Lineare Algebra 1. Semester (WS2017/18)

Dozent: Prof. