$ .



**Satz 2.1.15** Sei  $f: G \rightarrow G'$  ein Gruppenhomomorphismus. Die Abbildung  $f$  ist genau dann injektiv, wenn  $\ker(f) = \{1\}$ .  $\square$

*Beweis.* Angenommen  $f$  sei injektiv, dann gilt für  $x \in \ker(f)$ :  $f(x) = e_{G'} = f(1)$  und  $x = 1$  folgt von der Injektivität.

Angenommen  $\ker(f) = \{1\}$ , dann gilt für  $x, y \in G$  mit  $f(x) = f(y)$ :  $f(xy^{-1}) = f(x)f(y)^{-1} = f(x)f(x)^{-1} = e_{G'}$ , dass heißt  $xy^{-1} \in \ker(f)$ . Weiter folgt  $xy^{-1} = 1$  und  $x = y$ .  $\blacksquare$

**Satz 2.1.16** Sei  $f: G \rightarrow G'$  ein Gruppenabbildung, dann ist das Bild von  $f$  eine Untergruppe von  $G'$   $\square$

*Beweis.* Siehe Übungsblatt 3.  $\blacksquare$

## 2.2 Körper

### 2.2.1 Definition und Beispiele

**Definition 2.2.1** Ein **Körper** ist ein geordnetes Paar  $(K, +, \cdot)$  mit  $K$  einer Menge und  $+$ ,  $\cdot$  Verknüpfungen auf  $K$ , so dass die folgenden Eigenschaften erfüllt sind:

- $(K, +)$  ist eine kommutative Gruppe mit neutral Element 0.
- $(K \setminus \{0\}, \cdot)$  ist eine kommutative Gruppe mit neutral Element 1.
- Für jeden  $x, y, z \in K$  gilt  $x(y + z) = xy + xz$  (**Distributivgesetz**).

Das Element 0 heißt das **Nullelement** von  $K$  und das Element 1 heißt das **Einselement** von  $K$ .

#### Notation 2.2.2

1. In die Gleichung  $x(y + z) = xy + xz$  hätten Wir eigentlich  $x(y + z) = (xy) + (xz)$  schreiben müssen. Implizit hier ist, dass die Multiplication  $\cdot$  Vorrang der Addition  $+$  hat.

2. Wir schreiben  $K^\times$  für  $K \setminus \{0\}$ .

3. Für  $x \in K$  und  $y \in K^\times$  schreiben wir  $\frac{x}{y} = xy^{-1}$ .

**Beispiel 2.2.3** Hier sind Beispiele von Körpern:

- $(\mathbb{Q}, +, \cdot)$  ist ein Körper.
- $(\mathbb{R}, +, \cdot)$  ist ein Körper.
- $(\mathbb{C}, +, \cdot)$  ist ein Körper.

- $(\mathbb{Z}, +, \cdot)$  ist keiner Körper: 2 hat kein inverses Element.

**Satz 2.2.4** Sei  $(K, +, \cdot)$  ein Körper.

1. Es gilt  $(y + z)x = yx + zx$  für alle  $x, y, z \in K$ ,
2. Es gilt  $x0 = 0x = 0$  für alle  $x \in K$ ,
3. Es gilt  $\frac{x}{y} + \frac{z}{t} = \frac{xt + yz}{yt}$  für alle  $x, z \in K$  und  $y, t \in K^\times$ .
4. Seien  $x, y \in K$ , dann gilt  $xy = 0_K \Rightarrow x = 0_K$  oder  $y = 0_K$ . □

*Beweis.* 1. Es gilt  $(y + z)x = z(y + z) = xy + xz = yx + zx$ .

2. Es gilt  $0x = x0 = x(0 + 0) = x0 + x0$  und mit Satz 2.1.10.1 gilt  $0x = x0 = 0$ .

3. Es gilt

$$\begin{aligned} \frac{x}{y} + \frac{z}{t} &= xy^{-1} + zt^{-1} = xtt^{-1}y^{-1} + zyy^{-1}t^{-1} = xt(yt)^{-1} + yz(yt)^{-1} \\ &= (xt + yz)(yt)^{-1} = \frac{xt + yz}{yt}. \end{aligned}$$

4. Seien  $x, y \in K$ , mit  $xy = 0_K$ . Falls  $x \neq 0_K$ , dann gilt  $y = (x^{-1}x)y = x^{-1}(xy) = x^{-1}0_K = 0_K$ . ■

## 2.2.2 Teilkörper

**Definition 2.2.5** Sei  $(K, +, \cdot)$  ein Körper  $L \subset K$  eine Teilmenge, dann heißt  $L$  ein **Teilkörper** von  $K$  wenn  $L$  eine Untergruppe von  $(K, +)$  ist und  $L^\times$  eine Untergruppen von  $(K^\times, \cdot)$  ist.

**Satz 2.2.6** Sei  $L$  ein Teilkörper von  $(K, +, \cdot)$ , dann ist  $(L, +, \cdot)$  ein Körper. □

*Beweis.* Folgt von Satz 2.1.9. ■

### Beispiel 2.2.7

1.  $\mathbb{Q}$  ist ein Teilkörper von  $(\mathbb{R}, +, \cdot)$  und von  $(\mathbb{C}, +, \cdot)$ .
2.  $\mathbb{R}$  ist ein Teilkörper von  $(\mathbb{C}, +, \cdot)$ .
3.  $\mathbb{Q}(\sqrt{2}) = \{x + y\sqrt{2} \in \mathbb{R} \mid x, y \in \mathbb{Q}\}$  ist ein Teilkörper von  $\mathbb{R}$  (siehe Übungsblatt 3).

### 2.2.3 Körperhomomorphismus

**Definition 2.2.8** Seien  $(K, +, \cdot)$  und  $(K', +, \cdot)$  zwei Körper. Eine Abbildung  $f : K \rightarrow K'$  heißt **Körperhomomorphismus** wenn  $f : (K, +) \rightarrow (K', +)$  und  $f : (K \times, \cdot) \rightarrow (K'^\times, \cdot)$  Gruppenhomomorphismus sind.

**Satz 2.2.9** Sei  $f : K \rightarrow K'$  ein Körperhomomorphismus dann gilt für alle  $x \in K$  und  $y \in K^\times$ :

$$f(0_K) = 0_{K'}, \quad f(1_K) = 1_{K'}, \quad f(-x) = -f(x) \quad \text{und} \quad f(y^{-1}) = f(y)^{-1}.$$

*Beweis.* Folgt von Satz 2.1.12. ■

**Beispiel 2.2.10** Sei  $f : \mathbb{C} \rightarrow \mathbb{C}$  mit  $f(z) = \bar{z}$  die komplexe Konjugation, dann ist  $f$  ein Körperhomomorphismus (siehe Übungsblatt 3).

**Satz 2.2.11** Sei  $f : K \rightarrow K'$  ein Körperhomomorphismus, dann ist  $f$  injektiv. □

*Beweis.* Wir berechnen  $\ker(f) = \{x \in K \mid f(x) = 0_{K'}\}$ . Sei  $x \in \ker(f)$  mit  $x \neq 0_K$ , dann gilt  $0_{K'} \neq 1_{K'} = f(1_K) = f(xx^{-1}) = f(x)f(x^{-1}) = 0_{K'}f(x^{-1}) = 0_{K'}$  ein Widerspruch. Weiter folgt  $x \in \ker(f) \Rightarrow x = 0_K$  und  $\ker(f) = \{0_K\}$  und aus Satz 2.1.15 folgt, dass  $f$  injektiv ist. ■

### 2.2.4 Die Charakteristik eines Körper

**Definition 2.2.12** Sei  $K$  ein Körper,  $n \in \mathbb{N}$  und  $x \in K$ . Man definiert  $n \cdot x$  durch

$$n \cdot x = \underbrace{x + x + \cdots + x}_{n \text{ mal}}.$$

Man definiert  $\text{char}(K)$ , die **Charakteristik** von  $K$ , durch  $\text{char}(K) = 0$  falls  $n \cdot 1_K \neq 0$  für alle  $n \neq 0$ , und  $\text{char}(K) = \min\{n \in \mathbb{N} \setminus \{0\} \mid n \cdot 1_K = 0_K\}$  andernfalls.

