Cheat Sheet Algebra

Logik

Aussagenlogik

Aussage Eine Aussage ist eine sprachliche Äusserung, die wahr (w) oder falsch(f) sein kann.
Bsp: „Es gibt unendlich viele natürliche Zahlen."

Junktoren (Verknüpfungsoperatoren)

$\neg$	Negation, „nicht ..."
$\wedge$	Konjunktion, „... und ..."
$\vee$	Disjunktion, „... oder ..."
$\Rightarrow$	Implikation, „wenn ..., dann ..."
$\Leftrightarrow$	Äquivalenz, „... genau dann, wenn ..."
$\bigoplus$	Antivalenz, „entweder ... oder ..."

Für eine einzelne Aussage A gilt:

A	$\neg A$
f	w
w	f

Für zwei Ausagen A und B gilt:

A	B	$A \wedge B$	$A \vee B$	$A \Rightarrow B$	$A \Leftrightarrow B$	$A \bigoplus B$
f	f	f	f	w	w	f
f	w	f	w	w	f	w
w	f	f	w	f	f	w
w	w	w	w	w	w	f

Bindungsstärke: $\neg$ vor $\wedge$ vor $\vee$ vor $\Rightarrow$ vor $\Leftrightarrow$.

Rechenregeln

Duplizität	$A \wedge A$	$\Leftrightarrow A$
	$A \vee A$	$\Leftrightarrow A$
Doppelte Negation	$\neg\neg A$	$\Leftrightarrow A$
Kommutativität	$A \wedge B$	$\Leftrightarrow B \wedge A$
	$A \vee B$	$\Leftrightarrow B \vee A$
Assoziativität	$(A \wedge B) \wedge C$	$\Leftrightarrow A \wedge (B \wedge C)$
	$(A \vee B) \vee C$	$\Leftrightarrow A \vee (B \vee C)$
Distributiviät	$A \wedge (B \vee C)$	$\Leftrightarrow (A \wedge B) \vee (A \wedge C)$
	$A \vee (B \wedge C)$	$\Leftrightarrow (A \vee B) \wedge (A \vee C)$
De Morgan Regeln	$\neg(A \wedge B)$	$\Leftrightarrow \neg A \vee \neg B$
	$\neg(A \vee B)$	$\Leftrightarrow \neg A \wedge \neg B$
Implikation	$(A \Rightarrow B)$	$\Leftrightarrow (\neg A \vee B)$
Kontraposition	$(A \Rightarrow B)$	$\Leftrightarrow (\neg B \Rightarrow \neg A)$
Äquivalenz	$(A \Leftrightarrow B)$	$\Leftrightarrow (A \Rightarrow B) \wedge (B \Rightarrow A)$
Absorbtion	$A \wedge (A \vee B)$	$\Leftrightarrow A$
	$A \vee (A \wedge B)$	$\Leftrightarrow A$

Prädikatenlogik

Aussageform Eine Aussageform ist eine sprachliche Äusserung, in der Variablen vorkommen und die in Abhängigkeit der Variablenwerte wahr (w) oder falsch (f) sein kann – Aussageformen sind manchmal wahr, manchmal falsch.
Bsp: „Die Zahl x ist eine gerade Zahl."
Es wird unterschieden zwischen Objekt und Prädikat (Eigenschaft): für oberes Beispiel ist „ist gerade" das Prädikat, während x das Objekt ist.

Quantoren (Variablenbinder)

$A(x)$ sei eine Aussageform, M eine Menge von Objekten.
$\forall x \in M A(x)$ Für alle x der Menge M gilt $A(x)$
$\exists x \in M A(x)$ Für mindestens ein x der Menge M gilt $A(x)$

Besondere Ausdrücke

Für mindestens zwei gilt	$\exists x \exists y((A(x) \wedge A(y)) \Rightarrow (x \neq y))$
Es gibt höchstens ein	$\forall x \forall y ((A(x) \wedge A(y)) \Rightarrow (x = y))$

Beispiel: Prädikat: $L = x$ liebt y

- Jeder wird von jemanden geliebt: $\forall x \exists y\, Lyx$
- Jeder liebt jemanden: $\forall x \exists y\, Lxy$
- Jemand liebt alle: $\exists x \forall y\, Lxy$
- Jemand wird von allen geliebt: $\exists x \forall y\, Lyx$
- Jemand liebt sich selbst: $\exists x\, Lxx$
- Alle lieben sich selbst: $\forall x\, Lxx$
- Einer liebt einen: $\exists x \exists y\, Lxy$
- Einer wird geliebt: $\exists x \exists y\, Lyx$
- Jeder liebt jeden: $\forall x \forall y\, Lxy$
- Jeder wird von jedem geliebt: $\forall x \forall y\, Lyx$

Rechenregeln

$$\forall x A(x) \Leftrightarrow \neg\exists x \neg A(x)$$

„Für alle x gilt $A(x)$" ist äquivalent zu: „Es existiert kein x für das $A(x)$ nicht gilt."

$$\neg\forall x A(x) \Leftrightarrow \exists x \neg A(x)$$

„Nicht für alle x gilt $A(x)$." ist äquivalent zu: „Es existiert ein x für das $A(x)$ nicht gilt."

$$\neg\exists x A(x) \Leftrightarrow \forall x. \neg A(x)$$

„Es existiert kein x für das $A(x)$ gilt." ist äquivalent zu: „Für alle x gilt $A(x)$ nicht."
Rechenregeln mit beschränkten Quantoren:

$$\begin{array}{ll} \forall x \in M A(x) & \Leftrightarrow \neg\exists x \in M \neg A(x) \\ \forall x \in M A(x) & \Leftrightarrow \forall x(x \in M \Rightarrow A(x)) \\ \exists x \in M A(x) & \Leftrightarrow \exists x(x \in M \wedge A(x)) \end{array}$$

Die Rechenregel der Aussagenlogik werden mit Hilfe von Wahrheitstafeln bewiesen.

Mengenlehre

Eine Menge ist jede Zusammenfassung von bestimmten, wohlunterscheidbarer Objekte unserer Anschauung oder unseres Denkens zu einem Ganzen.
Kein Objekt kann in einer Menge doppelt vorkommen.

Symbole

$x \in M (x \notin M)$	x ist (kein) Element der Menge M
$x \mid A(x)$	für x gilt die Aussageform $A(x)$
$\emptyset = \{\}$	Leere Menge; enthält nichts
$\mathbb{N} = \{0, 1, 2, \dots\}$	Natürliche Zahlen
$\mathbb{N}^* = \{1, 2, 3, \dots\}$	Positive ganze Zahlen
$\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$	Ganze Zahlen
$\mathbb{Q} = \{x \mid x = \frac{a}{b} \wedge a \in \mathbb{Z} \wedge b \in \mathbb{N}^*\}$	Rationale Zahlen (=Brüche)
$\mathbb{R}$	Reelle Zahlen (= alle Zahlen)
$\mathbb{C}$	Komplexe Zahlen

Intervalle

Fortlaufende Mengen lassen sich als Intervalle schreiben:
$(a, b) = \{x \mid a \leq x \leq b\}$. Runde Klammern bedeuten exklusive, eckige Klammern inklusive. ∞ hat immer eine Runde Klammer zur Folge.

Beispiele für Mengendefinitionen

Aufzählende Notation	$M = \{x_1, x_2, \dots, x_n\}$
Intensionale Notation	$M = \{x \in X \mid A(x)\}$

Beispiel geraden Zahlen: $G = \{n \in \mathbb{N} \mid \exists m \in \mathbb{N}\ 2 \cdot m = n\}$

Mächtigkeit

Die Mächtigkeit $|M|$ entspricht im Prinzip der Anzahl Elemente einer Menge. Allerdings nur im Prinzip, weil: $|\mathbb{N}^*| = |\mathbb{N}| = |\mathbb{Z}| = |\mathbb{Q}| < |\mathbb{R}|$

Mengenoperationen

$A \cup B$	Vereinigungsmenge: $\forall x \in (A \cup B) \Leftrightarrow (x \in A \vee x \in B)$
$A \cap B$	Schnittmenge: $\forall x \in (A \cap C) \Leftrightarrow (x \in A \wedge x \in B)$
$A \backslash B$	Differenzmenge: $\forall x \in (A \backslash B) \Leftrightarrow ((x \in A) \wedge (x \notin B))$

Disjunkt (elementfremd) sind zwei Mengen wenn, $A \cap B = \emptyset$.

Mengenrelationen

$A = B$	Gleichheit: $(A = B) \Leftrightarrow (\forall x(x \in A) \Leftrightarrow (x \in B))$
$A \subseteq B$	Teilmenge: $(A \subseteq B) \Leftrightarrow (\forall x(x \in A) \Rightarrow (x \in B))$
$A \subsetneq B$	Echte Teilmenge: $(A \subsetneq B) \Leftrightarrow ((A \subseteq B) \wedge (A \neq B))$

Rechenregeln

Kommutativität	$A \cup B$	$= B \cup A$
	$A \cap B$	$= B \cap A$
Assoziativität	$(A \cup B) \cup C$	$= A \cup (B \cup C)$
	$(A \cap B) \cap C$	$= A \cap (B \cap C)$
Distributiviät	$A \cup (B \cap C)$	$= (A \cup B) \cap (A \cup C)$
	$A \cap (B \cup C)$	$= (A \cap B) \cup (A \cap C)$
De Morgan Regeln	$(C \backslash A) \cup (C \backslash B)$	$= C \backslash (A \cap B)$
	$(C \backslash A) \cap (C \backslash B)$	$= C \backslash (A \cup B)$
Idempotenzgesetz	$A \cup A$	$= A$
	$A \cap A$	$= A$

Beweise in der Mengenlehre werden durch Umwandlung zu logischen Aussagen geführt. Bsp: Zu zeigen:
$\forall x \in (A \cap B) \cap C \Leftrightarrow x \in A \cap (B \cap C)$

Beweis. Sei x fest, aber beliebig.

$$\begin{aligned} x \in (A \cap B) \cap C &\Leftrightarrow x \in (A \cap B) \wedge x \in C \\ &\Leftrightarrow (x \in A \wedge x \in B) \wedge x \in C \\ &\Leftrightarrow x \in A \wedge (x \in B \wedge x \in C) \\ &\Leftrightarrow x \in A \wedge x \in (B \cap C) \\ &\Leftrightarrow x \in A \cap (B \cap C) \end{aligned}$$

□

Mengenbildung

Sei A ein Menge von Mengen $A = \{X, Y\}$ mit $X = \{x_1, x_2, \dots, x_n\}, Y = \{y_1, y_2, \dots, y_n\}$

Vereinigung

Die Vereinigung $\bigcup A$ ist die Menge aller Elemente aller in A enthaltener Mengen: $\bigcup_{i \in I} Y_i := \bigcup A$, wobei I eine Indexmenge und $A = \{Y_i \mid i \in I\}$

$$x \in \bigcup A \Leftrightarrow \exists Y \in A(x \in Y)$$

Schnittmenge

Die Schnittmenge $\bigcap A$ ist die Menge aller Elemente die in jeder in A enthaltener Menge vorkommt: $\bigcap_{i\in I} Y_i := \bigcap A$, wobei I eine Indexmenge und $A = \{Y_i \mid i \in I\}$

$$x \in \bigcap A \Leftrightarrow \forall Y \in A(x \in Y)$$

Potenzmenge

Die Potenzmenge enthält alle Teilmengen von A als Elemente.

$$\mathcal{P}(A) := \{x \mid x \subseteq A\}$$

Es gelten:

$$|P(A)| = 2^{|A|}$$
$$A = \bigcup \mathcal{P}(A)$$
$$\cap\mathcal{P}(A) = \emptyset$$
$$\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$$
$$\mathcal{P}(A \cup B) \neq \mathcal{P}(A) \cup \mathcal{P}(B)$$

Kartesisches Produkt (Kreuzprodukt)

Das Kreuzprodukt zweier Mengen ist die Menge aller möglichen Kombination von Elementen aus der ersten Menge mit Elementen aus der zweiten Mengen. Die Ergebnismenge besteht aus Tupeln, wobei jedes Tupel eine mögliche Kombination darstellt. Diese 2-Tupel heissen geordnete Paare.

$$A \times B = \{(a, b) \mid a \in A \wedge b \in B\} \neq B \times A$$

Die Reihenfolge ist dabei relevant. Beispiel: $A = \{0, 1, 2\}, B = \{s, t\}$ $A \times B = \{(0, s), (0, t), (1, s), (1, t), (2, s), (2, t)\}$ Die Anzahl Elemente des Kreuzproduktes errechnet sich nach $|K| = |A| \cdot |B|$.

n-Tupel

Ein n-Tupel ist ein Term der Form $(a_1, a_2, \ldots, a_n)$. Zwei Tupel sind gleich, wenn:
$(a_1, \ldots, a_n) = (b_1, \ldots, b_n) \Leftrightarrow (a_1 = b_1) \wedge \cdots \wedge (a_n = b_n)$

Relationen

Eine Relation ist eine Teilmenge des kartesischen Produktes zweier Mengen.

$$R \subseteq A \times B$$

Eine Relation $R = A \times A = A^2$ heisst Relation auf A.

Eine Relation lässt sich umkehren: $R^{-1} = \{(a, b) \in B \times A\}$

Wenn $a \in A$ und $b \in B$ und $(a, b) \in R$, dann steht a in Relation zu b (aRb oder $a \sim_R b$).

Eigenschaften von Relationen

reflexiv	$\forall a \in A : (a, a) \in R$ $\Delta \subseteq R$
irreflexiv	$\forall a \in A : \neg(a, a) \in R$ $\Delta \cap R = \emptyset$
symmetrisch	$\forall a, b \in A : (a, b) \in R \Rightarrow (b, a) \in R$ $R \subseteq R^{-1}$
asymmetrisch	$\forall a, b \in A : (a, b) \in R \Rightarrow (b, a) \notin R$ $R \cap R^{-1} = \emptyset$
antisymmetrisch	$\forall a, b \in A : (a, b) \in R \wedge (b, a) \in R \Rightarrow a = b$ $R \cap R^{-1} \subseteq \Delta$
linear	$\forall a, b \in A : (a, b) \in R \vee (b, a) \in R$ $R \cup R^{-1} = A \times A$
transitiv	$\forall a, b, c \in A : (a, b) \in R \wedge (b, c) \in R \Rightarrow (a, c) \in R$ $R \circ R \subseteq R$

Achtung: reflexiv $\neq \neg$irreflexiv, symmetrisch $\neq \neg$ asymmetrisch $\neq \neg$ antisymmetrisch.

Besondere Relationen

Äquivalenzrelation Eine reflexive, symmetrische und transitive Relation heisst Äquivalenzrelation.

Beispiel: $R =$„a sitzt in der selben Reihe wie b.“ Die Relation ist:

- reflexiv (jeder sitzt in der selben Reihe wie er selbst,
- symmetrisch (wenn a in der selben Reihe sitzt wie b, dann sitzt auch b in der selben Reihe wie a)
- transitiv (wenn a in der selben Reihe sitzt wie b und b in der selben Reihe sitzt wie c, dann sitzt auch a in der selben Reihe wie c)

Bei Anwendung einer Äquivalenzrelation auf eine Menge, zerfällt die Menge in disjunkte Teilmengen (Äquivalenzklassen), deren Elemente in Relation zueinander stehen.

Halbordnung Eine reflexive, antisymmetrische und transitive Relation heisst Halbordnung. Beispiel: $R =$„$x \leq y$“

- reflexiv ($x \leq x$)
- antisymmetrisch ($x \leq y \wedge y \leq x \Rightarrow x = y$)
- transitiv ($x \leq y \wedge y \leq z \Rightarrow x \leq z$)

Ordnung Eine reflexive, antisymmetrische, transitive und lineare Relation heisst Ordnung.«

Funktionen

Eine Funktion ist eine Relation, die jedem Element einer Menge, genau ein Element einer anderen Menge zuordnet.

$$F : X \to Y$$

$f(x)$ bezeichnet dann das Element y von Y für das gilt: $(x, y) \in F$. Es gelten folgende Begriffe:

Definitionsmenge (Domäne) $\text{dom}(F) := X = \{x \mid \exists y((x, y) \in F)\}$

Wertebereich (Bild von F) $\text{im}(F) := \{y \in Y \mid \exists x(F(x) = y)\}$

Erweiterte Funktion $G \circ F : X \to Z$ oder $G \circ F(x) := G(F(x))$

Assoziativität $(G \circ F) \circ H = G \circ (F \circ H)$

Einschränkung Sind $F : A \to B$ und $X \subseteq A$ gegeben, dann ist $F \restriction X := F \cap (X \times B)$ auch eine Funktion und es gilt: $F \restriction X : X \to B$. $F \restriction X$ heisst Einschränkung von F nach X

Injektivität $\forall x_1, x_2 \in X$ gilt $x_1 \neq x_2 \Rightarrow F(x_1) \neq F(x_2)$

Surjektivität $Y = \text{im}(F)$

Bijektivität Sobald eine Funktion sowohl injektiv als auch surjektiv abbildet, ist sie bijektiv

Satz. *Die Komposition $(F \circ G)$ zweier Funktionen gleicher Art (injektiv, surjektiv, bijektiv) ist wieder eine Funktion gleicher Art.*

Satz. *Ist F bijektiv, so existiert F^{-1} D. h. Ist eine Funktion bijektiv, so hat sie eine Umkehrfunktion.*

$$F = (F^{-1})^{-1} \qquad (G \circ F)^{-1} = F^{-1} \circ G^{-1}$$

Äquivalenzklassen

Existiert eine Äquivalenzrelation, so lässt sich eine Menge in Äquivalenzklassen unterteilen:

$$x \sim y \Leftrightarrow F(x) = F(y)$$

Natürliche Zahlen $\mathbb{N}$

Peano-Axiome

1. Die 0 ist eine natürliche Zahl: $0 \in \mathbb{N}$
2. Der Nachfolger einer natürliche Zahl n sei $\sigma(n)$: $n \in \mathbb{N} \Rightarrow \sigma(n) \in \mathbb{N}$
3. Die 0 ist kein Nachfolger: $\forall n \in \mathbb{N}$: $\sigma(n) \neq 0$
4. Zwei verschiedene Zahlen haben verschiedene Nachfolger: $\forall n, m \in \mathbb{N} : (n \neq m) \Rightarrow (\sigma(n) \neq \sigma(m))$
5. Für jede Teilmenge M von $\mathbb{N}$ gilt, wenn M die folgenden Eigenschaften erfüllt:
   a) 0 ist in M
   b) Für jedes n in M ist auch $\sigma(n)$ in M

   dass $M = \mathbb{N}$. Formal:
   $0 \in M \wedge \forall n \in \mathbb{N}$: $(n \in M \Rightarrow \sigma(n) \in M) \Rightarrow M \subseteq \mathbb{N}$
   (Schliesst parallele Strukturen aus.) Induktionsprinzip.

Rekursion

Eine Menge $X \subset \mathbb{N}$ heisst *initiales Segment* von $\mathbb{N}$, wenn mit jeder Nachfolgerzahl $\sigma(n) = n + 1$ auch deren Vorgänger n ein Element von X ist.

$$\forall n \in \mathbb{N}(n + 1 \in X \Rightarrow n \in X)$$

Allgemeine rekursive Definition: Sei M eine beliebige Menge und $g : M \to M$ sowie $c \in M$, dann gibt es eine eindeutig bestimmte Funktion $f : \mathbb{N} \to M$ welche die Rekursionsgleichung erfüllt:

$$f(n) = \begin{cases} f(0) = c \text{ für n} = 0 \\ f(n + 1) = g(f(n)) \text{ sonst} \end{cases}$$

Verknüpfung

Ist A eine Menge, dann nennen wir die Abbildung $\circ : A \times A \to A$ eine Verknüpfung auf A (Bsp. Addition, Multiplikation ...). Seien $g : \mathbb{N} \to \mathbb{N}$ und $c : \mathbb{N} \to \mathbb{N}$, so gelten:

$$n \circ 0 = c(n)$$
$$n \circ (k + 1) = g(n \circ k)$$

Addition

Die Addition (Verknüpfung +)ist rekursiv definiert:

1. Eine Zahl + 0 ist wieder die Zahl selbst. $n + 0 = n$
2. Wird zu einer Zahl, der Nachfolger einer anderen Zahl addiert, ist das so, wie wenn erst die beiden Zahlen addiert werden und dann der Nachfolger gebildet wird: $m + \sigma(n) = \sigma(m + n)$

Zu zeigen: $\forall n \in \mathbb{N}\colon 0 + n = n$

Beweis: Vollständige Induktion über n.

$$\begin{aligned} n &= 0 && \text{(Induktionsanfang)} \\ 0 + 0 &= 0 && \text{(Addition 1: Für die 0 bewiesen)} \end{aligned}$$

Induktionschritt: Wir schliessen von $n = k$ auf $n = \sigma(k)$

$$\begin{aligned} 0 + k &= k && \text{Induktionsannahme; für } k \text{ gilt es bereits} \\ 0 + \sigma(k) &= \sigma(k) && \text{(Neu zu zeigen: gilt für Nachfolger)} \\ 0 + \sigma(k) &= \sigma(0 + k) && \text{(Addition 2)} \\ &= \sigma(k) && \text{(Induktionsannahme: für } \sigma(k) \text{ bewiesen)} \end{aligned}$$

□

Der Trick ist, die Induktionsannahme im Beweis zu verwenden. Es wird nur angenommen, dass die Formel für eine Zahl gilt. Bewiesen wird dann, wenn die Formel für eine Zahl gilt, gilt sie auch für alle anderen.

Für alle $n, k \in \mathbb{N}$ gilt: $(n + 1) + k = n + (k + 1)$

Summen

$$\sum_{i=1}^{0} a_i = 0 \qquad \sum_{i=1}^{n+1} a_i = \left(\sum_{i=1}^{n} a_i\right) + a_{n+1}$$

Die Gaussche Summenformel

$$1 + 2 + \cdots + n = \Sigma_{i=1}^{n} i = \frac{n \cdot (n + 1)}{2}$$

Zu zeigen: $\forall n \in \mathbb{N}\backslash\{0\}\colon \Sigma_{i=1}^{n} i = \frac{n \cdot (n+1)}{2}$

Beweis. Induktion über n

$$\begin{aligned} n &= 1 && \text{(Induktionsanfang)} \\ \Sigma_{i=1}^{1} i = 1 &= \frac{2}{2} = \frac{1 \cdot 2}{2} = \frac{1 \cdot (1 + 1)}{2} && \text{Beweis für 1} \end{aligned}$$

Induktionsschritt: Wir schliessen von $n = k$ auf $n = k + 1$

$$\begin{aligned} \Sigma_{i=1}^{k} i &= \frac{k \cdot (k + 1)}{2} && \text{Induktionsannahme} \\ \Sigma_{i=1}^{k+1} i &= \frac{(k + 1) \cdot ((k + 1) + 1)}{2} && \text{Neu zu zeigen} \\ \Sigma_{i=1}^{k+1} i &= \Sigma_{i=1}^{k} i + (k + 1) && \text{Summe um einen Term verkürzt} \\ &= \frac{k \cdot (k + 1)}{2} + (k + 1) && \text{Induktionsannahme} \\ &= \frac{k \cdot (k + 1)}{2} + \frac{2 \cdot (k + 1)}{2} && \text{Rechts um zwei erweitert} \\ &= \frac{k \cdot (k + 1) + 2 \cdot (k + 1)}{2} && \text{Zusammenzug} \\ &= \frac{(k + 1) \cdot (k + 2)}{2} && k + 1\text{ausklammern} \\ &= \frac{(k + 1) \cdot ((k + 1) + 1)}{2} && \text{Terme vertauscht} \end{aligned}$$

□

Rechenregeln der Addition

Neutrales Element	$0 + n = n$
Kommutativität	$n + m = m + n$
Assoziativität	$(n+m)+k = n+(m+k)$
Kürzbarkeit	$(n+k = m+k) \Rightarrow n = m$

Multiplikation

Die Multiplikation ist rekursiv definiert:

1. Eine Zahl mal 0 ist 0: $n \cdot 0 = 0$
2. Wird eine Zahl mit dem Nachfolger einer anderen Zahl multipliziert, ist das so, wie wenn erst die beiden Zahlen multipliziert und anschliessend die ursprüngliche Zahl addiert wird: $m \cdot \sigma(n) = \sigma(m \cdot n) + m$

Potenzen

1. Eine Zahl hoch 0 ist 1: $n^0 = 1$
2. Eine Zahl hoch dem Nachfolger einer anderen Zahl ist die eigentliche Zahl multipliziert mit der eigentlichen Zahl hoch der anderen Zahl: $m^{\sigma(n)} = m \cdot (m^n)$

Fakultät

1. $0! = 1$
2. $\sigma(m)! = \sigma(m) \cdot m!$

Beispiel: $n! > 2^n$ für $n \geq 4$

Beweis. Anfang: $4! = 24 > 16 = 2^4$
Annahme: $k! > 2^k$
Zu zeigen: $(k + 1)! > 2^{k+1}$

$$(k + 1)! = (k + 1) \cdot k! > (k + 1) \cdot 2^k > 2 \cdot 2^k = 2^{k+1}$$ □

Beweisstrategie: Von links und rechts der Mitte hin annähern.

Rechenregeln der Multiplikation

Absorbtion	$0 \cdot n = 0$
Neutrales Element	$1 \cdot n = n$
Kommutativität	$n \cdot m = m \cdot n$
Assoziativität	$(n \cdot m) \cdot k = n \cdot (m \cdot k)$
Distributivität	$n \cdot (m+k) = n \cdot m + n \cdot k$
Partialsummen	

$$\sum_{i=1}^{n} (c \cdot (a_1 + b_1)) = c \left(\sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i\right)$$

Produkte

$$\prod_{i=1}^{0} a_i = 1 \qquad \prod_{i=1}^{n+1} a_i = a_{n+1} \cdot \prod_{i=1}^{n} a_i$$

Die Ordnung der natürlichen Zahlen

Es sei A eine Menge und $\preceq$ eine Ordnung auf A.

1. Sei $X \subset A$, dann ist $m \in X$ dass minimale Element, wenn gilt: $\forall x \in X (m \preceq x)$.
2. Das Paar $(A, \preceq)$ heisst Wohlordnung, wenn jede nichtleere Teilmenge $X \subset A$ ein minimales Element besitzt.

Die 0 ist die kleinste natürliche Zahl.

Relationen

$$\begin{aligned} n \leq m &:\Leftrightarrow \exists k \in \mathbb{N}(m = k + n) \\ n < m &:\Leftrightarrow (n \leq m \wedge n \neq m) \end{aligned}$$

Satz. *Das Paar $(\mathbb{N}, \leq)$ ist eine Wohlordnung.*

Rechenregeln

$$\begin{aligned} 0 &\leq n \\ n < m &\Leftrightarrow (n + 1) \leq m \\ n < m &\Leftrightarrow (n + k) < (m + k) \\ n \leq m &\Leftrightarrow (n + k) \leq (m + k) \\ (n \leq n') \wedge (m \leq m') &\Leftrightarrow (n + m) \leq (n' + m') \\ \text{Für } c \in \mathbb{N}(c \neq 0) &: c \cdot n < c \cdot m \Leftrightarrow n < m \\ \text{Für } c \in \mathbb{N}(c \neq 0) &: c \cdot n \leq c \cdot m \Leftrightarrow n \leq m \\ n < n' \wedge m < m' &\Rightarrow n + m < n' + m' \wedge n \cdot m < n' \cdot m' \\ n \leq n' \wedge m \leq m' &\Rightarrow n + m \leq n' + m' \wedge n \cdot m \leq n' \cdot m' \end{aligned}$$

Beweis. Zu zeigen: $3 < 5$

$$\begin{aligned} (3 < 5) &= (3 < \sigma(4)) && \text{(Definition der 5)} \\ &\Leftrightarrow (3 = 4) \vee (3 < 4) && \text{(Kleiner 2: links falsch)} \\ (3 < 4) &= (3 < \sigma(3)) && \text{(Definition der 4)} \\ &\Leftrightarrow (3 = 3) \vee (3 < 3) && \text{(Kleiner 2: } (3 = 3) \text{ ist wahr)} \end{aligned}$$

□

Ganze Zahlen

$\mathbb{Z} = \{\cdots -2, -1, 0, 1, 2, \dots\}$
Es gilt: $x < y \Leftrightarrow \exists n \in \mathbb{N} > 0 \mid x + n = y$

Rechenregeln

	$-1\dot{z} = -z$
	$-(-z) = z$
Inverses Element bzgl. +	$-z + z = 0$
Absorbtion	$0 \cdot z = 0$
Neutrales Element bzgl. +	$0 + z = z$
Neutrales Element bzgl. $\cdot$	$1cdotz = z$
Assoziativität bzgl. +	$a+(b+c) = (a+b)+c$
Assoziativität bzgl. $\cdot$	$a \cdot (b \cdot c) = (a \cdot b) \cdot c$
Kommutativität bzgl. +	$a + b = b + a$
Kommutativität bzgl. $\cdot$	$a \cdot b = b \cdot a$
Distributiviät	$a \cdot (b+c) = a \cdot b + a \cdot c$

Definitionen

Subtraktion (-:$\mathbb{Z} \to \mathbb{Z}$)

$$a - b = a + (-b)$$

Betrag ($|.| : \mathbb{Z} \to \mathbb{Z}$)

$$|z| = \begin{cases} z & \text{falls } z \in \mathbb{N} \\ -1 \cdot z & \text{sonst} \end{cases}$$

Teilbarkeit

$$x \mid y \Leftrightarrow \exists q \in \mathbb{Z}(y = x \cdot q)$$

Teilbarkeit ist transitiv: $x \mid y \wedge y \mid z \Rightarrow x \mid z$.
Beispiel: $\forall a, b, c, d \in \mathbb{Z}\ (a \mid b) \wedge (a \mid d) \Rightarrow (a \cdot c) \mid (b \cdot d)$

Beweis. Es seien a, b, c, d fest, aber beliebig.
Es gelte $a \mid b$ und $c \mid d$
Zeige: $a \cdot c \mid b \cdot d$

$$a \mid b \Leftrightarrow \exists q_1 \in \mathbb{Z}\ b = a \cdot q_1$$
$$c \mid d \Leftrightarrow \exists q_2 \in \mathbb{Z}\ d = c \cdot q_2$$
$$(a \cdot q_1) \cdot (c \cdot q_2) = b \cdot d$$

Mit $q_3 = q_1 \cdot q_2$ gilt: $a \cdot c \cdot q_3 = b \cdot d \Rightarrow (a \cdot c) \mid (b \cdot d)$ □

Beispiel: $\forall a, b, c \in \mathbb{Z}\ a \mid b \wedge a \nmid c \Rightarrow a \nmid (b + c)$

Beweis. Es seien a, b, c fest, aber beliebig.
Es gelte $a \mid b$ und $a \nmid b$.
Zeige: $a \nmid (b + c)$. Anmerkung: Beweis durch Widerspruch:
$\neg(a \mid b \wedge a \nmid c \Rightarrow a \nmid (b + c)) = a \mid b \wedge a \nmid c \wedge a \mid (b + c)$
Annahme: $a \mid (b + c)$

$$a \mid b \Leftrightarrow a \cdot q_1 = b$$
$$a \mid (b + c) \Leftrightarrow a \cdot q_2 = b + c$$
$$a \cdot q_2 = a \cdot q_1 + c$$
$$a(q_2 - q_1) = c \Leftrightarrow a \mid c.\text{Widerspruch zum geltenden}$$ □

Hilfssätze

$$s \mid t \wedge s \mid u \Rightarrow s \mid (t + u)$$
$$s \mid t \wedge s \mid u \Rightarrow s \mid (t - u)$$

Teilen mit Rest

Sind $x, y \in \mathbb{N} \setminus \{0\}$, dann gibt es eindeutig bestimmte Zahlen, so dass:

1. $y = q \cdot x + r$
2. $r < x$

Kleinstes gemeinsames Vielfaches (KGV)

(engl. *least common multiple*, zum Erweitern von Brüchen)

$$\text{kgV}(x, y) = \min\{q \in \mathbb{N} \mid x \mid q \wedge y \mid q\}$$

Grösster gemeinsamer Teiler (GGT)

