Linear Algebra I

24. Februar 2021

Jung

Zusammenfassung. (For my cat) I love my cat dearly.

Inhaltsverzeichnis

1 Grundbegriffe

1.1 Logik

Kontraposition von $P \to Q$ ist $\neg Q \to \neg P$

1.2 Abbildungen

Definition 1.1. Eine Abbildung $f : A \to B$ heißt

$$\begin{aligned} \text{injektiv} &\iff \forall x, y \in A \quad \text{mit} \quad x \neq y \Rightarrow f(x) \neq f(y) \\ \text{surjektiv} &\iff \forall b \in B, \exists x \in A : f(x) = b \\ \text{bijektiv} &\iff \forall b \in B : \exists! x \in A : f(x) = b \\ \text{invertierbar} &\iff \exists f' : B \to A \quad \text{s.d} \quad f' \circ f = id_A, f \circ f' = id_B \end{aligned}$$

Definition 1.2 (Bild,Urbild,Faser)**.** Sei $f : A \to B$. Die Menge A heißt der Definitionsbereich von f. Die Menge B heißt der Wertebereich von f. Wenn $A' \subseteq A$, ist das Bild von A' unter f

$$f(A') := \{f(x) \mid x \in A'\}. \tag{1}$$

Die Menge $f(A) = \{f(x) \mid x \in A\}$ heißt das Bild von f. Wenn $B' \subseteq B$, ist das Urbild von B' unter f

$$f^{-1}(B') := \{x \in A \mid f(x) \in B'\}. \tag{2}$$

Wenn $B' = \{y\}$, nennt man die Menge $f^{-1}(y) := f^{-1}(\{y\}) = \{x \in A \mid f(x) = y\} \subseteq A$ die Faser von f in A.

1.3 Mengen

Definition 1.3 (Mächtigkeit)**.** Sei M eine Menge. Die Anzahl der Elemente von M ist die Mächtigkeit (Kardinalität) von M

$$\#(M) := n$$

Wenn M eine unendliche Menge ist, dann gilt $\#(M) := \infty$. Wenn M eine leere Menge ist (i.e. $M = \emptyset$), dann gilt $\#(M) := 0$

Definition 1.4 (Abzählbare Mengen)**.** Zwei Mengen M and N heißen gleichmächtig, wenn es eine bijektive Abbildung $f : M \to N$ gibt.

Eine Menge M heißt abzählbar unendlich, wenn sie mit $\mathbb{N}$ gleichmächtig ist (i.e.e $\exists f : \mathbb{N} \to M$, $f =$ bij.). Eine Menge heißt abzählbar, wenn sie endlich oder abzählbar unendlich ist.

Eine Methode um zu überprüfen, ob eine Menge endlich ist.

Lemma 1.1. *Sei $A =$ Menge. $A =$ endlich $\Leftrightarrow \exists n \in \mathbb{N} : |A'| \leq n, \forall A' \subseteq A, A' =$ endlich*

Definition 1.5 (Kartesisches Produkt)**.** Seien M und N zwei Mengen. Das kartesische Produkt von M und N ist

$$M \times N := \{(m, n) \mid m \in M \text{ und } n \in N\} \tag{3}$$

1.4 Relationen

Definition 1.6 (Relation)**.** Eine Relation auf einer Menge M ist eine Teilmenge $R \subseteq M \times M$. Eine Relation ist also eine Menge geordneter Paare. Wenn $(x, y) \in R$ schreiben wir

$$x \sim_R y \quad \text{oder} \quad x \sim y$$

und man sagt, dass x in Relation zu y steht.

Definition 1.7 (Eigenschaften einer Relation)**.** Eine Relation heißt

$$\begin{aligned} \text{reflexiv} &\iff \forall x \in M : (x, x) \in R \\ \text{symmetrisch} &\iff \forall x, y \in M : (x, y) \in R \Rightarrow (y, x) \in R \\ \text{antisymmetrisch} &\iff \forall x, y \in M : (x, y) \in R \text{ und } (y, x) \in R \Rightarrow x = y \\ \text{transitiv} &\iff \forall x, y, z \in M : (x, y) \in R \text{ und } (y, z) \in R \Rightarrow (x, z) \in R \end{aligned}$$

1.4.1 Äquivalenzrelationen

Definition 1.8. Eine Äquivlenzrelation auf einer Menge M ist eine Relation $\sim_R$ die ***reflexiv***, ***symmetrisch*** und ***transitiv*** ist.

Wenn $\sim_R$ eine Äquivalenzrelation ist und $x \sim_R y$, dann sagen wir, dass x äquivalent zu y (unter R) ist.

Definition 1.9 (Äquivalenzklasse)**.** Sei $\sim$ eine Äquivalenzrelation auf der Menge M. Eine Äquivalenzklasse für $\sim$ ist eine nichtleere Teilmenge $C \subseteq M$, die die folgende Axiome erfüllt.
(ÄK1) Wenn $x, y \in C$, dann $x \sim y$
(ÄK2) Wenn für $y \in M, \exists x \in C : x \sim y$, dann $y \in C$

Ein Repräsentant der Äquivalenzklasse C ist ein Element $x \in C$.
Ein Repräsentantensystem für die Äquivalenzrelation $\sim$ ist eine Teilmenge $M' \subseteq M$ mit der Eigenschaft, dass $|M' \cap C| = 1$ für jede Äquivalenzklasse C.

Bemerkung. *Für jedes $x \in M$ ist die Menge $\{y \in M \mid y \sim x\}$ eine Äquivalenzklasse. Da Äquivalenzklasse nicht leer sind, hat jede Äquivalenzklasse die Form $[x]$ für jeden Repräsentant.*

Satz 1.2. *Sei $\sim$ eine Äquivalenzrelation auf der Menge M.*

1. *Wenn C_1 und C_2 zwei Äquivalenzklassen sind, dann gilt entweder $C_1 \cap C_2 = \emptyset$ oder $C_1 = C_2$*
2. *Die Menge M ist die Vereinigung aller Äquivalenzklassen bezüglich $\sim$:*

$$M = \bigcup_{C = \text{Äq.Kl}} C$$

Eine Partition einer Menge M ist eine Teilmenge $\mathcal{P} \subset 2^M$ mit der folgenden Eigenschaft

$$A \cap B = \emptyset \quad \forall A, B \in \mathcal{P} \quad \text{und} \quad \bigcup_{A \in \mathcal{P}} A = M$$

Bemerkung. *Wenn $\mathcal{P}$ eine Partition von M ist, dann ist $x \sim_P y \Leftrightarrow \exists A \in \mathcal{P} : x, y \in A$ eine ÄR auf M. Die Umkehrung gilt auch (Jede ÄR wird durch eine Partition (in ÄK) definiert). Beweis (siehe Übung)*

Definition 1.10 (Quotienten-menge, -abbildung)**.** Sei $\sim$ eine Äquivalenzrelation auf die Menge M. Die Quotienten-menge (*Faktormenge*) von M durch $\sim$ ist die Menge

$$M/_\sim := \{C : C \text{ ist eine Äquivalenzklasse für } \sim \text{ in } M\}$$

Die Quotientenabbildung (oder kanonische Projektion, oder kanonische Surjektion) ist die Abbildung, die jedes Element in dessen Äquivalenzklasse abbildet:

$$p : M \longrightarrow M/_\sim \quad x \mapsto [x]$$

Man kann diese Menge auch als $M/_\sim = \{[x] : x \in M\}$

Beispiel 1.1 (Kongruenz Modulo m, ÄR auf $\mathbb{Z}$)**.** *$m \in \mathbb{N}$ auf $\mathbb{Z}$. Diese wird mit $\mathrm{mod} m$ bezeichnet*

$$x \equiv_m y \quad (x \sim_m y) \quad \textit{oder} \quad x \equiv y \bmod m \overset{\text{Def}}{\Longleftrightarrow} x = y + k \cdot m, \quad k \in \mathbb{Z}$$

$\overset{\text{Def}}{\Longrightarrow} x - y = k \cdot m \Longrightarrow m | x - y$

- *(Reflexivität) Sei $a \in \mathbb{Z}$, $m | a - a = m | 0 \Longrightarrow a \equiv a \bmod m$*
- *(Symmetrie) Sei $a, b \in \mathbb{Z} : a \equiv b \bmod m \Longrightarrow m | a - b$*

  $\Longrightarrow \exists k \in \mathbb{Z} : a - b = m \cdot k \Longrightarrow b - a = m \cdot (-k) \Longrightarrow m | b - a \Leftrightarrow b \equiv a \bmod m$

- *(Transitivität)*

$$a \equiv b \bmod m \Longrightarrow m|a-b$$
$$b \equiv c \bmod m \Longrightarrow m|b-c$$
$$\Longrightarrow m|1\cdot(a-b)+1\cdot(b-c) = m|a-c \Longrightarrow a \equiv c \bmod m$$

Also Kongruenz Modulo m ist eine ÄR auf $\mathbb{Z}$.

Beispiel 1.2 (Kongruenz Modulo m, ÄK, Quotienten-menge, -abbildung, Partition, Repräsentant(system)). $x \equiv y \bmod 3 \Leftrightarrow \exists k \in \mathbb{Z} : x - y = 3 \cdot k$ *Die Quotientenmenge ist* $\mathbb{Z}/_{\bmod 3} = \{.., [-1]_3, [0]_3, [1]_3, [2]_3, .., [17]_3\}$. *Daher die Quotientenabbildung* $q_{\bmod 3} : \mathbb{Z} \Rightarrow \mathbb{Z}/_{\bmod 3}$ *wird wie folgt definiert*

$$\forall x \in \mathbb{Z} : q_{\bmod 3}(x) = [x]_3 = \{x + 3 \cdot k | k \in \mathbb{Z}\}$$

$q_{\bmod 3}(17) = [17]_3 = \{.., -1, 2, 5, 8, .., 14, 17, 20, 23, ...\}$

$$\left.\begin{array}{lll} 8 \bmod 3 & = 2 & (8 = 2\cdot 3 + 2) \\ 17 \bmod 3 & = 2 & (17 = 5\cdot 3 + 2) \end{array}\right\} \Rightarrow 17 \equiv 8 \bmod 3$$

Man kann auch ein Beispiel vorstellen, welches (ÄK2) erfüllt. Also $[17]_3$ *ist eine ÄK für* $\bmod 3$. *Es gilt tatsächlich* $\forall x \in \mathbb{Z} = [x]_{\bmod 3}$ *(Bemerkung).*

Die Elemente der Partition sind nicht anders als die Restklassen von Modulo 3

$$\left.\begin{array}{ll} [0]_3 & = \{..., -6, -3, 0, 3, 6, ...\} \\ [1]_3 & = \{..., -5, -2, 1, 4, 7, ...\} \\ [2]_3 & = \{..., -4, -1, 2, 5, 8, ...\} \end{array}\right\}$$

Partition P *von* $\mathbb{Z}$ *ist* $P = [0]_3, [1]_3, [2]_3$. *Man kann zeigen, dass* $[17]_3 = [2]_3$ *(Satz 1.1)*
Ein Repräsentant von $[17]_3$ *ist 14.*
Ein Repräsentantensystem für $\bmod 3$ *ist* $\{0, 1, 2\}$

If you have time, add universal properties

1.4.2 Ordnungsrelation

Wenn R eine Relation auf M ist, dann ist die (von R) induzierte Relation auf M

$$R|_M := \{(x, y) \in R : x, y \in M\} \subseteq M \times M$$

Definition 1.11 (Ordnungsrelation). Sei M eine beliebige Menge

- Eine Ordnungsrelation auf M ist eine Relation $\preceq$ auf M, die ***reflexiv***, ***antisymmetrisch*** und ***transitiv*** ist.
- Eine partiell geordnete Menge ist ein geordnetes Paar $(M, \preceq)$, wobei $\preceq$ eine Ordnungsrelation auf M ist. Manchmal wird 'partiell' ausgelassen.
- $x, y \in M$ sind vergleichbar, wenn $x \preceq y$ oder $y \preceq y$. Sonst sind die unvergleichbar.
- Eine Ordnungsrelation heißt total wenn jede zwei Elemente vergleichbar sind.
- Sei (M,$\preceq$) eine (partielle) geordnete Menge und $N \subseteq M$ eine Teilmenge, ist (N,$\preceq$) auch eine (partiell) geordnete Menge.

  1. Eine obere (bzw. untere) Schranke von N ist ein Element $x \in M$ (aber $x \notin N$), wobei

  $$n \preceq x \quad (\text{ bzw. } x \preceq n) \quad \forall n \in N$$

  Es kann mehrere Schranken geben.

  2. Ein Maximum oder Minimum von N ist ein Element $m \in N$, wobei

  $$\nexists x \in N : m \preceq x \quad (\text{ bzw. } x \preceq m) \text{ und } m \neq x$$

  Wenn so ein Element existiert, kann man zeigen, dass es **eindeutig** ist.

3. Ein Maximales Element bzw Minimales Element von N ist ein Element $n \in \mathbb{N}$, wobei

$$n = \text{ maximales Element } \iff \text{ wenn } n' \in N \text{ und } n \leqslant n' \Rightarrow n = n'$$
$$n = \text{ minimales Element } \iff \text{ wenn } n' \in N \text{ und } n' \leqslant n \Rightarrow n = n'$$

   - *Maximales Element*: Es gibt keine anderen größeren Elemente im Vergleich dazu
   - *Maximum (Größtes Element)*: Man kann es mit allen anderen Elementen vergleichen und ist größer als alle. Ein Maximum ist nicht anders als ein eindeutiges maximales Element

4. Die untere Schranke a von N ist ein Infimum von N, falls $a = \max\{m \in M$: m ist eine **untere** Schranke von N$\}$
   Die obere Schranke b von N ist ein Supremum von N, falls $b = \min\{m \in M$: m ist eine **obere** Schranke von N$\}$

- Eine Wohlordnung $(M, \preceq)$ ist eine Ordnungsrelation, wobei

$$\text{Für jede } M' \subseteq M, M' \neq \emptyset : \exists x \in M', \text{s.d } x \preceq y \quad \forall y \in M'$$

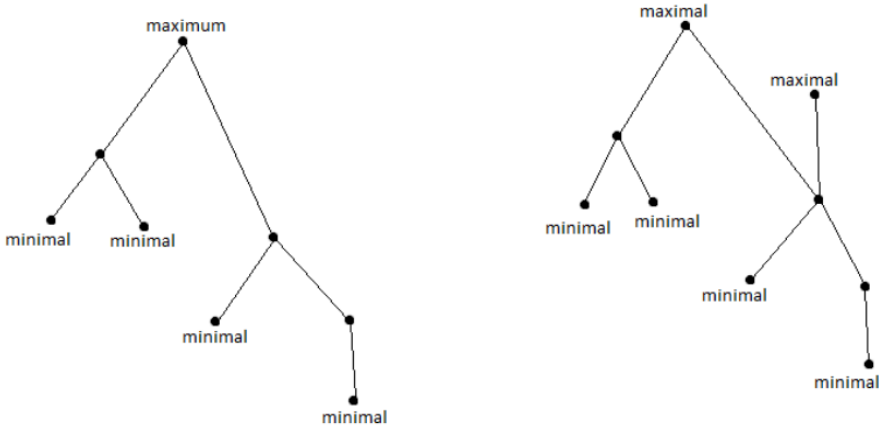


Abbildung 1: Hasse Diagramm von Maximum, maximalem und minimalem Element

Beispiel 1.3 (Teilbarkeit). *Teilbarkeit ist eine partielle Ordnungsrelation auf N (Der Beweis ist trivial). $(N, |)$ ist keine totale Ordnungsrelation, weil nicht alle Elemente mit einander vergleichbar sind wie zB. $2 \nmid 3$*

- $0 = \max(N, |)$, *weil* $\nexists x \in N, x \neq 0 : 0|x$
- $1 = \min(N, |)$, *weil* $\nexists x \in N, x \neq 1 : x|1$

Die Teilbarkeit auf $\mathbb{Z}$ ist aber keine Ordnungsrelation, weil sie nicht antisymmetrisch ist ($3|-3$ und $-3|3$ aber $3 \neq -3$)

1.5 Teilbarkeit

Definition 1.12 (Teilbarkeit in $\mathbb{Z}$). $a, b \in \mathbb{Z} : a|b \Leftrightarrow \exists c \in Z : b = a \cdot c$

Satz 1.3. *[Division mit Rest] Seien $a, b \in Z$ mit $b > 0$. Dann $\exists! q, r \in \mathbb{Z} : a = q \cdot b + r$ und $0 \leq r < b$*

Definition 1.13 (ggT und kgV). Seien $a, b \in \mathbb{Z}$

1. Ein größter gemeinsamer Teiler von a und b ist $d \in \mathbb{N}$, wobei:
   - (ggT 1) $d|a$ und $d|b$
   - (ggT 2) Wenn $d'|a$ und $d'|b$, dann $d'|d$
2. Ein kleinstes gemeinsames Vielfaches von a und b ist $m \in \mathbb{N}$, wobei:
   - (kgV 1) $a|m$ und $b|m$
   - (kgV 2) Wenn $a|m'$ und $b|m'$, dann $m|m'$

Bemerkung. *Weiterhin gilt*

- *ggT(0,a)=a*
- *ggT(0,0)=0*
- *kgV(0,0)=0*
- *kgV(0,a)=a*
- *Wenn $a|b$, dann ggT(a,b)=|a| und kgV(a,b)=|b|*

Lemma 1.4 (Satz von Bezout)**.** *Wenn d=ggT(a,b), dann* $\exists s,t \in \mathbb{Z} : d = as + bt$

Bemerkung. *Es gilt **nicht** umgekehrt für Satz von Bezout. Also* $0 \cdot a + 0 \cdot b = 0$ *aber für* $a, b \neq 0 \Rightarrow ggT(a,b) \neq 0$

Corollary 1.4.1. *Für* $a, b \in \mathbb{Z}$ *gilt* $ggT(a,b) = 1 \Leftrightarrow \exists s,t \in \mathbb{Z} : sa + bt = 1$

Lemma 1.5. *Seien* $a, b \in \mathbb{Z}$ *und q,r aus Satz 1.2. Dann gilt ggT(a,b) = ggT(b,r)*

1.6 Gruppen, Ringe, Körper

Definition 1.14. Eine innere Verknüpfung ist eine Abbildung $* : M \times M \longrightarrow M$. Weiterhin heißt die Abbildung *

a. *Assoziativ*

$$a * (b * c) = (a * b) * c, \quad \forall a, b, c \in M \tag{4}$$

b. *Kommutativ*

$$a * b = b * a, \quad \forall a, b, \in M \tag{5}$$

Ein Element $e \in M$ heißt neutrales Element für *

$$\Leftrightarrow \underbrace{e * m}_{\text{link neutral}} = \underbrace{m * e}_{\text{recht neutral}} = m \quad \forall m \in M \tag{6}$$

Bemerkung. *Wenn ein neutrales Element existiert, dann ist es eindeutig. Ein inverses Element von m ist ein m' wobei $m' * m = m * m' = e$*

Definition 1.15. Eine Gruppe ist ein geordnetes Paar (G,*), wobei G ist eine Menge und $* : G \times G \longrightarrow G$ die folgendes erfüllt

- (Gr.1) * ist assoziativ
- (Gr.2) $\exists e \in G$, $e =$ neutrales Element für *
- (Gr.3) $\forall g \in G \quad \exists g^{-1} \in G : g * g^{-1} = g^{-1} * g = e$

Definition 1.16 (Untere Gruppe)**.** Eine Untegruppe einer Gruppe $(G, *)$ ist eine Teilmenge $H \subseteq G$ die folgende Axiome erfüllt

- (UG1) $\forall h_1, h_2 \in H$ gilt $h_1 * h_2 \in H$
- (UG2) Das neutrale Element e von G liegt auch in H
- (UG3) $\forall h \in H$ gilt $h^{-1} \in H$

Definition 1.17 (Erzeugte Untergruppe)**.** Sei $S \subseteq G$ eine Teilmenge der Menge G. Die von S erzeugte Untegruppe von G ist die kleinste Untegruppe H, wobei $H \leq G$ und $S \subseteq H$. Also $H = \mathrm{Span}_{\mathbb{K}} S = \{a \in S\} \cup \{a^{-1} : a \in S\}$

Definition 1.18. Ein Ring ist ein Tripel $(R, +, \cdot)$ wobei

$$\begin{cases} + : R \times R \longrightarrow R \\ \cdot : R \times R \longrightarrow R \end{cases}$$

- (R1) $(R, +)$ ist eine kommutative Gruppe
- (R2) $\cdot$ ist assoziativ und hat ein neutrales Element
- (R3) $(a + b)c = ac + bc$ und $a(b + c) = ab + ac \quad \forall a, b, c \in R$ (Dsitributiv Gesetz)

Bemerkung. *Ein Ring heißt kommutativ wenn $\cdot$ kommutativ ist.*

Definition 1.19. Ein Körper ist ein Tripel $(K, +, \cdot)$ wobei K =Menge,

$$\begin{cases} + : K \times K \longrightarrow K \\ \cdot : K \times K \longrightarrow K \end{cases}$$

- (K1) $(K, +)$ ist eine kommutative Gruppe
- (K2) $(K \setminus \{0\}, \cdot)$ ist eine kommutative Gruppe
- (K3) $(a + b)c = ac + bc$ und $a(b + c) = ab + ac \quad \forall a, b, c \in K$

Definition 1.20 (Teilkörper)**.** Sei $\mathbb{K}$ =Körper. Eine Teilmenge $L \subseteq K$ heißt ein Teilkörper von $\mathbb{K}$, wenn gilt:

- (TK1) $\forall a, b \in \mathbb{L} : a + b, a \cdot b \in \mathbb{L}$
- (TK2) $0, 1 \in \mathbb{L}$
- (TK3) $a \in \mathbb{L} \Rightarrow -a \in \mathbb{L}$
- (TK4) $a \in \mathbb{L}, a \neq 0 \Rightarrow a^{-1} \in \mathbb{L}$

Definition 1.21 (Gruppenhomomorphismus)**.** Seien $(G_1, *)$ und $(G_2, \star)$ zwei Gruppen. Ein Gruppenhomomorphismus von G_1 nach G_2 ist eine Abbildung $\varphi : G_1 \to G_2$ mit der Eigenschaft

$$\varphi(g * g') = \varphi(g) \star \varphi(g') \quad \forall g, g' \in G_1 \tag{7}$$

Definition 1.22 (Gruppenisomorphismus)**.** Sei φ ein Gruppenhomomorphismus. φ ist ein Gruppenisomorphismus $\Leftrightarrow \exists \varphi^{-1} : \varphi^{-1} =$ Gruppenhomomorphismus.
Zwei Gruppen G_1 und G_2 sind isomorph ($G_1 \simeq G_2$), wenn es ein Gruppenisomorphismus gibt.

Die Definitionen von Iso- und Homomorphismus sind analog für andere Strukturen.

Beispiel 1.4 (Ringhomomorphismus)**.** *Das Tripel $(Mat_{2\times2}(\mathbb{R}, +, \cdot))$ ist ein nicht-kommutativer Ring (da Matrixmultiplikation nicht kommutativ ist und eine inverse Matrix existiert nicht immer für jede Matrix $\in Mat_{2\times2}$). $\mathbb{R}$ ist ein Körper und daher auch ein Ring. Definieren wir eine Abbildung $f : \mathbb{R} \to Mat_{2\times2}(\mathbb{R})$, wobei*

$$f : r \mapsto \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix}$$

Dann f ist ein Ringhomomorphismus, da es gilt

$$\begin{aligned} f(r+s) &= \begin{pmatrix} r+s & 0 \\ 0 & r+s \end{pmatrix} = \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix} + \begin{pmatrix} s & 0 \\ 0 & s \end{pmatrix} = f(r) + f(s) \\ f(rs) &= \begin{pmatrix} rs & 0 \\ 0 & rs \end{pmatrix} = \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix} \begin{pmatrix} s & 0 \\ 0 & s \end{pmatrix} = f(r)f(s) \end{aligned} \tag{8}$$

Beispiel 1.5 (Ring von ganzen Zahlen modulo n). *$\mathbb{Z}/n\mathbb{Z}$ ist die Die Menge aller Kongruenzklassen der ganzen Zahlen für einen Modulo n, wobei für $n > 0$*

$$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], ..., [n-1]\} \tag{9}$$

Die Addition ($+_n$) und die Multiplikation $\cdot_n$ von modulo n als:

$$\begin{array}{ll} +_n : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} & [a] +_n [b] := [a+b] \\ \cdot_n : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} & [a] \cdot_n [b] := [a \cdot b] \end{array} \tag{10}$$

Die Modulare Operationen haben die folgende Eigenschaften:

1. $\forall [a], [b], [c] \in \mathbb{Z}/n\mathbb{Z}$ *gilt* $[a] +_n ([b] +_n [c]) = ([a] +_n [b]) +_n [c]$ *und* $[a] \cdot_n ([b] \cdot_n [c]) = ([a] \cdot_n [b]) \cdot_n [c] \Rightarrow$ *die Addition($+_n$) und Multiplikation($\cdot_n$) sind assoziativ*
2. $\forall [a] \in \mathbb{Z}/n\mathbb{Z}$ *gilt* $[0] +_n [a] = [a] +_n [0] = [a]$ *und* $[1] \cdot_n [a] = [a] \cdot_n [1] = [a] \Rightarrow +_n$ *und* $\cdot_n$ *jeder hat ein neutrales Element*
3. $\forall [a] \in \mathbb{Z}/n\mathbb{Z}$ *gilt* $[a] +_n [-a] = [0] \Rightarrow$ *Es existiert ein inverses Element für alle* $a \in \mathbb{Z}/n\mathbb{Z}$
4. $\forall [a], [b] \in \mathbb{Z}/n\mathbb{Z}$ *gilt* $[a] +_n [b] = [b] +_n [a]$ *und* $[a] \cdot_n [b] = [b] \cdot_n [a] \Rightarrow$ *die Addition($+_n$) und Multiplikation($\cdot_n$) sind kommutativ*
5. $\forall [a], [b], [c] \in \mathbb{Z}/n\mathbb{Z}$ *gilt*

$$\begin{aligned} [a] \cdot_n ([b] +_n [c]) &= [a] \cdot_n [b+c] \\ &= [a \cdot (b+c)] \\ &= [a \cdot b + a \cdot c] \\ &= [a \cdot b] +_n [a \cdot c] \\ &= [a] \cdot_n [b] +_n [b] \cdot_n [c] \end{aligned} \tag{11}$$

   Analog gilt auch $([a] +_n [b]) \cdot_n [c] = ([a] \cdot_n [c]) +_n ([b] \cdot_n [c])$
   $\Rightarrow$ *Distributivgesetz*

Es ist auch offensichtlich, dass $\mathbb{Z}/n\mathbb{Z}$ anhand dem Multiplikation Operation $\cdot_n$ ein kommutativer Ring ist.