**Satz 2.2.13** Sei  $K$  ein Körper, dann gilt  $\text{char}(K) = 0$  oder  $\text{char}(K)$  ist eine Primzahl. □

*Beweis.* Angenommen dass  $\text{char}(K) \neq 0$ , seien  $n, m \in \mathbb{N}$  mit  $\text{char}(K) = nm$ . Dann gilt  $\text{char}(K) \cdot 1_K = (nm) \cdot 1_K = (n \cdot 1_K)(m \cdot 1_K)$  und aus Satz 2.2.4 folgt  $n \cdot 1_K = 0_K$  und  $m \cdot 1_K = 0_K$ . Aus der Definition folgt  $\text{char}(K) = n$  oder  $\text{char}(K) = m$ , dass heißt  $\text{char}(K)$  ist eine Primzahl. ■

## 2.3 Ringe

### 2.3.1 Definition und Beispiele

**Definition 2.3.1** Ein **Ring** ist ein geordnetes Paar  $(R, +, \cdot)$  mit  $R$  einer Menge und  $+, \cdot$  Verknüpfungen so dass die folgenden Eigenschaften erfüllt sind:

- $(R, +)$  ist eine kommutative Gruppe,
- es existiert ein **Einselement**  $1_R$  in  $R$  mit  $1_R \cdot x = x \cdot 1_R = x$  für alle  $x \in R$ ,
- die Verknüpfung  $\cdot$  ist associativ,
- für jeden  $x, y, z \in R$  gilt  $x(y + z) = xy + xz$  und  $(y + z)x = yx + zx$ .

**Definition 2.3.2** Ein Ring  $(R, +, \cdot)$  heißt **kommutativ** falls gilt:  $xy = yx$  für alle  $x, y \in R$

**Beispiel 2.3.3** Hier sind Beispiele von Ringe:

- $(\mathbb{Z}, +, \cdot)$ , ist ein kommutativer Ring.
- Ein Körper  $(K, +, \cdot)$  ist ein kommutativer Ring also sind  $(\mathbb{Q}, +, \cdot)$ ,  $(\mathbb{R}, +, \cdot)$  und  $(\mathbb{C}, +, \cdot)$  kommutative Ringe.

### 2.3.2 Unterringe

**Definition 2.3.4** Sei  $(R, +, \cdot)$  ein Ring und  $S \subset R$  eine Teilmenge, dann heißt  $S$  eine **Unterring** von  $R$  wenn gilt:

1.  $(S, +)$  ist eine Untergruppe von  $(R, +)$ ,
2.  $x, y \in S \Rightarrow xy \in S$ .
3.  $1 \in S$ .

**Satz 2.3.5** Sei  $S$  ein Unterring von  $(R, +, \cdot)$ , dann ist  $(S, +, \cdot)$  ein Ring. □

*Beweis.* Übung. ■

### 2.3.3 Ringhomomorphismus

**Definition 2.3.6** Seien  $(R, +, \cdot)$  und  $(R', +, \cdot)$  Ringe. Eine Abbildung  $f : R \rightarrow R'$  heißt **Ringhomomorphismus** wenn gilt:

1.  $f : (R, +) \rightarrow (R', +)$  ist ein Gruppenhomomorphismus.
2.  $f(1_R) = 1_{R'}$ .
3.  $f(xy) = f(x)f(y)$  für jeden  $x, y \in R$ .

#### Beispiel 2.3.7

1. Eine Körperhomomorphismus ist ein Ringhomomorphismus.
2. Sei  $K$  ein Körper, die Abbildung  $\mathbb{Z} \rightarrow K$  definiert durch  $n \mapsto n \cdot 1_K$  ist ein Ringhomomorphismus.

### 2.3.4 Die Ringe $\mathbb{Z}_n$

**Lemma 2.3.8 (Schulwissen)** Seien  $x, n \in \mathbb{Z}$ , mit  $n \neq 0$ . Dann existieren eindeutig bestimmte Elemente  $r, q \in \mathbb{Z}$  mit  $0 \leq r < n$  und  $x = qn + r$ .

Setze  $r_n(x) = r$ . □

**Definition 2.3.9** Sei  $n \in \mathbb{N}$  mit  $n \geq 2$  und sei  $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$ . Für  $x, y \in \mathbb{Z}_n$  sei  $x + y = r_n(x + y)$  und  $x \cdot y = r_n(xy)$ .

**Satz 2.3.10**  $(\mathbb{Z}_n, +, \cdot)$  ist ein kommutativer Ring. □

*Beweis.* Übung. ■

**Satz 2.3.11**  $(\mathbb{Z}_n, +, \cdot)$  ist ein Körper genau dann wenn  $n$  eine Primzahl ist. □

*Beweis.* Es gilt  $n \cdot 1_{\mathbb{Z}_n} = 0_{\mathbb{Z}_n}$  und  $m \cdot 1_{\mathbb{Z}_n} \neq 0_{\mathbb{Z}_n}$  für  $0 < m < n$ . Falls  $\mathbb{Z}_n$  ein Körper ist, gilt  $\text{char}(\mathbb{Z}_n) = n$  und  $n$  ist eine Primzahl.

Angenommen, dass  $n$  eine Primzahl ist, wir beweisen, dass jedem  $x \in \mathbb{Z}_n \setminus \{0_{\mathbb{Z}_n}\}$  ein inverses Element hat. Wir zeigen zuerst ein Lemma.

**Lemma 2.3.12** Sei  $n$  eine Primzahl ist. Dann ist  $\mathbb{Z}_n$  Nullteilerfrei, dass heißt: für  $x, y \in \mathbb{Z}_n$  mit  $x \cdot y = 0_{\mathbb{Z}_n}$  gilt  $x = 0_{\mathbb{Z}_n}$  oder  $y = 0_{\mathbb{Z}_n}$ . □

*Beweis.* Seien  $x, y \in \mathbb{Z}_n$  mit  $x \cdot y = 0_{\mathbb{Z}_n}$ . Dann ist  $xy$  ist durch  $n$  teilbar. Da  $n$  eine Primzahl ist, folgt:  $n$  teilt  $x$  oder  $y$ . Damit ist aber  $x = 0$  oder  $y = 0$ , da  $0 \leq x, y \leq n-1$ . ■

Sei nun  $x \in \mathbb{Z}_n \setminus \{0_{\mathbb{Z}_n}\}$ . Definiere eine Abbildung  $m_x : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$  durch  $m_x(y) = x \cdot y$ . Dann ist  $m_x$  injektiv: seien  $y, z$  mit  $m_x(y) = m_x(z)$ , es folgt  $x(y - z) = 0_{\mathbb{Z}_n}$ . Vom Lemma folgt  $y - z = 0_{\mathbb{Z}_n}$  und  $y = z$ .

Alle Elemente  $m_x(0), m_x(1), m_x(2), \dots, m_x(n-1)$  sind paarweise verschieden. Es sind dann  $n$  Elemente im Bild  $m_x(\mathbb{Z}_n)$  von  $m_x$ . Da  $\mathbb{Z}_n$  genau  $n$  Elemente hat gilt:  $m_x$  ist surjektiv. Insbesondere gilt: es gibt ein  $y \in \mathbb{Z}_n$  mit  $m_x(y) = 1_{\mathbb{Z}_n}$ . Dann ist  $y$  das inverses Element von  $x$  und  $\mathbb{Z}_n$  ist ein Körper. ■

# 3 Vektorräume und lineare Abbildungen

## 3.1 Vektorräume

### 3.1.1 Definitionen und Beispiele

**Definition 3.1.1** Sei  $K$  ein Körper. Ein **Vektorraum** über  $K$  (oder  $K$ -**Vektorraum**) ist eine Menge  $V$  zusammen mit zwei Abbildungen  $+: V \times V \rightarrow V$  (**Addition** genannt) und  $\cdot: K \times V \rightarrow V$  (**Skalarmultiplikation** genannt) mit den folgenden Eigenschaften:

- $(V, +)$  ist eine kommutative Gruppe,
- für alle  $x, y \in K$  und  $v \in V$ , es gilt  $(xy) \cdot v = x \cdot (y \cdot v)$ ,
- für alle  $v \in V$  gilt  $1_K \cdot v = v$ ,
- für alle  $x \in K$  und  $v_1, v_2 \in V$  es gilt  $x \cdot (v_1 + v_2) = x \cdot v_1 + x \cdot v_2$ .
- für alle  $x, y \in K$  und  $v \in V$  es gilt  $(x + y) \cdot v = x \cdot v + y \cdot v$ .