(engl. *greatest common divisor*, zum Kürzen von Brüchen)

$$\text{ggT}(x, y) = \max\{q \in \mathbb{N} \mid q \mid x \wedge q \mid y\}$$
$$\text{kgV}(x, y) \cdot \text{ggT}(x, y) = x \cdot y$$

Euklidischer Algorithmus

$$\text{ggt}(n, m) = \text{ggt}(n, m - n) = \text{ggt}(m, m - n)$$

Erweiterter euklidischer Algorithmus

Erklärt sich am besten an einem Beispiel: Gesucht:
$\text{ggt}(64, 14) = s \cdot 64 + t \cdot 14$

n	a	q	s	t
1	64		1	0
2	14		0	1
3	$a_1 \% a_2 = 8$	$a_1 / a_2 = 4$	$s_1 - q_3 \cdot s_2 = 1$	$t_1 - q_3 \cdot t_2 = -4$
4	$a_2 \% a_3 = 6$	$a_2 / a_3 = 1$	$s_2 - q_4 \cdot s_3 = -1$	$t_2 - q_4 \cdot t_3 = 5$
5	$a_3 \% a_4 = 2$	$a_3 / a_4 = 1$	$s_3 - q_5 \cdot s_4 = 2$	$t_3 - q_5 \cdot t_4 = -9$
6	$a_4 \% a_5 = 0$	$a_4 / a_5 = 3$	$s_4 - q_6 \cdot s_5 = -7$	$t_4 - q_6 \cdot t_5 = 32$

Die Lösung steht in Zeile 5 (mit $s = 2$ und $t = -9$):
$\text{ggt}(64, 14) = 2 = 2 \cdot 64 + (-9) \cdot 14 = 128 - 126 = 2$

Teilerfremdheit

Zahlen sind teilerfremd, wenn $\text{ggt}(m, n) = 1 \Leftrightarrow k \cdot x + k' \cdot y$.

Zahlentheorie

Primzahlen

Primzahlen sind folgendermassen definiert:

$$\forall n, m \in \mathbb{N}(P|n \cdot m \Rightarrow p|n \wedge p|m) \text{ und } p \neq 1$$
$$T(P) = \{1, p\} \text{ und } p \neq 1$$
$$|T(P)| = 2$$

- Es gibt unendlich viele Primzahlen!
- Jede natürliche Zahl $n \in \mathbb{N}$ ist das Produkt endlich vieler Primzahlen: $k = \prod_{i=1}^{n} p_i = p_1 \cdot p_2 \cdot \dots$
- Der kleinste Teiler $d > 1$ einer natürlichen Zahl $n \geq 2$ ist eine Primzahl (Satz vom kleinsten Teiler)

Modulare Arithmetik

Sei $n \in \mathbb{N}$ beliebig. Wir definieren die Modulo-Relation $\equiv_n$ auf $\mathbb{Z}$ wie folgt:

$$r \equiv_n s :\Leftrightarrow n|(r - s)$$

Synonyme schreibweisen:

$$r \equiv_n x$$
$$r \mod n = x$$

Chinesischer Restsatz

$$x \equiv_{m_i} a_i$$
$$M := \prod m_1$$
$$M_i := M/m_i$$

Finde r_i, s_i sodass $r_i \cdot m_i + s_i \cdot M_i = 1$ (Euklid). Setze $e_i = s_i \cdot M_i$.
Die Lösung ist dann $x = \sum a_i \cdot e_i \equiv y \mod M$
Beispiel:

$$x \equiv_3 2 \qquad \to a_1 = 2$$
$$x \equiv_4 3 \qquad \to a_2 = 3$$
$$x \equiv_5 2 \qquad \to a_3 = 5$$
$$M = m_1 \cdot m_2 \cdot m_3 = 3 \cdot 4 \cdot 5 = 60$$
$$M_1 = M/m_1 = 20, \qquad (M_2 = 15, M_3 = 12)$$

Als nächstes s_1 mit Hilfe des erweiterten Euklid bestimmen:

$$1 = r_1 \cdot m_1 + s_1 \cdot M_1 \Rightarrow r_1 = 7, s_1 = -1 \Rightarrow e_1 = -20$$
$$1 = r_2 \cdot m_2 + s_2 \cdot M_2 \Rightarrow r_2 = 4, s_2 = -1 \Rightarrow e_1 = -15$$
$$1 = r_3 \cdot m_3 + s_3 \cdot M_3 \Rightarrow r_3 = 5, s_1 = -2 \Rightarrow e_1 = -24$$
$$x = 2 \cdot (-20) + 3 \cdot (-15) + 5 \cdot (-24) = -133 = 47 \mod 60$$

Grundstrukturen

n-stellige Verknüpfung Sind $A_1, \dots, A_n, B$ Mengen, dann nennt man eine Abbildung $\circ : A_1 \times \cdots \times A_n \to B$ eine n-stellige Verknüpfung auf B. $\circ A^n \to A$ nennt man eine n-stellige Verknüpfung auf A.

Einfache algebraische Strukur bezeichnet ein Paar $S = (A, (f_i)_{i \in I})$. Dabei heisst die Menge A Grundmenge von S. $(f_i)_{i \in I}$ ist eine endliche Familie von Verknüpfungen auf diese Grundmenge.

Zusammengesetze algebraische Struktur bezeichnete die verallgemeinerte einfache algebraische Struktur. Sie ist ein Tupel $S = (A_1, \dots, A_n, (f_i)_{i \in I})$. Sie besteht aus endlich vielen Grundmengen $(A_1, \dots, A_n)$ und einer endlichen Familie von von Vernupfungen, so dass es für alle $i \in I$ natürliche Zahlen p, m und Grundmengen A_r, A_s, A_k gibt mit:

$$f_i : A_r^p \times A_s^m \to A_k$$

Signatur von S $(f_i)_{i \in I}$ heisst Signatur von S.

Für zweiwertige (binäre) Verknüpfunge $\circ$ werden folgende Begriffe verwendet:
Assoziativitat: wenn $\forall a, b, c \in A(A \circ (b \circ c) = (a \circ b) \circ c)$
Kommutativität: wenn $\forall a, b \in A(A \circ b = b \circ a)$

Neutralität

Ein Element $e_i \in A$ ist:
linksneutral bezüglich $\circ$ falls $\forall a \in A(e_i \circ a = a)$
linksneutral bezüglich $\circ$ falls $\forall a \in A(a \circ e_1 = a)$
neutral bezüglich $\circ$ falls $\forall a \in A(e_i \circ a = a \circ e_i = a)$
Wenn es ein neutrales Element gibt, kann es kein zweites neutrales Element geben.

Halbgruppen, Gruppen und Monoide

Eine Struktur $(G, \circ)$ bestehend aus einer Menge G
und einer Verknüpfung $\circ : G \times G \to G$ heisst:

Halbgruppe	wenn die Verknüpfung assoziativ ist
Monoid	wenn zusätzlich ein neutrales Element $e \in G$ existiert
Gruppe	wenn zusätzlich ein für jedes $g \in G$ ein inverses Element g^{-1}existiert
Kommutative Gruppe	wenn die Verknüpfung zusätzlich kommutativ ist.

Für inverse Elemente gilt: $(a^{-1})^{-1} = a$. (Das inverse vom inversen ist das element selbst)

- In Gruppen kann gekürzt werden $(a \cdot x = b \cdot x \Rightarrow a = b)$

Beispiele für Halbgruppen, Gruppen und kommutative Gruppen

Halbgruppen	$(\mathbb{N}, +), (\mathbb{Z}, -)$
Monoid	$(\mathbb{N} \cup 0, +)$
Gruppe	$(\mathbb{Q}, *)$
Kommutative Gruppe	$(\mathbb{Z}, +)$

Unterstrukturen

Sei $(A, \circ)$ eine Struktur und $U \subset A$. U heisst abgeschlossen falls gilt:

$$\forall a, b \in U(a \circ b \in U)$$

Je nach übergeordneter Struktur handelt es sich um Unterhalbgruppen, Untermonoide oder Untergruppen.

Regeln

- Ist $(G, \circ)$ eine Halbgruppe und seien $(U_i)_{i \in I}$ Unter…, dann ist $\bigcap_{i \in I} U_i$ ebenfalls eine Unter….