Beispiel 1.6 ($\mathbb{Z}/p\mathbb{Z}$). *$\mathbb{Z}/n\mathbb{Z}$ ist ein Körper $\Leftrightarrow$ $n =$ primzahl*

Anhand dem Beispiel 1.5 $\Rightarrow$ $\mathbb{Z}/n\mathbb{Z}$ ist ein Ring.

Beweis:

$\boxed{\Leftarrow}$ *Nehmen wir an $n =$ primzahl und $[a] \neq [0] \Rightarrow a$ und n sind teilerfremd $\Rightarrow ggT(a,n) = 1 \overset{Corr1.3.1}{\Longrightarrow} \exists s, t \in \mathbb{Z} : sa + nt = 1$. Wir können diese Gleichung in Operatoren von $\mathbb{Z}/n\mathbb{Z}$ überführen. Da $[n] = [0]$, dann haben wir $[s \cdot a] = [a \cdot s] = [s] \cdot_n [a] = [a] \cdot_n [s] = [1]$. Also gilt es $\forall [x] \in (\mathbb{Z}/p\mathbb{Z}, \cdot_p), [x] \neq [0] \quad \exists [x^{-1}] \in (\mathbb{Z}/p\mathbb{Z}, \cdot_p) : [x] \times [x^{-1}] = [x^{-1}] \times [x] = [1]$.*

$\boxed{\Rightarrow}$ *Nehmen wir an $\mathbb{Z}/n\mathbb{Z}$ ist ein Körper $\Rightarrow \forall [a] : 0 < a < n \exists a^{-1}$, s.d $[a] \cdot_p [a^{-1}] = [1] \Rightarrow \exists k : a \cdot a^{-1} + k \cdot n = 1 \Rightarrow gcd(a,n) = 1 \Rightarrow n =$ Primzahl*

2 Additional material - Solving equations

Definition 2.1 (Matrix)**.** Seien $m, n \in \mathbb{N}^{\times}$ und sei R ein Ring. Eine $(m \times n)$-Matrix mit Einträge in R ist eine Abbildung

$$A : \{1, \ldots, n\} \times \{1, \ldots, m\} \longrightarrow R \tag{12}$$

Wir bezeichnen $a_{i,j} := A(i, j)$ und stellen A als eine Tabelle dar

$$A = (a_{ij})_{i=1,\ldots,m} = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & \ldots & \vdots \\ a_{m1} & \ldots & a_{mn} \end{pmatrix} \tag{13}$$

Die Menge aller $(m \times n)$-Matrizen mit Einträge in R wird mit $\mathrm{Mat}_{m\times n}(R)$ bezeichnet.

Definition 2.2 (Row operations)**.** A row operation on a matrix is one of three operations:

- Multiplying a row by a nonzero number
- Adding a multiple of a row onto another row
- Exchanging two rows

Definition 2.3 (Echelon form)**.** A matrix is in echelon form if:

1. In every row, the first nonzero is 1, called a pivotal 1.
2. The pivotal 1 of a lower row is always to the right of the pivotal 1 of an upper row
3. In every column that contains a pivotal 1, all other entries are 0.
4. Any rows consisting entirely of 0's are at the bottom.

Satz 2.1 (Solution of $A\mathbf{x} = \mathbf{b}$ unchanged by row operations)**.** *. If the matrix $[A|\mathbf{b}]$ can be turned into $[A'|\mathbf{b}']$ by a sequence of row operations, then the set of solutions to $A\mathbf{x} = \mathbf{b}$ coincide with that to $A'\mathbf{x} = \mathbf{b}'$.*

Satz 2.2. *Given any matrix A, there exists a unique matrix $\tilde{A}$ in echelon form that can be obtained from A by row operations*

Algorithm 2.1 (Row reduction)**.** *To bring a matrix to echelon form*

1. *Find the first column that is not all 0's; call this the first pivotal column and call its first nonzero entry a pivot. If the pivot is not in the first row, move the row containing it to the first row position*
2. *Divide the first row by the pivot, so that the first entry of the first pivotal column is 1*
3. *Add appropriate multiples of the first row to other rows to make all other entries of the first pivotal column 0. The 1 in the first column is now a pivotal 1*
4. *Choose the next column that contains at least 1 nonzero entry beneat the first row, and put the row containing the new pivot in second row position. Make the pivotal a pivotal 1.*
5. *Repeat until the matrix is in echelon form. Each time choose the first column that has a nonzero entry in a lower row that the lowest row containing a pivotal 1, and put the row containg that entry directly below the lowest row containing a pivotal 1.*

Satz 2.3 (Solutions to linear equations)**.** *Given $A\mathbf{x} = \mathbf{b}$, whereby A is a $m \times n$ matrix which row reduces to $[\tilde{A}|\tilde{b}]$. Then*

1. *If $\tilde{b}$ contains a pivotal 1, the system has no solutions.*
2. *If $\tilde{b}$ does not contain a pivotal 1, solutions are uniquely determined by the values of the nonpivotal variables*
   - *If each column of $\tilde{A}$ contains a pivotal 1 (no nonpivotal variables), the system has a unique solution.*
   - *If at least one variable is nonpivotal (represented by the nonpivotal column of $\tilde{A}$), the values of the nonpivotal variables can be chosen freely and these values uniquely determine the values of the pivotal variables. There is exactly one solution for each value of the nonpivotal variables.*

Definition 2.4 (Pivotal column, pivotal variable)**.** A column of A is pivotal if the corresponding column of $\tilde{A}$ contains a pivotal 1. The corresponding variable in the domain is called a pivotal variable.

Satz 2.4 (Unique solution). $A\mathbf{x} = \mathbf{b}$ *has a unique solution for every* $\mathbf{b}$ *iff* A *row reduces to the identity*

Proof If $\tilde{A} = I$, then $I\mathbf{x} = \tilde{\mathbf{b}} \Rightarrow \mathbf{x} = \tilde{\mathbf{b}}$ is a unique solution to $\tilde{A}\mathbf{x} = \tilde{\mathbf{b}}$. Satz 2.1 $\Rightarrow \mathbf{x} = \tilde{\mathbf{b}}$ is a unique solution to $A\mathbf{x} = \mathbf{b}$

Bemerkung. n *linearly independent vectors in* $\mathbb{R}^n$ *span* $\mathbb{R}^n$*: the matrix* A *formed using those vectors as columns row reduces to the identity, so there is a pivotal 1 in every column and every row.*

Bemerkung. *A square matrix A is one to one iff it is onto*

$$\begin{aligned} A \text{ one to one} &\iff \text{every column of } \widetilde{A} \text{ contains a pivotal } 1 \\ &\iff \text{every row of } \widetilde{A} \text{ contains a pivotal } 1 \\ &\iff A \text{ is onto.} \end{aligned}$$

Satz 2.5 (Wide matrices). *Let* $A \in Mat_{m\times n}$ *and let* $T(x) = Ax, T : \mathbb{R}^n \to \mathbb{R}^m$ *be the associated matrix transformation. If* $m < n$*,* T *is not injective.*

Proof Satz 2.3 2. second bullet point

Satz 2.6 (Tall matrices). *Let* $A \in Mat_{m\times n}$ *and let* $T(x) = Ax, T : \mathbb{R}^n \to \mathbb{R}^m$ *be the associated matrix transformation. If* $m > n$*,* T *is either bijective or not surjective .*

Proof Satz 2.3 1. and 2. first bullet point

Corollary 2.6.1 (Solving several system of equations simultaneously). *Several systems of* n *linear equations in* n *unknowns, with the same coefficients (e.g.* $A\mathbf{x} = \mathbf{b}_1, ..., A\mathbf{x} = \mathbf{b}_k$*) can be solved at once with row reduction.*

$$[A \mid \mathbf{b}_1, .., \mathbf{b}_k] \text{ row reduced to } [\tilde{A} \mid \tilde{\mathbf{b}_1}, .., \tilde{\mathbf{b}_k}]$$

If $\tilde{A} = I$*, then* $x = \tilde{\mathbf{b}_i}$ *is the solution to the ith equation* $A\mathbf{x} = \mathbf{b}_i$

Satz 2.7 (Computing inverse of a mtrix). *If* $A \in Mat_{n\times n}$ *has an inverse* A^{-1}*, the inverse can be determined as follows*

$$[A|I] \text{ row reduced to } [I|A^{-1}]$$

Proof Based on Corollary 2.6.1, row reducing $[A|I]$ is equivalent to finding x_i so that $Ax_i = e_i$ for all $i = 1, ..., n$. Thus, when $\tilde{A} = I$, one gains a matrix $X \in \text{Mat}_{n\times n}$, such that $AX = I \Rightarrow X = A^{-1}$.