Die Elemente in  $V$  heißen **Vektoren**, die Elemente in  $K$  heißen **Skalare**. Das Nullelement  $0_v$  von  $(V, +)$  heißt **Nullvektor** (oder **die 0 von  $V$** ).

**Notation 3.1.2** Sei  $V$  ein  $K$ -Vektorraum man setze

- $v_1 - v_2 = v_1 + (-1) \cdot v_2$  für alle  $v_1, v_2 \in V$ ,
- $xv = x \cdot v$  für alle  $x \in K$  und  $v \in V$ .

**Beispiel 3.1.3** Sei  $K$  ein Körper.

1. Der **Nullvektorraum**  $V = \{0\}$  über  $K$  (für  $+$  und  $\cdot$  gibt es nur eine Möglichkeit). Man schreibt einfach  $V = 0$ .
2. Der Vektorraum  $V = K$ : Addition und Skalarmultiplikation sind durch Addition und Multiplikation von  $K$  definiert.

3. Sei  $V = K^n$  das  $n$ -fache Kartesische Produkt von  $K$ . Wir schreiben Elemente als Spalten:

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

wobei  $x_i \in K$ . Wir definieren  $+: V \times V \rightarrow V$  durch

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{pmatrix}$$

und  $\cdot: K \times V \rightarrow V$  durch

$$x \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} xx_1 \\ \vdots \\ xx_n \end{pmatrix}$$

Dann ist  $(V, +, \cdot)$  ein Vektorraum (siehe Übungsblatt 4).

4. Sei  $I$  eine Menge, dann ist  $K^I = \{\text{Abbildungen } f: I \rightarrow K\}$  ein Vektorraum, wobei für  $f, g \in K^I$  und  $x \in K$ , sind  $f + g$  und  $x \cdot f$  die Abbildungen definiert durch

$$(f + g)(i) = f(i) + g(i) \text{ und } (x \cdot f)(i) = xf(i)$$

für alle  $i \in I$ .

5. Sei  $L$  ein Körper so das  $K$  ein Teilkörper von  $L$  ist ( $K \subset L$ ). Dann ist  $L$  ein  $K$ -Vektorraum mit Addition und Skalarmultiplikation gegen durch Addition und Multiplikation von  $L$ .

Zum Beispiel sind  $\mathbb{R}$  und  $\mathbb{C}$  Vektorräume über  $\mathbb{Q}$  (und auch über  $\mathbb{R}$ ).

Der Körper  $\mathbb{Q}(\sqrt{2}) = \{x + y\sqrt{2} \in \mathbb{R} \mid x, y \in \mathbb{Q}\}$  ist ein  $\mathbb{Q}$ -Vektorraum.

6. Seien  $V$  und  $W$  zwei  $K$ -Vektorräume, dann ist  $V \times W$  auch ein  $K$ -Vektorraum wobei Addition und Skalarmultiplikation durch

$$(v_1, w_1) + (v_2, w_2) = (v_1 + v_2, w_1 + w_2) \text{ und } x \cdot (v, w) = (x \cdot v, x \cdot w)$$

gegeben sind.

**Definition 3.1.4** Seien  $V$  und  $W$  zwei Vektorräume. Der  $K$ -Vektorraum  $V \times W$  wird mit  $V \oplus W$  bezeichnet und heißt **(externe) direkte Summe** von  $V$  und  $W$ .



### 3.1.2 Unterräume

**Definition 3.1.5** Sei  $V$  ein  $K$ -Vektorraum, ein **Unterraum**  $W$  von  $V$  ist eine Teilmenge  $W$  von  $V$ , so dass gilt:

- $(W, +)$  ist eine Untergruppe von  $(V, +)$ ,
- $xw \in W$  für alle  $x \in K$  und  $w \in W$ .

**Lemma 3.1.6** Sei  $V$  ein  $K$ -Vektorraum und sei  $W$  ein Unterraum von  $V$ . Dann ist  $W$  ein  $K$ -Vektorraum mit Addition und Skalarmultiplikation durch Einschränkung der Addition und Skalarmultiplikation von  $V$  gegeben.  $\square$

*Beweis.* Übung. ■

**Beispiel 3.1.7** Sei  $K$  ein Körper.

1. Sei  $V$  ein  $K$ -Vektorraum, dann ist  $\{0_V\}$  ein Unterraum von  $V$ . Statt  $\{0_V\}$  schreibt man einfach  $0_V$  oder sogar  $0$ .

2. Sei  $V$  ein  $K$ -Vektorraum und sei  $v \in K$ . Dann ist  $\langle v \rangle = \{xv \in V \mid x \in K\}$  ein Unterraum von  $V$ . Für  $v = 0_V$  gilt  $\langle v \rangle = 0_V$ . Für  $v \neq 0_V$  heißt  $\langle v \rangle$  eine **Gerade** von  $V$ .

3. Seien  $W_1$  und  $W_2$  zwei Unterräume von ein  $K$ -Vektorraum  $V$ . Dann sind

$$W_1 \cap W_2 \quad \text{und} \quad W_1 + W_2 = \{w_1 + w_2 \in V \mid w_1 \in W_1 \text{ und } w_2 \in W_2\}$$

Unterräume.

4. Sei  $I$  eine Menge, dann ist

$$K^{(I)} = \{f \in K^I \mid f(i) \neq 0 \text{ für nur endliche viele } i \in I\}$$

ein Unterraum von  $K^I$ .

5. Für ein Intervall  $I$  in  $\mathbb{R}$ , dann ist

$$C^0(I) = \{f \in \mathbb{R}^I \mid f \text{ ist stetig}\}$$

ein Unterraum von  $\mathbb{R}^I$ .

**Definition 3.1.8** Sei  $V$  ein  $K$ -Vektorraum. Zwei Unterräume  $W_1$  und  $W_2$  sind in **direkte Summe** falls  $W_1 \cap W_2 = 0_V$ . In diesem Fall schreibt man  $W_1 \oplus W_2 = W_1 + W_2$  und nennt man  $W_1 \oplus W_2$  die **interne direkte Summe**.

## 3.2 Lineare Abbildungen

### 3.2.1 Definitionen und Beispiele

**Definition 3.2.1** Seien  $V$  und  $W$  zwei  $K$ -Vektorräume. Eine Abbildung  $f : V \rightarrow W$  heißt **linear** oder  **$K$ -linear** falls gilt:

- $f : (V, +) \rightarrow (W, +)$  ist ein Gruppenhomomorphismus,
- $f(x \cdot v) = x \cdot f(v)$  für alle  $x \in K$  und  $v \in V$ .

Eine lineare Abbildung heißt auch **Homomorphismus**. Falls  $W = V$ , heißt dann eine lineare Abbildung auch **Endomorphismus**.

**Definition 3.2.2** Seien  $V$  und  $W$  zwei  $K$ -Vektorräume. Wir definieren

$$\begin{aligned}\text{Hom}_K(V, W) &= \{f : V \rightarrow W \mid f \text{ ist ein Homomorphismus}\} \\ \text{End}_K(V) &= \text{Hom}_K(V, V).\end{aligned}$$

**Lemma 3.2.3** Seien  $V$  und  $W$  zwei  $K$ -Vektorräume. Eine Abbildung  $f : V \rightarrow W$  ist  **$K$ -linear** genau dann wenn

$$f(x_1v_1 + x_2v_2) = x_1f(v_1) + x_2f(v_2)$$

für alle  $x_1, x_2 \in K$  und  $v_1, v_2 \in V$ . □

*Beweis.* Siehe Übungsblatt 4. ■

**Definition 3.2.4** Sei  $f : V \rightarrow W$  eine lineare Abbildung.

1.  $f$  heißt **Monomorphismus** falls  $f$  injektiv ist.
2.  $f$  heißt **Epimorphismus** falls  $f$  surjektiv ist.
3.  $f$  heißt **Isomorphismus** falls  $f$  bijektiv ist.