Jede (Halb-) Gruppe besitzt eine kleinste Unter(halb)gruppe und jeder Monoid besitzt einen kleinsten Untermonoid, die eine gegebene Teilmenge der (Halb-) Gruppe bzw. des Monoids enthalten.

Morphismen

Homomorphismus

Ein (Halb-) Gruppenhomomorphismus ist die Abbildung $f : G \to G'$ einer Struktur $(G, \circ)$ in eine andere Struktur $(G', \sim)$, so dass für alle $a, b \in G$ gilt:

$$f(a \circ b) = f(a) \sim f(b)$$

Beim Monoidhomomorphismus wird zusätzliche das neutrale Element von $(G, \circ)$ auf das neutrale Element von $(G',\ )$ abgebildet.

Monomorphismus bezeichnet injektive (d. h. jedes $a \in G$ wird auf ein anderes $b \in G'$ abgebildet) Homomorphismen.

Epimorphismus bezeichnet surjektive (d. h. durch die Abbildung wird jedes $b \in G'$ erreicht) Homomorphismen

Isomorphismus bezeichnet Homomorphismen die sowohl injektiv als auch bijektiv sind.

Nicht jeder Homomorphismus zwischen zwei Monoiden ist zwingend ein Monoidhomomorphismus. Beispiel:

$$f : (\mathbb{N}, +) \to (\mathbb{N}, \cdot)$$
$$f(0) = 0$$
$$f(0 + 0) = f(0) \cdot f(0) = 0$$

Aber das neutrale Element der Addition (1) wird nicht auf das neutralen Element der Multiplikation abgebildet.

Regeln

1. Sind $f : (G, \cdot) \to (G', \circ)$ und $h : (G', \sim) \to (G'', \bullet)$ Homomorphismen, dann ist auch $h \circ f : (G, \cdot) \to (G'', \bullet)$ ein entsprechender Homomorphismus.
2. Ist $f : (G, \sim) \to (G', \circ)$ ein Homomorphismus, dann ist das Bild $Im(f) \subset G'$ eine entsprechende Unterstruktur von $(G', \circ)$.
3. Es sei $f : G \to G'$ ein Gruppenhomomorphismus zwischen den Gruppen $(G, \sim)$ und $(G', \circ)$ mit den neutralen Elementen e und e', dann gelten:
   - $f(e) = e'$
   - $\forall a \in G(f(a^{-1}) = f(a)^{-1})$
4. Ist $f : (G, \sim) \to (G', \circ)$ ein Gruppenhomomorphismus, dann der Kern $ker(f) = \{a \in G | f(a) = e'\}$ eine Untergruppe von $(G, \sim)$
5. Ist $f : (G, \circ) \to (G', \sim)$ ein Gruppenhomomorphismus mit $ker(f) = \{e\}$, dann ist f injektiv.
6. Ist $f : (G, \sim) \to (G', \circ)$ ein Isomorphismus, dann ist auch $f^{-1} : (G', \circ) \to (G, \sim)$ ein Isomorphismus.

Bild (Im) Menge die durch eine Funktion erzeugt wird.

Kern Alle $g_n \in G$ die auf $e \in G'$ abgebildet werden. Wobei e das neutrale Element von G' ist.

Ringe und Körper

Eine Struktur $(G, +, \cdot)$ heisst Ring, wenn folgende Bedingungen erfüllt sind:

1. $(G, +)$ ist eine kommutative Gruppe
2. $(G, \cdot)$ ist eine Halbgruppe
3. Es gilt das Distributivgesetz, d. h. für alle Elemente a, b, c des Ringes gelten:
   - $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$
   - $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$

Konventionen

- Wenn $(R, +, \cdot)$ ein Ring ist, dann bezeichnen wir das neutrale Element von $(G, +)$ mit 0
- Falls vorhanden bezeichnen wir das neutrale Element von $(G, \cdot)$ mit 1.
- Das inverse Element von $g \in G$ bezüglich $\sim$ bezeichnen wir mit $-g$.
- Das inverse Element von $g \in G$ bezüglich $\circ$ bezeichnen wir mit g^{-1}.

Typische Ringe

$(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot)$ und $(\mathbb{Z}, +, \cdot)$. Sowie der Nullring $(\{0\}, +, \cdot)$

Potenz

Sei $(G, +, \cdot)$ ein Ring mit 1, dann ist die n-te Potenz von $g \in G$ definiert als:

$$r^0 := 1$$
$$r^{n+1} := r \cdot r^n$$

Rechenregeln in Ringen

Sei $G, +, \cdot)$ ein Ring. Für alle Elemente $a, b \in R$ und alle Zahlen $n, k \in \mathbb{N}$ gelten folgende Identitäten:

1. $0 \cdot a = a \cdot 0 = 0$
2. $(-a) = (-1) \cdot a$
3. $-(a \cdot b) = (-a) \cdot b = a \cdot (-b)$
4. $(-a) \cdot (-b) = a \cdot b$
5. $0 = 1 \Rightarrow G = \{0\}$
6. $a^n \cdot a^k = a^{n+k}$
7. $a^{n \cdot k} = (r^n)^k$

Begriffe

rechter Nullteiler	$b \in G$ heisst rechter Nullteiler, falls ein $a \in G \setminus \{0\}$ existiert, so dass $a \cdot b = 0$
linker Nullteiler	$b \in G$ heisst linker Nullteiler, falls ein $a \in G \setminus \{0\}$ existiert, so dass $b \cdot a = 0$
Nullteiler	ist sowohl rechter, wie auch linker Nullteiler
Integritätsring	Die Verknüpfung $\cdot$ ist kommutativ und $0 \in G$ ist der einzige Nullteiler.
Körper	Integritätsring mit $(G \setminus \{0\}, \cdot)$ ist eine kommutative Gruppe.

In einem Integritätsring gilt stets: $1 \neq 0$.
Ein kommuativer Ring $(G, +, \cdot)$ mit $G \neq \{0\}$, ist genau dann ein Integritätsring, wenn für jedes $g \in G \setminus \{0\}$ die Abbildung $f_g : (G, +) \to (G, +)$ mit $f_g(x) := g \cdot x$ ein injektiver Gruppenhomomorphismus ist.
Ein Integritätsring $(R, +, \cdot)$ ist genau dann ein Körper, wenn alle Funktionen $f_g : G \to G$ mit $f_g(x) = r \cdot x$ mit $r \in G \setminus \{0\}$ surjektiv sind.

Folgerungen

1. Jeder endliche Integritätsring ist ein Körper.
2. Für $p \in \mathbb{N} gilt : (\mathbb{Z}_{/p}, +, \cdot)$ ist ein Körper $\Leftrightarrow p$ ist eine Primzahl.

Ringhomomorphismus

Es seien die Ringe $(R,+,\cdot)$ und $(R',+',\cdot')$ gegeben. Ein Ringhomomorphismus $f:(R,+,\cdot)\to(R',+',\cdot')$ ist eine Abbildung $f:R\to R'$, die:

1. Ein Gruppenhomomorphismus $f:(R,+)\to(R',+')$ und
2. ein Halbgruppenhomomorphismus $f:(R,\cdot)\to(R',\cdot')$ ist.
3. Sind $(R,\cdot)$ und $(R',\cdot')$ Monoide, muss f ein Monoidhomomorphismus sein.

Vektorräume

Es sei K ein Körper, seine Elemente heissen *Skalare*. Sie sind mit k bezeichnet.

K-Vektorraum (K-VR) ist ein Tripel $(V,+,\cdot)$ mit:

1. $(V,+)$ ist eine kommutative Gruppe (s. o.)
2. Es ist $\cdot: K\times V\to V$ und für alle Elemente $k_1,k_2\in K$ und $v_1,v_2\in V$ gelten:
   a) $k_1\cdot(k_2\cdot v_1)=k_1\cdot k_2\cdot v_1$
   b) $k_1\cdot(v_1+v_2)=k_1\cdot v_1+k_1\cdot v_2$
   c) $(k_1+k_2)\cdot v_1=k_1\cdot v_1+k_2\cdot v_1$
   d) Für die 1 von K gilt: $1\cdot v_1=v_1$

   Elemente von V werden mit v bezeichnet.