3 Abstrakt $\mathbb{K}$-Vektorraum

Definition 3.1 ($\mathbb{K}$-Vektorraum)**.** Sei $\mathbb{K}$ ein Körper, ist ein $\mathbb{K}$-Vektorraum ein Tripel $(V, +, \cdot)$ wobei V =Menge

$$\begin{aligned} + &: V \times V \longrightarrow V \quad \text{innere Verknüpfung, Vektoraddition} \\ \cdot &: \mathbb{K} \times V \longrightarrow V \quad \text{äußere Verknüpfung, skalare Multiplikation} \end{aligned} \tag{14}$$

, s.d. folgende Axiome gelten

- (VR1) (V,+)=albesche Gruppe
- (VR2.1) $(\lambda + \mu) \cdot \vec{v} = \lambda \cdot \vec{v} + \mu \cdot \vec{v} \quad \forall \lambda, \mu \in \mathbb{K}$ und $\vec{v} \in V$
- (VR2.2) $\lambda \cdot (\vec{v} + \vec{w}) = \lambda \cdot \vec{v} + \lambda \cdot \vec{w} \quad \forall \lambda \in \mathbb{K}$ und $\vec{v}, \vec{w} \in V$
- (VR2.3) $(\lambda\mu) \cdot \vec{v} = \lambda \cdot (\mu \cdot \vec{v}) \quad \forall \lambda, \mu \in \mathbb{K}$ und $\vec{v} \in V$
- (VR2.4) $1 \cdot \vec{v} = \vec{v} \quad \forall \vec{v} \in V$, wobei $1 \in \mathbb{K}$

Lemma 3.1. *Für jeden $\mathbb{K}$-Vektorraum V gelten*

1. $\lambda \cdot \vec{0_V} = \vec{0_V} \ \forall \lambda \in \mathbb{K}$.
2. $0_{\mathbb{K}} \cdot \vec{v} = 0_V \ \forall \vec{v} \in V$.
3. $(-\lambda) \cdot \vec{v} = \lambda \cdot (-v) = -(\lambda \cdot \vec{v}) \ \forall \lambda$
4. *Aus $\lambda \cdot \vec{v} = \vec{0_V}$ für $\lambda \in \mathbb{K}$ und $\vec{v} \in V$ folgt $\lambda = 0_{\mathbb{K}}$ oder $\vec{v} = \vec{0_V}$*

Proof *(Lemma 3.1.4).*

Fall 1: $\lambda = 0 \xrightarrow{\text{Lemma 3.1.2.}} \checkmark$

Fall 2: $\lambda \neq 0 \xrightarrow{\mathbb{K}=\text{Körper}} \exists \lambda^{-1} \in K : \lambda\lambda^{-1} = \lambda^{-1}\lambda = 1$. Dann gilt

$$\lambda\vec{v} = \vec{0_V} \Rightarrow \lambda^{-1}(\lambda\vec{v}) \overset{VR2.3}{=} (\lambda^{-1}\lambda)\vec{v} = \vec{0_v}$$

□

Bemerkung. *Der unterliegende Körper $\mathbb{K}$ von V spielt eine größe Rolle im Beweis von Lemma 3.1.4 für den 2. Fall. Sei $\mathbb{X}$ eine beliebige Struktur, gilt die Aussage von Lemma 3.1.1 im Allgemein nicht.*
Gegenbeispiel Sei $\mathbb{K} = \mathbb{Z}$ und $V = \mathbb{Z}/6\mathbb{Z}$, es gilt

$$2 \cdot [3] = [6] = [0]$$

Beispiel 3.1. $\mathbb{K} \subseteq \mathbb{L}$ *($\mathbb{K}$ ist ein Teilkörper von $\mathbb{L}$) $\Rightarrow \mathbb{L}$ ist ein $\mathbb{K}$-VR* $(\mathbb{L}, +_{\mathbb{L}}, \cdot_{\mathbb{L}})$

$$\begin{aligned} +_{\mathbb{L}} &: \mathbb{L} \times \mathbb{L} \to \mathbb{L} \\ \cdot_{\mathbb{L}} &: \mathbb{K} \times \mathbb{L} \to \mathbb{L} \end{aligned} \tag{15}$$

Beispiel 3.2 ($\mathbb{K}$-wertige Funktionen)**.** *sind Abbildungen $f : X \to \mathbb{K}$ für eine beliebige Menge X. Wir definieren $Abb(X, \mathbb{K}) = \{f : X \to \mathbb{K}\}$. $Abb(X, \mathbb{K})$ hat eine $\mathbb{K}$-VR Struktur durch*

$$\begin{aligned} f + g &: X \longrightarrow \mathbb{K}, \quad x \mapsto f(x) + g(x) \\ \lambda \cdot f &: X \longrightarrow \mathbb{K}, \quad x \mapsto \lambda f(x). \end{aligned} \tag{16}$$

Wir haben $0_{func} : X \longrightarrow \mathbb{K}$ mit $x \mapsto 0, \forall x \in X$ und $-f : X \longrightarrow \mathbb{K}$ mit $x \mapsto -f(x), \forall x \in X$.

3.1 $\mathbb{K}$-UVR und Erzeugersystem

Definition 3.2 ($\mathbb{K}$-Untervektorraum)**.** Sei $V = \mathbb{K}$-Vektorraum. Ein $\mathbb{K}$-Untervektorraum von V ($\mathbb{K}$-UVR_V) ist eine Teilmenge $U \subseteq V$ mit den Eigenschaften:

- (UVR1) $U \neq \emptyset$
- (UVR2.3) $\forall \vec{v}, \vec{w} \in U, \forall \lambda, \mu \in \mathbb{K}$ gilt $\lambda \cdot \vec{v} + \mu \cdot \vec{w} \in U$

Definition 3.3 (Nullvektor und Nullraum)**.** Jeder $\mathbb{K}$-Vektorraum V enthält den Nullvektor $\vec{0}$, welches das neutrale Element der Gruppe $(V, +)$ ist. Eine einlementige $V = \{\vec{0}\}$ heißt der Nullraum und er hat 2 folgende Operationen.

$$\begin{aligned} \vec{0} + \vec{0} &= \vec{0} \\ \lambda \cdot \vec{0} &= \vec{0} \quad \forall \lambda \in \mathbb{K} \end{aligned} \tag{17}$$

Bemerkung. *$\{\vec{0}\}$ gehört zu allen $\mathbb{K}$-Vektor und Untervektorräumen.*

Definition 3.4 ($\mathbb{K}$-lineare Abbildung)**.** Seien V, W zwei $\mathbb{K}$-Vektorräume. Eine $\mathbb{K}$-lineare Abbildung (oder ein Homomorphismus von $\mathbb{K}$-Vektorräume) von V nach W ist eine Abbildung $f : V \to W$ mit den Eigenschaften

- (LA1) $f(\vec{v_1} + \vec{v_2}) = f(\vec{v_1}) + f(\vec{v_2}), \quad \forall v_1, v_2 \in V$
- (LA2) $f(\lambda v) = \lambda f(v), \quad \forall \lambda \in \mathbb{K}$ und $\forall v \in V$.

Die Menge aller $\mathbb{K}$-linearen Abbildungen von V nach W wird mit $\mathrm{Hom}_{\mathbb{K}}(V, W)$.
Eine $\mathbb{K}$-lineare Abbildung von V nach V heißt $\mathbb{K}$-linearer Endomorphismus von V. Die Menge aller Endomorphismen von V wird mit $\mathrm{End}_{\mathbb{K}}(V, W)$.
Ein Endomorphismus der auch ein Isomorphismus ist, heißt $\mathbb{K}$-linearer Automorphismus von V. Die Menge aller Automorphismen von V wird mit $\mathrm{Aut}_{\mathbb{K}}(V, W)$.
Der Kern von f wird definiert als $\mathrm{Ker}(f) := \{\vec{v} \in V : f(\vec{v}) = \vec{0_W}\}$

Bemerkung. *Warum ist $\mathbb{K}$-lineare Abbildung ein $\mathbb{K}$-VR Homomorphismus? $\to$ Umschreiben (LA1) und (LA2)*

$$\begin{aligned} f(v_1 +_V v_2) &= f(v_1) +_W f(v_2), \quad \forall v_1, v_2 \in V \\ f(\lambda \cdot_V v) &= \lambda \cdot_W f(v), \quad \forall \lambda \in \mathbb{K} \quad \textit{und} \quad \forall v \in V \end{aligned}$$

Bemerkung. *$f : (V, +) \longrightarrow (W, +)$ ist ein Gruppenhomomorphismus und es gelten*