**Lemma 3.2.5** Sei  $f : V \rightarrow W$  ein Isomorphismus, dann ist die Umkehrabbildung  $f^{-1} : W \rightarrow V$  auch ein Isomorphismus. □

*Beweis.* Siehe Übungsblatt 4. ■

**Definition 3.2.6** Zwei  $K$ -Vektorräume  $V$  und  $W$  heißen **isomorph** falls es ein Isomorphismus  $f : V \rightarrow W$  gibt. Dann schreibt man  $V \simeq W$ .

**Lemma 3.2.7** Sei  $f : V \rightarrow W$  dann gilt  $f(0) = 0$ . □

*Beweis.* Folgt aus Satz 2.1.12, weil  $f : (V, +) \rightarrow (W, +)$  ein Gruppenhomomorphismus ist. ■

**Lemma 3.2.8** Seien  $f : V \rightarrow W$  und  $g : W \rightarrow U$  zwei Homomorphismen dann ist  $g \circ f$  auch ein Homomorphismus.  $\square$

*Beweis.* Seien  $x_1, x_2 \in K$  und  $v_1, v_2 \in V$ , dann gilt

$$\begin{aligned} g \circ f(x_1 v_1 + x_2 v_2) &= g(f(x_1 v_1 + x_2 v_2)) = g(x_1 f(v_1) + x_2 f(v_2)) \\ &= x_1 g(f(v_1)) + x_2 g(f(v_2)) = x_1 g \circ f(v_1) + x_2 g \circ f(v_2). \end{aligned}$$

Aus Lemma 3.1.6 folgt, dass  $g \circ f$  ein Homomorphismus ist.  $\blacksquare$

**Beispiel 3.2.9** 1. Seien  $V$  und  $W$  zwei  $K$ -Vektorräume. Die **Nullabbildung**  $f : V \rightarrow W$  ist die Abbildung definiert durch  $f(v) = 0$  für alle  $v \in V$ . Die Nullabbildung ist linear. Man schreibt  $f = 0$ .

2. Sei  $V$  ein  $K$ -Vektorraum, die Identitätsabbildung  $\text{Id}_V$  ist linear.

3. Sei  $V$  ein  $K$ -Vektorraum und sei  $x \in K$ . Dann ist die Abbildung  $f_x : V \rightarrow V$ , welche definiert durch  $f_x(v) = xv$  ist, linear. Die Abbildung  $f_x$  heißt **Homothetie (oder zentrische Streckung)** von **Streckfaktor**  $x$ .

4. Die Abbildung  $K^2 \rightarrow K^2$  definiert durch

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}$$

wobei  $a, b, c, d \in K$ , ist linear.

4. Die Abbildung  $K \rightarrow K$ ,  $x \mapsto x^2$  ist nicht linear.

**Definition 3.2.10** Sei  $f : V \rightarrow W$  eine lineare Abbildung. Der **Kern** von  $f$  ist  $\ker(f) = \{v \in V \mid f(v) = 0\}$ .

**Bemerkung 3.2.11** Der Kern von einer linearen Abbildung  $f$  ist der Kern von  $f$  als Gruppenhomomorphismus  $f : (V, +) \rightarrow (W, +)$ .

**Lemma 3.2.12** Sei  $f : V \rightarrow W$  eine lineare Abbildung.

1.  $\ker(f)$  ist ein Unterraum von  $V$ .

2.  $f$  ist injektiv genau dann, wenn  $\ker(f) = 0$ .  $\square$

*Beweis.* 1. Seien  $v, v' \in \ker(f)$  und  $x \in K$ , dann gilt  $f(v + v') = f(v) + f(v') = 0$  i.e.  $v + v' \in \ker(f)$  und  $f(xv) = xf(v) = 0$  i.e.  $xv \in \ker(f)$ .

2. Folgt aus Satz 2.1.15, weil  $f : (V, +) \rightarrow (W, +)$  ein Gruppenhomomorphismus ist.  $\blacksquare$

**Lemma 3.2.13** Sei  $f : V \rightarrow W$  eine lineare Abbildung und seien  $V' \subset V$  und  $W' \subset W$  Unterräume.

1. Dann ist  $f(V')$  ein Unterraum von  $W$ .

2. Dann ist  $f^{-1}(W')$  ein Unterraum von  $V$ .  $\square$

*Beweis.* 1. Seien  $w, w' \in f(V')$  und sei  $x \in K$ . Aus der Definition von  $f(V')$ , gibt es  $v, v' \in V'$  so dass,  $f(v) = w$  und  $f(v') = w'$ . Dann gilt  $w + w' = f(v) + f(v') = f(v + v') \in f(V')$ , weil  $v + v' \in V'$ . Es gilt auch  $xw = xf(v) = f(xv) \in f(V')$ , weil  $xv \in V'$ .

2. Seien  $v, v' \in f^{-1}(W')$  und sei  $x \in K$ . Aus der Definition, gilt  $f(v) \in W'$  und  $f(v') \in W'$ . Dann gilt  $f(v + v') = f(v) + f(v') \in W'$ . Es gilt auch  $f(xv) = xf(v) \in W'$ . ■

# 4 Linear Unabhängigkeit

## 4.1 Linearkombinationen

**Definition 4.1.1** Sei  $V$  ein  $K$ -Vektorraum und seien  $v_1, \dots, v_m \in V$ . Dann ist  $v \in V$  eine **Linearkombination von**  $v_1, \dots, v_m$  falls es Skalar  $x_1, \dots, x_m \in K$  gibt mit

$$v = \sum_{i=1}^m x_i v_i = x_1 v_1 + \dots + x_m v_m.$$

**Beispiel 4.1.2** 1. Der Nullvektor ist eine Linearkombination von alle Vektoren  $v_1, \dots, v_m \in V$ : es gibt Skalar:  $x_1 = \dots = x_m = 0$  so dass  $0_V = \sum_i 0 \cdot v_i = \sum_i x_i v_i$ .

2. Seien  $v_1, v_2, v_3 \in \mathbb{Q}^2$  mit

$$v_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, v_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \text{ und } v_3 = \begin{pmatrix} -1 \\ 1 \end{pmatrix}$$

und sei

$$v = \begin{pmatrix} 2 \\ 1 \end{pmatrix}.$$

Dann gilt  $v = 2 \cdot v_1 + 1 \cdot v_2 + 0 \cdot v_3 = 3 \cdot v_1 + 0 \cdot v_2 + 1 \cdot v_3$  und  $v$  ist eine Linearkombination von  $v_1, v_2, v_3$ . Man kann hier schon bemerken, dass Linearkombinationen nicht immer eindeutig sind.

**Definition 4.1.3** Sei  $V$  ein  $K$ -Vektorraum. Die **lineare Hülle** einer Teilmenge  $M$  von  $V$  ist definiert als:

$$\langle M \rangle := \{v \in V \mid v \text{ ist eine Linearkombination von Vektoren in } M\}.$$

(Wir setzen  $\langle \emptyset \rangle = \{0\}$ ). Wir schreiben  $\langle v_1, \dots, v_m \rangle$  für  $\langle \{v_1, \dots, v_m\} \rangle$ .