$\Rightarrow$ K selbst mit seiner Addition und Multiplikation ist ein K-VR
$\Rightarrow$ Der Körper $\mathbb{C}$ ist ein 2-dimensionaler VR über $\mathbb{R}$
$\Rightarrow$ Der Körper $\mathbb{R}$ ist ein ∞-dimensionaler VR über $\mathbb{Q}$
$\Rightarrow$ Die Menge $\mathbb{R}\times\mathbb{R}$ ist ein 2-dimensionaler $\mathbb{R}$-VR.

Rechenregeln

$$0_K\cdot v=0_V=k\cdot 0_V$$
$$-k\cdot v=-(k\cdot v)=k\cdot(-v)$$
$$k\cdot v\Rightarrow(k=0_K)\vee(v=0_v)$$

Untervektorraum

Ist V ein K-VR und $U\subset V$ ($U\neq\emptyset$) abgeschlossen unter den Verknüpfungen $\cdot,+$, dann ist U ein Untervektorraum von V und somit auch ein K-VR.
Jede Gerade in $\mathbb{R}^2$ durch den Nullpunkt ist ein solcher 1-dimensionaler Untervektorraum.

Erzeugender Untervektorraum

$$\langle U\rangle:=\left\{\sum_{i=1}^{n}k_i\cdot v_i|(n\in\mathbb{N})\wedge(k_1,\dots,k_n\in K)\wedge(v_1,\dots v_n\in V)\right\}$$

Beispiele:

- $\langle\emptyset\rangle=\{(0,0,0)\}$
- $\langle\{(1,0),(0,1)\}\rangle=\mathbb{R}^2$

Erzeugendensystem bezeichnet eine Menge U, wenn gilt $\langle U\rangle=V$ mit $U\subset V$

Lineare unabhängig (frei) ist eine Menge U wenn für alle paarweise verschiedenen Vektoren $v_1,\dots,v_n\in U$ und für alle Skalare $k_1,\dots k_n\in K$ stet gilt:

$$\sum_{i=0}^{n}k_i\cdot v_i\neq 0\text{ oder }r_1,\dots,r_n=0$$

Basis bezeichnet ein linear unabhängiges (freies) Erzeugendensystem (geschrieben als B).

Lässt sich ein Vektor eines Untervektorraums aus anderen Vektoren desselben Untervektorraums erzeugen, dann ist der Untervektorraum nicht frei.

$$(v=\sum_{i=1}^{n}k_i\cdot v_i)\wedge(v,v_1,\dots,v_n\in U)\wedge(k_1,\dots,k_n\in K)\Leftrightarrow U\text{ ist nicht frei}$$

Jeder Vektor v aus V lässt sich aus jeder beliebigen Basis erzeugen:

$$v=\sum_{i=1}^{n}k_i\cdot b_i\Leftrightarrow B=\{b_1,\dots,b_n\}\text{ist eine Basis von }V$$

Sätze, Axiome, Theoreme

- Ist A eine Menge und „$\leq$“ eine Halbordnung auf A, so dass für jede total geordnete Teilmenge eine obere Schranke bezüglich $\leq$ existiert, dann besitzt A maximale Elemente.
- Ist $\mathcal{F}$ eine Familie von Mengen mit der Eigenschaft, dass mit jeder Kette $U\subset\mathcal{F}$ die Beziehung $\cup U\in\mathcal{F}$ gilt, dann hat das Paar $(\mathcal{F},\subset)$ maximale Elemente.
- Ist V ein K-VR und ist $E\subset V$ ein Erzeugendensystem und $F\subset V$ eine freie Teilmenge von V, dann gibt es eine Menge $U\subset V$ mit $X\cap F\neq\emptyset$, so dass $F\cup U$ eine Basis von V ist.
- Jeder Vektorraum hat eine Basis. Hat ein Vektorraum eine endliche Basis, dann ist jede weitere Basis dieses Vektorraums ebenfalls endlich und besitzt gleich viele Elemente.

Dimension

Die Dimension eines Vektorraums V über K ist $\dim_K(V)=|B|$.
Beispiele:

- $\dim_{\mathbb{Q}}(\mathbb{R})=\infty$
- $\dim_{\mathbb{Q}}(\mathbb{Q})=1$ (weil $\{1\}\subset\mathbb{Q}$ eine Basis von $\mathbb{Q}$ ist)

Lineare Abbildungen und Matrizen

Sind W und V beides K-VR. Eine Abbildung $f:V\to W$ heisst K-linear oder K-VR Homomorphismus falls für alle Element $\lambda\in K$ und alle Vektoren $v,w\in V$ die Gleichungen:

$$f(v+w)=f(v)+f(w)\qquad f(\lambda v)=\lambda f(v)$$

erfüllt werden. Die Menge aller derartiger Abbildungen wird als $\mathrm{Hom}_K(V,W)$ bezeichnet.
Für K-lineare Abbildungen gilt:

$$f(\sum_{i=1}^{n}\lambda_i\cdot v_i)=\sum_{i=1}^{n}\lambda_i\cdot f(v_i)$$

Beispiele:

- $f:\mathbb{R}^3\to\mathbb{R}^2$ mit $f((x,y,z)):=(y,z)$
- $f:\mathbb{R}^2\to\mathbb{R}^3$ mit $f((x,y)):=(0,y,z)$

Kern Für $f\in\mathrm{Hom}_K(V,W)$ ist der Kern definiert als:

$$\ker(f):=\{v\in V|f(v)=0\}$$

- Sind V und W zwei K-VR und $f,g\in\mathrm{Hom}_K(V,W)$, so dass f und g auf einer Basis von V dieselben Werte annehmen, dann gilt: $f=g$
- Sind V und W zwei K-VR und ist $B=\{b_1,\dots,b_n\}$ eine Basis von V sowie $f:B\to W$ eine beliebige Funktion, dann lässt sich f eindeutig zu einer K-linearen Abbildung $f:V\to W$ fortsetzen.
- Zwei K-VR gleicher, endlicher Dimension sind stets isomorph zueinander. $\Rightarrow$ Ist V ein endlich dimensionaler K-VR, dann gibt es eine Zahl $n\in\mathbb{N}$, so dass V isomorph zu K^n ist.
- Sind V und W zwei K-VR und ist $f\in\mathrm{Hom}_K(V,W)$, dann ist $\ker(f)$ ein Untervektorraum von V und $\mathrm{im}(f)$ ein Untervektorraum von W.
- Sind V und W zwei K-VR endlicher Dimension und ist $f\in\mathrm{Hom}_K(V,W)$, dann gilt:

$$\dim_K(\mathrm{im}(f))+\dim_K(\ker(f))=\dim_K(V)$$

- Sind V und W zwei K-VR endlicher und gleicher Dimension, dann sind für $f\in\mathrm{Hom}_K(V,W)$ folgende Aussage äquivalent:
  - f ist ein Isomorphismus
  - f ist ein Epimorphismus
  - f ist ein Monomorphismus

Matrizen

Eine Matrix ist eine rechteckige Anordnung von Elementen. Matrizen können beliebige Dimensionalität besitzen. Die Elemente der Matrix über K heissen Komponenten. Sie entstammen einer Menge K (Körper oder Ring). Formal handelt es sich um eine Funktion:

$$A:\{1,\dots,m\}\times\{1,\dots,n\}\to K,\quad(i,j)\mapsto a_{ij}$$

Sie ordnet jedem Indexpaar (i,j) einen Funktionswert a_{ij} zu.
Eine Matrix mit m-Zeilen und n-Spalten wie folgt darstellen:

$$A=\mathbf{A}=\underline{A}=\begin{pmatrix}a_{11}&a_{12}&\cdots&a_{1n}\\a_{21}&a_{22}&\cdots&a_{2n}\\\vdots&\vdots&\ddots&\vdots\\a_{m1}&a_{m2}&\cdots&a_{mn}\end{pmatrix}=(a_{ij})$$

Addition

$$A+B:=(a_{ij}+b_{ij})_{i=1\dots\ m;j=1\dots\ n}$$

$$\begin{pmatrix}1&-3\\1&2\end{pmatrix}+\begin{pmatrix}0&3\\2&1\end{pmatrix}=\begin{pmatrix}1+0&(-3)+3\\1+2&2+1\end{pmatrix}=\begin{pmatrix}1&0\\3&3\end{pmatrix}$$

Die Addition ist assoziativ, kommutativ und besitzt mit der Nullmatrix ein neutrales Element.