- $f\left(\vec{0_V}\right) = \vec{0_W}$.
- $f(-\vec{v}) = -f(\vec{v})$
- *f ist injektiv genau dann, wenn* $\mathrm{Ker}(f) := \left\{\vec{v} \in V : f(\vec{v}) = \vec{0_W}\right\} = \left\{\vec{0_V}\right\}$

Lemma 3.2. *Sei V ein $\mathbb{K}$-VR und $(U_i)_{i \in I}$ eine nicht-leere Familie von $\mathbb{K}$-UVR. Dann ist $U = \bigcap_{i \in I} U_i$ ein $\mathbb{K}-UVR_V$.*

Definition 3.5 (Lineare Hülle)**.** Sei V ein $\mathbb{K}$-VR und $A \subseteq V$ eine Teilmenge. Dann ist

$$\langle A \rangle := \left\{ \sum_{i=1}^{r} \alpha_i a_i ; r \in \mathbb{N}, \alpha_i \in K, a_i \in A \text{ für } i = 1, \ldots, r \right\} = \bigcap_{\substack{A \subseteq U \subseteq V \\ U = \mathbb{K}-UVR_V}} U \tag{18}$$

der kleinste UVR in V, der A enthält. Der von A in V erzeugte $\mathbb{K}$-UVR $\langle A \rangle$ ist die lineare Hülle von A in V.

Bemerkung. *$\langle A \rangle$ ist der kleinste $\mathbb{K} - UVR_V$ der A enthält $\Leftrightarrow \langle A \rangle = \min\{U : A \subseteq \langle A \rangle \subseteq U \subseteq V, \quad U = \mathbb{K} - UVR_V\}$. Also*

$$W = \langle A \rangle \Longleftrightarrow \begin{cases} W = \mathbb{K} - UVR_V & \textit{und} \\ A \subseteq W & \textit{und} \\ \forall\ \mathbb{K} - UVR_V\ \ U \textit{ mit } A \subseteq U \textit{ gilt } W \subseteq U \end{cases} \tag{19}$$

Bemerkung. *Sei U ein $\mathbb{K} - UVR_V$ und $S, t \subseteq V$ beliebige Teilmengen. Dann gilt*

- $U = \langle U \rangle$
- $S \subseteq T \Rightarrow \langle S \rangle \subseteq \langle T \rangle$
- $\langle \emptyset \rangle = \langle \{\vec{0}\} \rangle = \{\vec{0}\}$

Definition 3.6 (Summe von UVR)**.** Sei U_1, U_2 zwei $\mathbb{K} - UVR_V$. Die Summe von U_1 und U_2 ist der $\mathbb{K} - UVR_V$

$$U_1 + U_2 := \langle U_1 \cup U_2 \rangle \tag{20}$$

Satz 3.3. *Wenn U_1, U_2 zwei $\mathbb{K} - UVR_V$ sind, dann gilt*

$$U_1 + U_2 = \{v_1 + v_2 \quad : \quad v_1 \in U_1, v_2 \in U_2\} \tag{21}$$

Lemma 3.4. *Seien U_1, U_2 zwei $\mathbb{K} - UVR_V$. Es gilt*

$$U_1 \cup U_2 = U_1 + U_2 \Leftrightarrow U_1 \subseteq U_2 \quad \textit{oder} \quad U_2 \subseteq U_1 \tag{22}$$

Lemma 3.5. *Seien $S, T \subseteq V$, $T \subseteq S$ zwei Mengen von Vektoren. Es gilt*

$$\langle T \rangle = \langle S \rangle \Longleftrightarrow v \in \langle T \rangle, \quad \forall v \in S. \tag{23}$$

If you have time, add the proof for Lemma 3.4 and 3.5

Definition 3.7 (Erzeugersystem)**.** Sei V ein $\mathbb{K} - VR$. Ein Erzeugersystem von V ist eine Menge $S \subseteq V$ mit der Eigenschaft, dass

$$V = \langle S \rangle \tag{24}$$

Ein $\mathbb{K} - VR$ heißt endlich erzeugt wenn es eine endliche Menge S (i.e. $|S| < \infty$) gibt mit $V = \langle S \rangle$.
Eine Menge $S \subseteq V$ ist ein minimales Erzeugersystem (bzg. der Inklusion) von V ist wenn folgende zwei Bedingungen erfüllt sind:

- $\langle S \rangle = V$
- $\langle S \backslash v \rangle \neq V, \quad \forall v \in S$ (i.e. $\langle T \rangle \neq \langle S \rangle, \quad \forall T \subsetneq S$)

If you have time, add the proof for min.Erzeugersystem

3.2 Lineare Abhängigkeit

Definition 3.8 (Lineare Unabhängigkeit)**.** Sei $S = \{v_1, v_2, .., v_n\} \subseteq V$. S ist lineare unabhängig $\Leftrightarrow$ Aus $\lambda_1 v_1 + \cdots + \lambda_n v_n = 0$, mit $\lambda_i \in \mathbb{K}$ notwendig $\lambda_1 = \cdots = \lambda_n = 0$ folgt.
Eine bel. unendliche Teilmenge $S \subseteq V$ ist lin. unabhängig $\Leftrightarrow$ Jede endliche Teilmenge von S ist lin.unabhängig.
S ist lin.abhhängig $\Leftrightarrow$ S ist nicht lin. unabhängig $\Leftrightarrow \exists(\lambda_1, ..., \lambda_n) \neq (0, ..., 0)$ s.d $\lambda_1 v_1 + \cdots + \lambda_n v_n = 0$

Bemerkung. *Wenn $S = \{v_1, v_2, .., v_n\}$ lin. unabhängig ist, dann gelten*

- $v_i \neq 0$
- $v_i \neq v_j, \forall i \neq j$
- $T \subseteq S \Rightarrow T =$ *lin. unabhängig*

Satz 3.6. *Sei $S \subseteq V, S \neq \emptyset$. $S =$ lin. unabhängig $\Leftrightarrow v \notin \mathrm{Span}_{\mathbb{K}}(S \backslash v), \forall v \in S$*

Bemerkung. *$S \subseteq V$ ist eine maximale linear unahängige Menge, wenn folgende 2 Bedingungen erfüllt sind:*

- *$S =$ lin. unabhängig*
- *$S \cup \{v\} =$ lin.abhängig $\forall v \in V \backslash S$*

Satz 3.7. *Sei $S \subseteq V, S \neq \emptyset$*

$$S \textit{ist lin. unabh} \Leftrightarrow v \notin \mathrm{Span}_{\mathbb{K}}(S \backslash v) \forall v \in S$$

Definition 3.9 (Basis)**.** Eine Teilmenge $B \subseteq V$ ist eine Basis von V, wenn die folgende Axiome erfüllt sind:

- (B1) S=lin. unabhängig
- (B2) $\langle S \rangle$=V

Bemerkung. *Sei $V = \mathbb{K}$-VR, $S \subseteq V$*

- $v \in \mathrm{Span}_{\mathbb{K}} S \Leftrightarrow \exists \lambda_1, \ldots, \lambda_n, v_1, \ldots, v_m \in S : v = \sum^n \lambda_i v_i$
- $v \in$ *Basis von V* $\Leftrightarrow \exists! \lambda_1, \ldots, \lambda_n, v_1, \ldots, v_n \in B_V : v = \sum^n \lambda_i v_i$

Bemerkung. *Äquivalente Aussagen sind:*

- B *ist eine Basis von* V
- B *ist das minimales Erzeugersystem von* V
- B *ist eine maximale linear unabhängige Menge in* V
- $\langle B \rangle$ *ist linear unabhängig.*

Bemerkung. *Wenn* $\{v_1, .., v_n\}$ *eine Basis von* V *ist, dann gilt*

$$\forall v \in V, \exists! \lambda_1, \ldots, \lambda_n \in \mathbb{K} \text{ so dass } v = \lambda_1 v_1 + \cdots + \lambda_n v_n \tag{25}$$

Lemma 3.8 (Zornsche Lemma)**.** *Sei* $(M, \leq)$ *eine geordnete Menge. Wenn jede total geordnete Teilmenge* $N \subseteq M$ *eine obere Schranke in* M *hat, dann existiert ein maximales Element in* M

- *Total geordnet:* $\forall n, n' \in N \Rightarrow n \leq n'$ *oder* $n' \leq n \Leftrightarrow$ *Jede zwei Elemente sind vergleichbar.*
- *Obere Schranke:* $m \in M$ *s.d.* $n \leq m \quad \forall n \in N$
- *Max. Element:* $n_0 \in N$ *s.d.* $n_0 \leq n \Rightarrow n_0 = n$

Das Auswahlaxiom. Zu jeder Menge $\mathcal{P}$ von nicht-leeren Mengen gibt es eine Funktion f die jedem $X \in \mathcal{P}$ ein Element $f(X) \in X$ zuordnet

Satz 3.9. *Sei* $S =$ *E.S für* V*, ein* $\mathbb{K}$*-VR. Wenn* $T \subseteq S =$ *max. l.u Teilmenge von* S *ist, dann* $T =$ *Basis von* V*. Insbesondere, ist jede max. l.u Menge eine Basis von* V*.*

Satz 3.10. *Jeder Vektorraum hat eine Basis*

Corollary 3.10.1. *Jedes E.S eines* $\mathbb{K} - VR$ *enthält eine Basis.* $\rightsquigarrow$ *Sei* V *ein beliebig* $\mathbb{K}$*-VR. Wenn* $S = \{v_1, ..., v_n\} =$ ***endlich*** *E.S von* V*, enthält* S *eine Basis (Satz).*

Bemerkung. *Wenn* $\lambda_1, \ldots, \lambda_n \in \mathbb{K}$ *so dass* $v = \lambda_1 v_1 + \cdots + \lambda_n v_n$ *mit* $\lambda_j \neq 0 \Rightarrow v_j \in \mathrm{Span}_{\mathbb{K}}(v_1, \ldots, \hat{v_j}, \ldots, v_n) = \mathrm{Span}_{\mathbb{K}}(v_1, \ldots, v_n)$.