**Lemma 4.1.4** Die lineare Hülle  $\langle M \rangle$  ist ein Unterraum. □

*Beweis.* Der Nullvektor ist immer eine Linearkombination also  $0_V \in \langle M \rangle$ . Seien  $v, w \in \langle M \rangle$ . Dann gibt es Elemente  $v_1, \dots, v_m \in M$  und Elemente  $w_1, \dots, w_l \in M$  und Skalare  $x_1, \dots, x_m, y_1, \dots, y_l \in K$  so dass:

$$v = \sum_{i=1}^m x_i v_i \text{ und } w = \sum_{j=1}^l y_j w_j.$$

Dann gilt

$$v + w = \sum_{i=1}^m x_i v_i + \sum_{j=1}^l y_j w_j$$

i.e.  $v + w \in \langle M \rangle$ . Für  $x \in K$  gilt auch

$$xv = x \sum_{i=1}^m x_i v_i = \sum_{i=1}^m (xx_i) v_i$$

i.e.  $xv \in \langle M \rangle$ . ■

**Definition 4.1.5** Sei  $U$  ein Unterraum von  $V$  ein  $K$ -Vektorraum. Eine Teilmenge  $M$  von  $U$  **erzeugt**  $U$  falls  $\langle M \rangle = U$ . In diesem fall heißt  $M$  ein **Erzeugendensystem (EVS)** von  $U$ .

**Definition 4.1.6** Ein Vektorraum  $V$  ist **endlich erzeugt**, falls  $V = \langle M \rangle$  mit  $M$  einer endlichen Teilmenge von  $V$ .

**Beispiel 4.1.7** 1.  $\{0\} = \langle \emptyset \rangle$  i.e.  $\emptyset$  ist ein EVS von  $V = \{0\}$ .

2. Es gilt  $K^2 = \langle v_1, v_2 \rangle$  i.e.  $\{v_1, v_2\}$  ist ein EVS von  $K^2$  wobei

$$v_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ und } v_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

2. Sei  $v \in K^2$ , dann ist  $\{v_1, v_2, v\}$  ein EVS von  $K^2$ .

3. Seien  $1, \sqrt{2} \in \mathbb{Q}(\sqrt{2}) = \{x + y\sqrt{2} \mid x, y \in \mathbb{Q}\}$ . Dann ist  $(1, \sqrt{2})$  ein EVS von  $\mathbb{Q}(\sqrt{2})$  über  $\mathbb{Q}$ .

**Lemma 4.1.8** Sei  $I$  eine unendliche Menge, dann ist  $K^{(I)}$  nicht endlich erzeugt. □

*Beweis.* Per Definitionem gilt

$$K^{(I)} = \{f : I \rightarrow K \mid f(i) \neq 0 \text{ nur für endliche viele } i \in I\}.$$

Nehmen wir an, dass es Elemente  $f_1, \dots, f_n \in K^{(I)}$  gibt so dass  $K^{(I)} = \langle f_1, \dots, f_n \rangle$ . Sei

$$J = \{j \in I \mid f_i(j) \neq 0 \text{ für ein } i \text{ mit } 1 \leq i \leq n\}.$$

Dann ist  $J$  endlich. Da  $I$  unendlich ist gibt es ein Element  $k \in I \setminus J$ . Sei  $f : I \rightarrow K$  definiert durch

$$f(i) = \delta_{i,k} = \begin{cases} 1 & \text{falls } i = k \\ 0 & \text{andernfalls.} \end{cases}$$

Es gilt  $f \in K^{(I)}$  aber  $f \notin \langle f_1, \dots, f_n \rangle$ . ■

## 4.2 Linear Unabhängigkeit

**Definition 4.2.1** 1. Ein  $n$ -Tupel  $(v_1, \dots, v_n)$  von Vektoren in  $V$  heißt ein **Vektorsystem**.

2. Ein Vektorsystem  $(v_1, \dots, v_n)$  heißt **linear abhängig**, falls es Skalare  $x_1, \dots, x_n \in K$  gibt, welche nicht alle gleich 0 sind (i.e.  $(x_1, \dots, x_n) \neq (0, \dots, 0)$ ), mit

$$\sum_{i=1}^n x_i v_i = 0.$$

Andernfalls heißt  $(v_1, \dots, v_n)$  **linear unabhängig**.

**Definition 4.2.2** Eine Teilmenge  $M \subset V$  heißt **linear unabhängig**, falls alle Vektorsysteme  $(v_1, \dots, v_n)$  mit  $v_1, \dots, v_n \in M$  linear unabhängig sind. Andernfalls, heißt  $M$  **linear abhängig**.

Die leere Menge ist immer linear unabhängig.

**Beispiel 4.2.3** 1. Sei  $v \in V$ , dann ist  $\{v\}$  genau dann linear unabhängig, wenn  $v \neq 0$ .

2. Sei  $v \in V$ , dann ist  $(v, v)$  linear abhängig.

3. Seien  $v_1, v_2 \in V$ , dann ist  $(v_1, v_2)$  linear abhängig genau dann wenn es  $x_1, x_2 \in K$  gibt, die nicht beide gleich nul sind, mit  $x_1 v_1 + x_2 v_2 = 0$ .

Gilt  $v_1 \neq 0$  und  $v_2 \neq 0$ , dann ist  $(v_1, v_2)$  linear abhängig genau dann wenn  $Kv_1 = Kv_2$  wobei  $Kv_i = \{xv_i \mid x \in K\}$ .

4. 2. Seien  $v_1, v_2, v_3 \in \mathbb{Q}^2$  mit

$$v_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, v_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \text{ und } v_3 = \begin{pmatrix} -1 \\ 1 \end{pmatrix}.$$

Dann ist  $(v_1, v_2, v_3)$  linear abhängig, weil  $1 \cdot v_1 + (-1) \cdot v_2 + 1 \cdot v_3 = 0$ .

5.  $(1, \sqrt{2})$  ist in  $\mathbb{Q}(\sqrt{2})$  linear unabhängig (als  $\mathbb{Q}$ -Vektorraum): seien  $x, y \in \mathbb{Q}$  mit  $x \cdot 1 + y\sqrt{2} = 0$ . Fall  $y \neq 0$  gilt  $\sqrt{2} = \frac{x}{y} \in \mathbb{Q}$  ein Widerspruch also gilt  $y = 0$  und dann  $x = 0$ .

**Lemma 4.2.4** Sei  $(v_1, \dots, v_n)$  ein linear unabhängiges System, dann ist ein Untersystem  $(v_{i_1}, \dots, v_{i_k})$  von  $(v_1, \dots, v_n)$  auch linear unabhängig.  $\square$

*Beweis.* Seien Skalare  $x_{i_1}, \dots, x_{i_k}$  so dass

$$x_{i_1}v_{i_1} + \dots + x_{i_k}v_{i_k} = \sum_{j=1}^k x_{i_j}v_{i_j} = 0.$$

Dann setzen wir  $x_i = 0$  für  $i \in \{1, \dots, n\} \setminus \{i_1, \dots, i_k\}$ . Es gilt

$$x_1v_1 + \dots + x_nv_n = \sum_{j=1}^n x_jv_j = 0.$$

Als  $(v_1, \dots, v_n)$  linear unabhängig ist gilt  $x_1 = \dots = x_n = 0$  so dass  $x_{i_1} = \dots = x_{i_k} = 0$  und  $(v_{i_1}, \dots, v_{i_k})$  ist linear unabhängig. ■

**Lemma 4.2.5** Sei  $V$  ein Vektorraum.

1. Sei  $(v_1, \dots, v_m, v)$  ein linear abhängiges Vektorsystem. Ist  $(v_1, \dots, v_m)$  linear unabhängig, dann gilt  $v \in \langle v_1, \dots, v_m \rangle$ .
2. Sei  $M \cup \{v\}$  linear abhängig wobei  $M \subset V$  und  $v \in V$ . Ist  $M$  linear unabhängig, dann gilt  $v \in \langle M \rangle$ . □

*Beweis.* 1. Es gibt Skalare  $(x_1, \dots, x_m, x)$ , nicht alle gleich 0, so dass

$$x_1v_1 + \dots + x_mv_m + xv = 0.$$

Falls  $x = 0$  dann gilt  $x_1v_1 + \dots + x_mv_m = 0$  mit  $x_1, \dots, x_m$  nicht alle gleich 0 i.e.  $(v_1, \dots, v_m)$  ist linear abhängig. Ein Widerspruch. Also ist  $x \neq 0$  und wir haben

$$x = \frac{x_1}{x}v_1 + \dots + \frac{x_m}{x}v_m \in \langle v_1, \dots, v_m \rangle.$$

2. Es gibt Elemente  $v_1, \dots, v_m \in M$ , so dass  $(v_1, \dots, v_m, v)$  ein linear abhängiges Vektorsystem ist. Aber als  $M$  linear unabhängig ist, ist  $(v_1, \dots, v_m)$  linear unabhängig, dann gilt aus 1, dass  $w \in \langle v_1, \dots, v_m \rangle \subset \langle M \rangle$ . ■

**Korollar 4.2.6** Sei  $M \subset V$  linear unabhängig und sei  $v \in V$  mit  $v \notin \langle M \rangle$ , dann ist  $M \cup \{v\}$  linear unabhängig.