Skalarmultiplikation

$$\lambda\cdot A:=(\lambda\cdot a_{ij})_{i=1,\dots,m;\ j=1,\dots,n}$$

$$5\cdot\begin{pmatrix}1&-3&2\\1&2&7\end{pmatrix}=\begin{pmatrix}5\cdot1&5\cdot(-3)&5\cdot2\\5\cdot1&5\cdot2&5\cdot7\end{pmatrix}=\begin{pmatrix}5&-15&10\\5&10&35\end{pmatrix}$$

λ und die Elemente entstammen demselben Ring $(K,+,\cdot,0)$.

Multiplikation

Zwei Matrizen können multipliziert werden, wenn die Spaltenanzahl der linken ($A = (a_{ij})$) mit der Zeilenanzahl der rechten Matrix ($B = (b_{ij})$)übereinstimmt.

$$c_{ij} = \sum_{k=1}^{m} a_{ik} \cdot b_{kj}$$

B : p Zeilen q Spalten

$$\begin{pmatrix} b_{11} & b_{12} & \dots & b_{1q} \\ b_{21} & b_{22} & \dots & b_{2q} \\ \vdots & \vdots & \ddots & \vdots \\ b_{p1} & b_{p2} & \dots & b_{pq} \end{pmatrix}$$

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1p} \\ a_{21} & a_{22} & \dots & a_{2p} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{np} \end{pmatrix} \quad \begin{pmatrix} c_{11} & c_{12} & \dots & c_{1q} \\ c_{21} & c_{22} & \dots & c_{2q} \\ \vdots & \vdots & \ddots & \vdots \\ c_{n1} & c_{n2} & \dots & c_{nq} \end{pmatrix}$$

A : n Zeilen p Spalten

$C = A \times B$: n Zeilen q Spalten

Die Multiplikation ist nicht kommutativ!

Einheitsmatrix

Die $(n \times n)$-Einheitsmatrix ist definiert als:

$$E_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

Darstellende Matrix

Es sei $v = \lambda_1, \dots, \lambda_n) \in K^n$, für $i = 1, \dots, n$. Mit $v[i] := \lambda_i$ ist die i-te Komponente von v bezeichnet.

Θ: $\mathrm{Hom}_K(K^n, K^m) \to K^{m,n}$

$$\Theta(f) = \begin{pmatrix} f(e_1)[1] & \cdots & f(e_i)[1] & \cdots & f(e_n)[1] \\ \vdots & & \vdots & & \vdots \\ f(e_1)[m] & \cdots & f(e_i)[m] & \cdots & f(e_n)[m] \end{pmatrix}$$

Beispiel: $f : \mathbb{R}^3 \to \mathbb{R}^2, f(x, y, z) = (2x - 3y, x - 2y + z)$
Im Urbild ($\mathbb{R}^3$) und im Zielraum ($\mathbb{R}^2$) die Standardbasis wählen:

$$A = \left(\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right), \quad B = \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right)$$

Es gilt:

$$f \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 2 \cdot 1 - 3 \cdot 0 \\ 1 - 2 \cdot 0 + 0 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$$

entsprechend: $f \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} -3 \\ -2 \end{pmatrix}, f \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

Somit wird $\Theta_B^A(f) = \begin{pmatrix} 2 & -3 & 0 \\ 1 & -2 & 1 \end{pmatrix}$

Ψ: $K^{m,n} \to \mathrm{Hom}_K(K^n, K^m)$

$$\Psi(A)(v) = A \circ \begin{pmatrix} v[1] \\ \vdots \\ v[n] \end{pmatrix}$$

Beispiel: $\Psi(\Theta(f))(2, 3, 1)$:

$$\Psi(\Theta(f))(2, 3, 1) = \begin{pmatrix} 2 & -3 & 0 \\ 1 & -2 & 1 \end{pmatrix} \circ \begin{pmatrix} 2 \\ 3 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 \cdot 2 - 3 \cdot 3 \\ 2 - 2 \cdot 3 + 1 \end{pmatrix}$$

$$= (-5, -3) = f(2, 3, 1)$$

Beweistechniken

Direkter Beweis

Strategie: Zwingende Argumente für die Richtigkeit von A finden.
Bsp: „Beweisen, dass jede durch 4 teilbare natürliche Zahl gerade ist.“

Beweis. Direkt

1. Sei n eine beliebige durch 4 teilbare Zahl
2. n muss also von der Form $n = 4 \cdot m (m \in \mathbb{N})$ sein
3. Sei $k = 2 \cdot m \Rightarrow n = 2 \cdot k$ sein
4. Deswegen muss n gerade sein □

Beweis durch Widerspruch

Strategie: Annehmen, das A falsch sei. Unter dieser Annahme eine Folgerung herleiten, von der entweder bekannt ist, dass sie falsch ist, oder die im Widerspruch zu Annahme steht.
Bsp: „Beweisen, dass es keine grösste natürliche Zahl gibt.“

Beweis. durch Widerspruch

1. Sei m die grösste natürliche Zahl
2. Es gilt für jede natürliche Zahl n: $n + 1$ ist ebenfalls eine natürliche Zahl $\wedge n < n + 1$
3. Also muss $m + 1$ eine natürliche Zahl sein $> m$ sein ↯

Beweis durch Implikation

Problem: Beweisen, dass $A \Rightarrow B$ wahr ist.
Strategie: Unter der Annahme, dass A wahr ist, folgern, dass dann B wahr sein muss.
Bsp: „Für jede natürliche Zahl n gilt: $(n^2 + 1 = 1) \Rightarrow (n = 0)$“

Beweis. durch Implikation

1. Angenommen, $n^2 + 1 = 1$ sei wahr
2. Dann ist $n^2 = 0$ bzw. $n = \sqrt{0} = 0$
3. Also: $(n^2 + 1 = 1) \Rightarrow (n = 0)$ □

Beweis durch Kontraposition

Problem: Beweisen, dass $A \Rightarrow B$ wahr ist.
Strategie: Die Kontraposition $(\neg B \Rightarrow \neg A)$ beweisen.
Bsp: „Für jede natürliche Zahl n gilt: $(n^2 + 1 = 1) \Rightarrow (n = 0)$“

Beweis. durch Kontraposition

1. Es muss gelten: $n \neq 0 \Rightarrow (n^2 + 1 \neq 1)$
2. Ist $n \neq 0 \Rightarrow n^2 \neq 0$
3. daraus folgt, dass $n^2 + m \neq m$ für jedes $n \neq 0$
4. Also muss $n^2 + 1 \neq 1 (n \neq 0)$ □

Beweis durch Äquivalenz

Problem: Beweisen, dass $A \Leftrightarrow B$ wahr ist. Strategie: Beweisen, dass $A \Rightarrow B \wedge B \Rightarrow A$
Als erstes also beweisen, dass $A \Rightarrow B$ und als zweites beweisen, dass $B \Rightarrow A$ Bsp: „Für jede natürliche Zahl n gilt:
$(n^2 + 1 = 1) \Leftrightarrow (n = 0)$“

Beweis. durch Äquivalenz

1. Für den Beweis $(n^2 + 1 = 1) \Rightarrow (n = 0)$ siehe z.B. Implikation
2. Bleibt zu beweisen, dass $n = 0 \Rightarrow n^2 + 1 = 1$
   a) Einsetzen von $n = 0 : 0^2 + 1 = 1$, d. h. $1 = 1$, was wahr ist
   b) Folglich gilt: $n = 0 \Rightarrow n^2 + 1 = 1$
3. Beide Teilaussagen sind wahr, also ist die ganze Aussage wahr □

Beweistechnik durch vollständige Induktion

$$(E(0) \wedge \forall n \in \mathbb{N}(E(n) \Rightarrow E(n + 1))) \Leftrightarrow \forall n \in \mathbb{N}(E(n))$$

Man zeigt etwas für die 0, anschliessend nimmt man an, dass wenn es für eine natürliche Zahl gilt, dann auch für deren Nachfolger. Gilt es für 0 und alle Nachfolger, gilt es für alle. Beispiele bei der Addition der natürlichen Zahlen.

Revision: 1.0, Datum: 18. Januar 2016