Satz 3.11 (Ergänzungssatz)**.** *Sei* $V = \mathbb{K}$*-VR,* $T = \{v_1, \ldots, v_m\} \subseteq V$ *eine l.u Menge und* $S = \{w_1, \ldots, w_n\} \subseteq V$ *ein E.S von* V*. Dann gilt*

1. $m \leq n$
2. *Nach eventuellem Umbenennen der Vektoren in* S *gilt* $\mathrm{Span}_{\mathbb{K}}(v_1, \ldots, v_m, w_{m+1}, \ldots, w_n) = V$

Corollary 3.11.1. *Sei* $V =$ *endlich erzeugter* $\mathbb{K}$*-VR. Jedes l.u System in* V *kann zu einer Basis ergänzt werden*

3.3 Dimension

Satz 3.12. *Sei* $V =$ *endlich erzeugter* $\mathbb{K}$*-VR (i.e. existiert mindestens 1 endlich E.S). Wenn* B *und* C *Basen von* V *sind, dann gilt* $|B| = |C|$

Definition 3.10. Sei $V = \mathbb{K}$-VR. Die Dimension von V ist

$$\dim_{\mathbb{K}} V := \begin{cases} n, & \text{falls } V \text{ eine endliche Basis mit } n \text{ Elementen besitzt,} \\ \infty, & \text{falls } V \text{ keine endliche Basis besitzt.} \end{cases} \tag{26}$$

Corollary 3.12.1. *Sei* $V =$ *endlichdimensionaler* $\mathbb{K}$*-VR und* $W \subseteq V$ *ein* $\mathbb{K}$*-UVR. Dann gilt*

1. W *ist endlichdimensional mit* $\dim_{\mathbb{K}} W \leq \dim_{\mathbb{K}} V$*.*
2. *Wenn* $\dim_{\mathbb{K}} W = \dim_{\mathbb{K}} V \Rightarrow W = V$

Satz 3.13. *Seien* V, W *zwei endlichdimensionale* $\mathbb{K}$*-VR. Wenn* $B_V = \{v_1, \ldots, v_n\}$ *eine Basis von* V *ist und* $B_W = \{w_1, \ldots, w_m\}$ *eine Basis von* W *ist, dann ist*

$$B := \{(v_1, \mathbf{0}_W), \ldots, (v_n, \mathbf{0}_W), (\mathbf{0}_V, w_1), \ldots, (\mathbf{0}_V, w_m)\} \tag{27}$$

eine Basis des $\mathbb{K}$*-VR* $V \times W$*. Insbesondere, ist* $V \times W$ *auch ein endlichdimensionaler VR und es gilt*

$$\dim_{\mathbb{K}} V \times W = \dim_{\mathbb{K}} V + \dim_{\mathbb{K}} W \tag{28}$$

4 Lineare Abbildungen

Einige Begriffe zur Erinnerung. Für V und W zwei $\mathbb{K}$-VR, V' und W' die jeweiligen $\mathbb{K}$-UVR, $f : V \to W$ eine $\mathbb{K}$-LA,

- $\operatorname{Ker} f = \{v \in V \mid f(v) = 0\} \subseteq V$
- $\operatorname{Bild} f = \{f(v) \mid v \in V\} = \{w \in W \mid \exists v \in W : f(v) = w\} \subseteq W$
- $f^{-1}(W') = \{v \in V \mid f(v) \in W'\} \subseteq V$
- $f(V') = \{f(v) \mid v \in V'\} \subseteq W$

$\Rightarrow \operatorname{Ker} f = f^{-1}(\{0\})$, $\operatorname{Bild} f = f(V)$

Satz 4.1. *Sei $f : V \to W$ eine $\mathbb{K}$-LA, V und W zwei $\mathbb{K}$-VR, V' und W' die jeweiligen $\mathbb{K}$-UVR.*

1. $f(V') \subseteq_{\mathbb{K}} W$. *Insbesondere ist* $\operatorname{Bild} f = f(V) \subseteq_{\mathbb{K}} W$
2. $f^{-1}(W') \subseteq_{\mathbb{K}} V$. *Insbesondere ist* $\operatorname{Ker}(f) = f^{-1}(\{0\}) \subseteq_{\mathbb{K}} V$
3. $\forall S \subseteq V$ *gilt* $f(\langle S \rangle) = \langle f(S) \rangle$
4. *Wenn eine Familie* $(v_i)_{i \in I}, v_i \in V$ *l.a. ist, dann ist auch die Familie* $(f(v_i))_{i \in I}, f(v_i) \in W$ *l.a. Insbesondere gilt* $\dim_{\mathbb{K}} f(V) \leq \dim_{\mathbb{K}} V$.
5. $f =$*bij.* $\Rightarrow f^{-1} : W \to V$ *eine* $\mathbb{K}$*-LA.*
6. $f =$*Iso.* $\Rightarrow \dim_{\mathbb{K}} f(V) = \dim_{\mathbb{K}} V$.

If you have time, add the proof for Satz 4.1

Satz 4.2 (Dimensionssatz)**.** *Sei $V, W =$ zwei $\mathbb{K}$-VR mit $\dim_{\mathbb{K}} V < \infty$, $f : V \to W$ eine $\mathbb{K}$-LA. Dann gilt*

$$\dim_{\mathbb{K}} V = \dim_{\mathbb{K}} \operatorname{Ker} f + \dim_{\mathbb{K}} \operatorname{Bild} f \tag{29}$$

Satz 4.3 (Dimension of sums)**.** *Sei $V =$ $\mathbb{K}$-VR, U_1, U_2 endlich dimensionale $\mathbb{K}$-UVR von V. Dann gilt*

$$\dim_{\mathbb{K}}(U_1 + U_2) = \dim_{\mathbb{K}} U_1 + \dim_{\mathbb{K}} U_2 - \dim_{\mathbb{K}}(U_1 \cap U_2) \tag{30}$$

Lemma 4.4. *Sei V, W zwei $\mathbb{K}$-VR mit $\dim_{\mathbb{K}} V = \dim_{\mathbb{K}} W < \infty$ sind, und wenn $f \in \operatorname{Hom}_{\mathbb{K}}(V, W)$, dann sind folgende Aussagen äquivalent:*

1. $f =$ *Iso*
2. $f =$ *inj.*
3. $f =$ *surj.*

4.1 Quotientenräume

Definition 4.1 (Affiner Unterraum)**.** Sei $V = \mathbb{K}$-VR, $U \subseteq_{\mathbb{K}} V$. Wir betrachten die folgende ÄR auf V

$$\forall a, b \in V : a \sim_U b \Leftrightarrow a - b \in U \Leftrightarrow a \equiv b \mod U \tag{31}$$

Die ÄK des Vektors $a \in V$ bildet einen affinen Unterraum A.

$$\forall a \in V : [a] = a + U = \{a + u | u \in U\} = A \tag{32}$$

Beweis.
zZ1: Die Relation in Gl.31 ist eine ÄR

- Reflexivität: $a - a = 0 \in U$, da $U = \mathbb{K}$-UVR
- Symmetrie: $a \sim b \Rightarrow a - b \in U \Rightarrow -(a - b) = b - a \in U$, da $U = \mathbb{K}$-UVR $\Rightarrow b \sim a$
- Transitivität: $a \sim b \Rightarrow a - b \in U, b \sim c \Rightarrow b - c \in U \Rightarrow (a - b) + (b - c) = a - c \in U \Rightarrow a \sim c$, da $U = \mathbb{K}$-UVR

zZ2: [a]=a+U
$\boxed{\subseteq}$ Sei $x \in [a] \Rightarrow x \sim a \Rightarrow x - a \in U \Rightarrow x + (x - a) \in x + U$
$\boxed{\supseteq}$ Sei $x \in a + U \Rightarrow \exists u \in U \Leftrightarrow x - a = u \in U \Leftrightarrow x \sim a \Rightarrow x \in [a]$ □