**Lemma 4.2.7** Sei  $V$  ein Vektorraum so dass  $V$  nicht endlich erzeugt ist.

Dann gibt es für jedes  $n \in \mathbb{N}$  ein  $n$ -elementige Teilmenge  $M_n$  von  $V$  mit  $M_n$  linear unabhängig und  $M_0 \subset M_1 \subset M_2 \subset \dots$ . □

*Beweis.* Wir konstruieren  $M_n$  per Induktion. Sei  $M_0 = \emptyset$ , die leere Menge ist linear unabhängig. Sei  $M_n$  schon definiert. Da  $V$  nicht endlich erzeugt ist gilt  $\langle M_n \rangle \neq V$ . Sei  $v \in V \setminus \langle M_n \rangle$ . Dann ist  $M_{n+1} = M_n \cup \{v\}$  linear unabhängig (siehe Korollar oben) und hat  $n + 1$  Elemente. ■



**Satz 4.2.8** Seien  $v_1, \dots, v_m \in V$ . Dann ist äquivalent

1. Die Vektoren sind linear unabhängig.
2. Ist  $v = x_1 v_1 + \dots + x_m v_m$  eine Darstellung eines Elementes  $v \in \langle v_1, \dots, v_m \rangle$  mit Koeffizienten  $x_1, \dots, x_m \in K$ , so sind diese eindeutig durch  $v$  bestimmt.  $\square$

*Beweis.* (1.  $\Rightarrow$  2.) Seien  $v = x_1 v_1 + \dots + x_m v_m$  und  $v = x'_1 v_1 + \dots + x'_m v_m$  zwei Darstellungen. Dann gilt  $(x_1 - x'_1)v_1 + \dots + (x_m - x'_m)v_m = 0$  und weil  $(v_1, \dots, v_m)$  linear unabhängig ist gilt  $x_1 = x'_1, \dots, x_m = x'_m$ . Die zwei Darstellungen sind gleich.

(2.  $\Rightarrow$  1.) Seien  $x_1, \dots, x_m \in K$  mit  $x_1 v_1 + \dots + x_m v_m = 0$ . Dann gibt es auch eine weitere Darstellung  $0 \cdot v_1 + \dots + 0 \cdot v_m = 0$  von  $0 \in V$ . Diese zwei Darstellungen sind gleich i.e.  $x_1 = 0, \dots, x_m = 0$ .  $\blacksquare$

# 5 Basen und Dimension

## 5.1 Definition und Beispiele

**Definition 5.1.1** Sei  $V$  ein  $K$ -Vektorraum

1. Ein System  $(v_1, \dots, v_n)$  von Vektoren, heißt eine (**endliche**) **Basis** wenn
  - $(v_1, \dots, v_n)$  ein EZS ist und
  - $(v_1, \dots, v_n)$  linear unabhängig sind.
2. Ein System  $(v_i)_{i \in I}$  (gegebenfalls  $I$  unendlich) von Vektoren, heißt eine **Basis** wenn
  - $(v_i)_{i \in I}$  ein EZS ist und
  - $(v_i)_{i \in I}$  linear unabhängig sind.

**Beispiel 5.1.2** 1. Die leere Menge  $\emptyset$  ist die einzige basis von  $V = 0$ .

2. Sei  $V = K^n$ . Für  $i \in \mathbb{N}$  mit  $0 \leq i \leq n$ , sei  $e_i \in V$  definiert als

$$e_i = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

wo die Eins auf die  $i$ -te Zeile ist. Dann ist  $(e_1, \dots, e_n)$  eine Basis von  $V$ . Diese Basis heißt **Standardbasis von  $K^n$** .

3. Sei  $V = \mathbb{Q}(\sqrt{2})$ . Dann ist  $V$  ein  $\mathbb{Q}$ -Vektorraum und  $(1, \sqrt{2})$  ist eine Basis von  $V$ .

**Satz 5.1.3** Ein System  $(v_1, \dots, v_n)$  von Vektoren, ist eine Basis genau dann, wenn für alle Vektoren  $v \in V$  es genau eine Darstellung

$$v = \sum_{i=1}^n x_i v_i$$

gibt, wobei  $x_i$  in  $K$  für alle  $i$  ist.

□

*Beweis.* Alle Vektoren  $v \in V$  haben eine Darstellung

$$v = \sum_{i=1}^n x_i v_i$$

genau dann, wenn  $(v_1, \dots, v_n)$  ein EZS ist. Nach Satz 4.2.8 ist die Darstellung eindeutig genau dann, wenn  $(v_1, \dots, v_n)$  linear unabhängig sind. ■

## 5.2 Basen und Abbildungen

**Satz 5.2.1** Sei  $(v_1, \dots, v_n)$  eine Basis von  $V$ . Dann gilt  $V \simeq K^n$ . □

*Beweis.* Sei  $f : K^n \rightarrow V$  definiert als

$$f \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \sum_{i=1}^n x_i v_i.$$

Wir zeigen, dass  $f$  ein Isomorphismus ist. Zuerst zeigen wir, dass  $f$  linear ist. Es gilt

$$\begin{aligned} f \left( x \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + y \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \right) &= f \begin{pmatrix} xx_1 + yy_1 \\ \vdots \\ xx_n + yy_n \end{pmatrix} = \sum_{i=1}^n (xx_i v_i + yy_i v_i) \\ &= x \sum_{i=1}^n x_i v_i + y \sum_{i=1}^n y_i v_i = xf \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + yf \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}. \end{aligned}$$

Nach Lemma 3.2.3 ist dann  $f$  linear. Sei  $(x_1, \dots, x_n) \in \ker(f)$ , dann gilt

$$\sum_{i=1}^n x_i v_i = 0$$

und als  $(v_1, \dots, v_n)$  linear unabhängig sind gilt  $(x_1, \dots, x_n) = (0, \dots, 0) = 0_{K^n}$ . Also ist  $f$  injektiv. Das Bild von  $f$  ist  $\langle v_1, \dots, v_n \rangle$  und weil  $(v_1, \dots, v_n)$  ein EZS ist, ist  $f$  surjektiv. ■

**Korollar 5.2.2** Sei  $V$  ein Vektorraum und sei  $(v_1, \dots, v_n)$  eine Basis.

1. Seien  $f : V \rightarrow W$  und  $g : V \rightarrow W$  zwei lineare Abbildungen. Es gilt  $f = g$  genau dann, wenn  $f(v_i) = g(v_i)$  für alle  $1 \leq i \leq n$ .
2. Seien  $w_1, \dots, w_n$  Vektoren in ein Vektorraum  $W$ , es gibt genau eine lineare Abbildung  $f : V \rightarrow W$  mit  $f(v_i) = w_i$  für alle  $1 \leq i \leq n$ .

*Beweis.* 1. Falls  $f = g$ , dann gilt  $f(v_i) = g(v_i)$  für alle  $1 \leq i \leq n$ . Umgekehrt, Falls  $f(v_i) = g(v_i)$  für alle  $1 \leq i \leq n$ , sei  $v \in V$ , dann gibt es Elemente  $x_1, \dots, x_n \in K$  mit  $v = x_1 v_1 + \dots + x_n v_n$  und es gilt

$$f(v) = \sum_{i=1}^n x_i f(v_i) = \sum_{i=1}^n x_i g(v_i) = g(v).$$

2. Eindeutigkeit folgt von 1. Sei  $v \in V$ , dann gibt es eindeutig bestimmte Elemente  $x_1, \dots, x_n \in K$  mit  $v = x_1 v_1 + \dots + x_n v_n$  und wir definieren

$$f(v) = \sum_{i=1}^n x_i f(v_i) = \sum_{i=1}^n x_i w_i \in W.$$

Eine einfache Rechnung zeigt, dass  $f$  linear ist. ■

**Satz 5.2.3** Sei  $f : V \rightarrow W$  eine lineare Abbildung und sei  $(v_1, \dots, v_n)$  eine Basis von  $V$ .

1.  $f$  ist injektiv genau dann, wenn  $(f(v_1), \dots, f(v_n))$  linear unabhängig ist.
2.  $f$  ist surjektiv genau dann, wenn  $(f(v_1), \dots, f(v_n))$  ein EZS ist.
3.  $f$  ist bijektiv genau dann, wenn  $(f(v_1), \dots, f(v_n))$  eine Basis ist. □

*Beweis.* Siehe Übungsblatt 6. ■

## 5.3 Existenz

**Satz 5.3.1** Jeder endlich erzeugte Vektorraum besitzt eine Basis und jede solche Basis ist endlich. □

*Beweis.* Sei  $(v_1, \dots, v_n)$  ein EZS von  $V$  mit  $n$  minimal *i.e.* es gibt kein EZS mit weniger als  $n$  Elemente. Falls  $(v_1, \dots, v_n)$  linear unabhängig ist, ist  $(v_1, \dots, v_n)$  eine Basis. Andernfalls gibt es ein  $k < n$  so dass  $(v_1, \dots, v_k)$  linear unabhängig ist und  $(v_1, \dots, v_k, v_{k+1})$  linear abhängig ist. Nach Lemma 4.2.5.1. gilt  $v_{k+1} \in \langle v_1, \dots, v_k \rangle$ . Also ist  $(v_1, \dots, \widehat{v_k}, \dots, v_n) = (v_1, \dots, v_k, v_{k+2}, \dots, v_n)$  ein EZS. Ein Widerspruch als  $n$  minimal war. ■

**Satz 5.3.2** Sei  $V$  ein Vektorraum und  $(v_1, \dots, v_n)$  ein System von Vektoren aus  $V$ . Dann ist äquivalent:

1.  $(v_1, \dots, v_n)$  bildet eine Basis,
2.  $(v_1, \dots, v_n)$  ist ein maximales linear unabhängiges System,
3.  $(v_1, \dots, v_n)$  ist ein minimales EZS. □

*Beweis.* ( $1 \Rightarrow 2$ ) Angenommen  $(v_1, \dots, v_n)$  sei eine Basis, dann ist  $(v_1, \dots, v_n)$  linear unabhängig. Wenn  $(v_1, \dots, v_n)$  nicht maximal wäre, dann würde es ein Vektor  $v \in V$  geben, so dass  $(v_1, \dots, v_n, v)$  linear unabhängig ist. Aber als  $(v_1, \dots, v_n)$  eine Basis ist gilt  $v \in \langle v_1, \dots, v_n \rangle$  i.e. es gibt Skalare  $(x_1, \dots, x_n) \in K^n$  mit

$$v = \sum_{i=1}^n x_i v_i \text{ das heißt } -v + \sum_{i=1}^n x_i v_i = 0$$

und  $(v_1, \dots, v_n, v)$  ist linear abhängig, ein Widerspruch.

( $2 \Rightarrow 1$ ) Angenommen  $(v_1, \dots, v_n)$  sei maximales linear unabhängiges System und sei  $v \in V$ . Dann ist  $(v_1, \dots, v_n, v)$  linear abhängig und aus Lemma 4.2.5.1. gilt  $v \in \langle v_1, \dots, v_n \rangle$ . Also ist  $(v_1, \dots, v_n)$  ein EZS und eine basis.

( $1 \Rightarrow 3$ ) Angenommen  $(v_1, \dots, v_n)$  sei eine Basis, dann ist  $(v_1, \dots, v_n)$  ein EZS. Wenn  $(v_1, \dots, v_n)$  nicht minimal wäre, dann würde es ein Vektor  $v_k$  geben, so dass  $(v_1, \dots, \widehat{v_k}, \dots, v_n)$  ein EZS ist. Dann gilt  $v_k \in \langle v_1, \dots, \widehat{v_k}, \dots, v_n \rangle$  i.e. es gibt Skalare  $(x_1, \dots, \widehat{x_k}, \dots, x_n) \in K^{n-1}$  mit

$$v_k = \sum_{i=1, i \neq k}^n x_i v_i \text{ das heißt } -v_k + \sum_{i=1, i \neq k}^n x_i v_i = 0$$

und  $(v_1, \dots, v_n)$  ist linear abhängig, ein Widerspruch.

( $3 \Rightarrow 1$ ) Angenommen  $(v_1, \dots, v_n)$  sei ein minimales EZS. Falls  $(v_1, \dots, v_n)$  linear abhängig ist, dann gibt es gibt Skalare  $(x_1, \dots, x_n) \in K^n$  nicht alle nul mit

$$\sum_{i=1}^n x_i v_i = 0.$$

Sei  $k$  mit  $x_k \neq 0$ , dann gilt

$$v_k = - \sum_{i=1, i \neq k}^n \frac{x_i}{x_k} v_i,$$

also gilt  $v_k \in \langle v_1, \dots, \widehat{v_k}, \dots, v_n \rangle$  und  $\langle v_1, \dots, \widehat{v_k}, \dots, v_n \rangle = \langle v_1, \dots, v_n \rangle$  ein Widerspruch als  $(v_1, \dots, v_n)$  ein minimales EZS war. ■

**Satz 5.3.3 (Basisergänzungssatz)** Sei  $(v_1, \dots, v_r)$  ein linear unabhängiges system und sei  $(w_1, \dots, w_m)$  ein EZS. Dann lässt sich  $(v_1, \dots, v_r)$  durch Elemente in  $(w_1, \dots, w_m)$  zu einer Basis ergänzen, i.e. es gibt paarweise verschiedene Indizes  $i_1, \dots, i_k \in \{1, \dots, m\}$  so dass

$$(v_1, \dots, v_r, w_{i_1}, \dots, w_{i_k})$$

eine Basis bildet. □

*Beweis.* Sei  $(w_{i_1}, \dots, w_{i_k})$  minimal so dass  $(v_1, \dots, v_r, w_{i_1}, \dots, w_{i_k})$  ein EZS ist. Wir zeigen, dass  $(v_1, \dots, v_r, w_{i_1}, \dots, w_{i_k})$  linear unabhängig ist. Wenn nicht, würde das System  $(v_1, \dots, v_r, w_{i_1}, \dots, w_{i_k})$  linear abhängig sein. Dann würde es Skalare, die nicht alle nul sind,  $(x_1, \dots, x_r, y_{i_1}, \dots, y_{i_k})$  geben mit

$$\sum_{j=1}^r x_j v_j + \sum_{j=1}^k y_{i_j} w_{i_j} = 0.$$

Da  $(v_1, \dots, v_n)$  linear unabhängig ist gibt es ein  $j_0$  mit  $y_{i_{j_0}} \neq 0$ . Es gilt

$$w_{j_0} = - \sum_{j=1}^r x_j v_j - \sum_{j=1, j \neq j_0}^k y_{i_j} w_{i_j}$$

also  $w_{j_0} \in \langle v_1, \dots, v_r, w_{i_1}, \dots, \widehat{w}_{j_0}, \dots, w_{i_k} \rangle$  und  $\langle v_1, \dots, v_r, w_{i_1}, \dots, \widehat{w}_{j_0}, \dots, w_{i_k} \rangle$  ist ein EZS. Ein Widerspruch weil  $(w_{i_1}, \dots, w_{i_k})$  minimal war, so dass das System  $(v_1, \dots, v_r, w_{i_1}, \dots, w_{i_k})$  ein EZS ist. ■

**Theorem 5.3.1** Sei  $(v_1, \dots, v_r)$  eine linear unabhängiges system, sei  $(w_1, \dots, w_m)$  ein EZS und sei  $(e_1, \dots, e_n)$  eine Basis. Dann gilt  $r \leq n \leq m$ . □

*Beweis.* Das System  $(e_2, \dots, e_n)$  ist linear unabhängig und kann, dank Basisergänzungssatz, mit Elemente  $(w_{i_1}, \dots, w_{i_{k_1}})$  aus dem EZS  $(w_1, \dots, w_m)$  in eine Basis  $(w_{i_1}, \dots, w_{i_{k_1}}, e_2, \dots, e_n)$  ergänz werden. Da  $e_1 \notin \langle e_2, \dots, e_n \rangle$  ist  $k_1 \geq 1$ .