Bemerkung. *Ein affiner Unteraum kann entweder $A = \emptyset$ oder Gl.32*

Die ÄK von $a \in V$ ist der $\mathbb{K}$-UVR U verschoben um den Vektor a. Die Quotientenmenge $V/\sim$ oder $V/U = \{[a] \mid a \in V\} = \{a + U \mid a \in V\}$ ist ein $\mathbb{K}$-VR $(V/U, +, \cdot)$ wobei

$$\begin{aligned} +&: V/U \times V/U \to V/U, \quad [a] + [b] := [a + b] \text{ bzw. } (a + U) + (b + U) := (a + b) + U \\ \cdot&: \mathbb{K} \times V/U \to V/U, \quad \alpha[a] := [\alpha a] \text{ bzw. } \alpha(a + U) := (\alpha a) + U, \quad a, b \in V, \alpha \in \mathbb{K} \end{aligned} \tag{33}$$

Beweis. zZ:$(V/U, +, \cdot) = \mathbb{K}$-VR

- $(V/U, +) =$ albesche Gruppe
  $(V/U, +)$ ist kommutativ wegen der Kommutativität der Addition von Körper $\mathbb{K}$
  Für den Nullvektor $0_{V/U} = [0_V] = U$ gilt $[0_V] + [a] = [0_V + a] = [a]$ bzw. $(0_V + U) + (a + U) = (0_V + a) + U = a + U$
  Sei $[a] \in (V/U, +)$, dann gilt $[a] + [-a] = [-a] + [a] = [-a + a] = [a - a] = [0] \Rightarrow [-a] = [a]^{-1}$
- $(\lambda + \mu)([v] + [w]) = \lambda([v] + [w]) + \mu([v] + [w]) = (\lambda + \mu)[v] + (\lambda + \mu)[w]$
- $(\lambda\mu)[v] = [\lambda\mu v] = \lambda[\mu v]$
- $1 \cdot [a] = [1a] \quad \forall a \in V$

□

Die Operationen $+$ und $\cdot$ von V/U sind wohldefiniert (i.e. sie sind unabhängig von der Wahl des Repräsentanten der ÄK).

Beweis.

- $a' \sim a \Leftrightarrow [a'] = [a] \Leftrightarrow a + U = a' + U$
- $a' \sim a \Leftrightarrow [a'] = [a] \Leftrightarrow \lambda[a'] = \lambda[a] \forall \lambda \in K$

□

Bemerkung. *Jede ÄK modulo U ist ein affiner UVR*

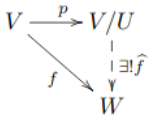
Bemerkung. *Für jeden affinen UVR von V ist der unterliegende $\mathbb{K}-UVR$ eindeutig (d.h. $v+U = v+U' \Rightarrow U = U'$) und $\dim(v + U) = \dim_{\mathbb{K}} U$*

Satz 4.5. *1. Die kanonische Projektion*

$$\begin{aligned} p :& V \to V/U \\ & v \mapsto [v] \end{aligned}$$

ist eine $\mathbb{K}-$LA mit $\operatorname{Ker} p = U$

2. *(universelle Eigenschaft) $\forall \mathbb{K}-$LA $f : V \to W$ mit $U \subseteq \operatorname{Ker} f, \quad \exists! \hat{f} : V/U \to W$ s.d. $\hat{f} \circ p = f$*



(d.h. $\hat{f} \circ p = f$).

   (a) $\hat{f} =$*surj.* $\Leftrightarrow f =$ *surj.*
   (b) $\hat{f} =$*inj.* $\Leftrightarrow \operatorname{Ker} f =$*U*

Corollary 4.5.1. *$\varphi : V \to W = \mathbb{K}$-LA dann gilt*

$$\operatorname{Bild} \varphi \cong V/\operatorname{Ker} \varphi$$

Corollary 4.5.2. *Sei $V = \mathbb{K}$-VR, $\dim_{\mathbb{K}} V < \infty$, $U \subseteq_K V$*

$$\dim_{\mathbb{K}} V/U = dim_{\mathbb{K}} V - \dim_{\mathbb{K}} U \tag{34}$$

Corollary 4.5.3. *Sei $V = \mathbb{K}$-VR, $\dim_{\mathbb{K}} V < \infty$, $U \subseteq_K V$, $B =$ Basis von U, $p : V \to V/U$ die kanonische Projektion und $C \subseteq V$ mit $|C| = |p(C)|$. Dann gilt*

$$p(C) \text{ ist eine Basis von } V/U \iff C \cap B = \emptyset \text{ und } B \cup C \text{ ist eine Basis von } V \ .$$

5 Universal property

Short reminder: An equivalence relation on a set X is a subset $\sim \subseteq X \times X$ (such that if $(x, y) \in \sim \Rightarrow x \sim y$) which is reflexive, symmetric and transitive. The quotient set $X/\sim$ is the set of equivalence classes on X. The canonical projection $\pi : X \to X/\sim$ is the map sending x to its equivalence class under $\sim$.

The quotient set $X/\sim$ can be described in terms of the universal property: it is the *'largest* set which agrees with the equivalence relation $\sim$.On one hand, it is the case that whenever $a \sim b$ in X then $\pi(a) = \pi(b)$. Moreover, for any set Y and any map $g : X \to Y$ which equates equivalent things (i.e. $g(a) = g(b), \quad \forall a \sim b$), then there is a unique map $f : X/\sim \to Y$ such that $f \circ \pi = g$. Graphically, the statement looks like this

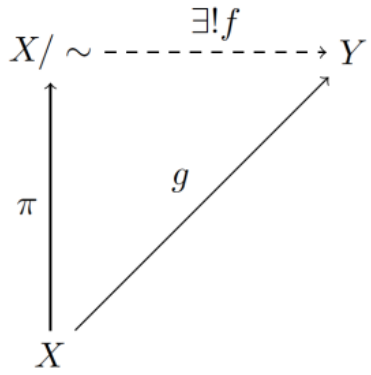
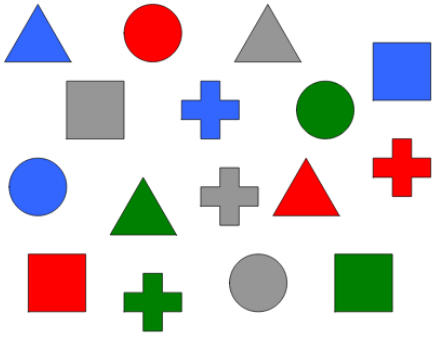


Abbildung 2: Universal property & canonical projection

Beispiel 5.1. *We consider a set X of objects with different properties. We then define an equivalence relation in*

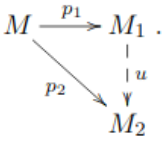


which $a \sim b \Leftrightarrow a$ and b have the same form. Hence, the quotient is {[cross],[triangle], [square], [circle]} and the canonical projection can be defined as $\pi : (color \times form) \to form$. The function g can assign a natural number to a form $g : (color \times form) \to n, n \in \mathbb{N}$ and the function f is a uniquely defined as a map from an equivalence class in $X/\sim$ to a natural number $f : [form] \to n, n \in \mathbb{N}$.

Satz 5.1. *Sei $\sim$ eine ÄR auf die Menge M und $p : M \to M/\sim$ die Quotientenabbildung. Sei $f : M \to A$.*

1. *$\exists\, u : M/\sim \to A$ mit $u \circ p = f \Leftrightarrow p(a) = p(b) \Rightarrow f(a) = f(b)$*
2. *Wenn u existiert, dann gilt*
   (a) *u ist eindeutig.*
   (b) *u ist surjektiv $\Leftrightarrow$ f ist surjektiv.*
   (c) *u ist injektiv $\Leftrightarrow \sim_f = \sim$ (i.e. $p(a) = p(b) \Leftrightarrow f(a) = f(b)$)*

Corollary 5.1.1. *Wenn $p_1 : M \to M_1$ und $p_2 : M \to M_2$ zwei surjektive Abbildung mit $\sim_{p1} = \sim_{p2}$, dann $\exists u : M_1 \to M_2$ s.d. folgendes Diagramm kommutativ ist.*



Glossar

$\mathbb{N}^\times$ for $\mathbb{X} = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, $X^\times := X \backslash \{0\}$. 8

$\subseteq_{\mathbb{K}}$ denotes a $\mathbb{K}$-UVR. 14

Points to cover

- Elementary matrices (Vorlesungskript)
- Proposition 2.3.7
- Explain why $\mathbb{Z}/p\mathbb{Z}$ is a field
- Polynomial ring
- Kernel and image
- Inklusion Ordnungsrelation
- kartesisches Produkt
- $F = \mathbb{K}$-LA , $f =$inj $\Rightarrow \operatorname{Ker} f = \{0\}$