Dann ist  $(w_{i_1}, \dots, w_{i_{k_1}}, e_3, \dots, e_n)$  auch linear unabhängig und kann, dank Basisergänzungssatz, mit Elemente  $(w_{i_{k_1+1}}, \dots, w_{i_{k_1+k_2}})$  aus  $(w_1, \dots, w_m)$  in eine Basis  $(w_{i_1}, \dots, w_{i_{k_1}}, w_{i_{k_1+1}}, \dots, w_{i_{k_1+k_2}}, e_3, \dots, e_n)$  ergänz werden mit  $k_2 \geq 1$ . Wenn wir alle Elemente  $e_i$  ersetzen haben wir eine Basis

$$(w_{i_1}, \dots, w_{i_{k_1}}, w_{i_{k_1+1}}, \dots, w_{i_{k_1+k_2}}, \dots, w_{i_{k_1+\dots+k_{n-1}+1}}, \dots, w_{i_{k_1+\dots+k_n}}).$$

Es gibt also  $k_1 + \dots + k_n \leq m$  und als  $k_i \geq 1$  für alle  $i$  gilt  $n \leq m$ .

Dank Basisergänzungssatz gibt es Elemente  $(e_{i_1}, \dots, e_{i_k})$  aus dem EZS  $(e_1, \dots, e_n)$  so dass  $(v_1, \dots, v_r, e_{i_1}, \dots, e_{i_k})$  eine Basis ist. Dann ist  $(v_1, \dots, v_r, e_{i_1}, \dots, w_{i_k})$  eine Basis und  $(e_1, \dots, e_n)$  ein EZS, so dass  $r + k \leq n$  also  $r \leq n$ . ■

**Korollar 5.3.4** Sei  $V$  ein endlich erzeugten Vektorraum. Jede zwei Basen bestehen aus gleichviel Elementen.

*Beweis.* Seien  $(v_1, \dots, v_n)$  und  $(e_1, \dots, e_m)$  zwei basen. Dann sind beide Systeme auch EZS und linear unabhängig. Es gilt also  $n \leq m$  und  $m \leq n$  aus Theorem 5.3.1. ■

## 5.4 Dimension

**Definition 5.4.1** Sei  $V$  ein endlich erzeugten Vektorraum. Die Anzahl von Elementen in jeder Basis heißt **die Dimension** von  $V$  und ist  $\dim V$  oder  $\dim_K V$  bezeichnet.

Wenn  $V$  nicht endlich erzeugt ist, sagt man das  $V$  **unendlich dimensional** ist und schreibt man  $\dim_K V = \infty$ .

**Korollar 5.4.2** Sei  $V$  ein Vektorraum und  $n \in \mathbb{N}$ . Dann ist äquivalent:

1.  $\dim V = n$ ,
2. es existiert ein linear unabhängiges System von  $n$  Vektoren und alle Systeme von mehr als  $n + 1$  Vektoren sind linear abhängig.

*Beweis.* (1.  $\Rightarrow$  2.) Es gibt eine Basis  $(e_1, \dots, e_n)$  mit  $n$  Elemente, insbesondere gibt es ein linear unabhängiges System  $(e_1, \dots, e_n)$  von  $n$  Vektoren. Sei  $(v_1, \dots, v_r)$  ein linear unabhängiges System, dann gilt aus Theorem 5.3.1  $r \leq n$ . Also sind alle Systeme von mehr als  $n + 1$  Vektoren linear abhängig.

(2.  $\Rightarrow$  1.) Es gibt in  $V$  ein maximales unabhängiges System von  $n$  Vektoren. Also eine Basis mit  $n$  Vektoren, und es folgt  $\dim V = n$ . ■

**Korollar 5.4.3** Sei  $V$  ein Vektorraum und  $n \in \mathbb{N}$ . Dann ist äquivalent:

1.  $\dim V \geq n$ ,
2. es existiert ein linear unabhängiges System von  $n$  Vektoren.

*Beweis.* (1.  $\Rightarrow$  2.) Falls  $\dim V \neq \infty$ , dann gibt es eine Basis mit  $\dim V$  Elemente und diese Basis ist ein linear unabhängiges System. Ein Untersystem mit  $n$  Elemente ist auch linear unabhängig nach Lemma 4.2.4.

Falls  $\dim V = \infty$ , dann gilt nach Lemma 4.2.7, dass es ein linear unabhängiges System mit  $n$  Elemente gibt.

(2.  $\Rightarrow$  1.) Falls  $\dim V = \infty$  dann gilt  $\dim V \geq n$ . Andernfalls, gibt es eine Basis mit  $\dim V$  Elemente. Nach Theorem 5.3.1 gilt  $n \leq \dim V$ . ■

**Korollar 5.4.4** Sei  $V$  ein Vektorraum mit  $\dim V < \infty$ .

1. Ein unabhängiges System mit  $\dim V$  Elemente ist eine Basis.
2. Ein EZS mit  $\dim V$  Elemente ist eine Basis.

*Beweis.* Wir setzen  $n = \dim V$  und betrachten eine Basis  $(e_1, \dots, e_n)$ .

1. Sei  $(v_1, \dots, v_n)$  ein unabhängiges System, dann können wir  $(v_1, \dots, v_n)$  mit  $(e_1, \dots, e_n)$  ergänzen, um eine Basis zu bilden. Aber Basen haben  $n$  Elemente *i.e.*  $(v_1, \dots, v_n)$  war schon eine Basis.

2. Das leere System ist ein unabhängiges System und kann mit  $(v_1, \dots, v_n)$  ergänzt werden, um eine Basis zu bilden. Diese Basis hat genau  $n$  Elemente *i.e.* die Ergänzung war  $(v_1, \dots, v_n)$  und  $(v_1, \dots, v_n)$  ist eine Basis. ■

**Korollar 5.4.5** Sei  $U$  ein Unterraum in  $V$ , dann gilt  $\dim U \leq \dim V$ . Gleichheit gilt genau dann, wenn  $U = V$ .

*Beweis.* Falls  $\dim V = \infty$  sind wir schon fertig. Andernfalls, gibt eine Basis mit  $\dim V$  Elemente in  $V$ . Sei  $(v_1, \dots, v_r)$  ein unabhängiges System in  $U$ . Dann ist  $(v_1, \dots, v_r)$  auch ein unabhängiges System in  $V$ . Nach Theorem 5.3.1 gilt  $r \leq \dim V$ . Es gilt also ein maximales unabhängiges System in  $U$  *i.e.* eine Basis in  $U$ . Diese Basis besteht aus  $\dim U$  Elementen und ist linear unabhängig. Dann gilt  $\dim U \leq \dim V$ .

Wenn  $U = V$  dann gilt Gleichheit. Angenommen  $\dim U = \dim V$ , gibt es eine Basis  $(v_1, \dots, v_n)$  von  $U$  mit  $n$  Elementen. Diese Basis ist dann ein unabhängiges System von  $V$  mit  $n$  Elementen, also eine Basis nach Korollar 5.4.4. Es gilt  $U = \langle v_1, \dots, v_n \rangle = V$ . ■

## 5.5 Basen in Unendlich dimensionale Vektorräume

Wir werden den folgende Satz nicht beweisen:

**Satz 5.5.1** Alle Vektorräume (auch unendlich dimensional) besitzen eine Basis. □

**Bemerkung 5.5.2** Dieser Satz ist äquivalent zum Auswahlaxiom 1.3.1.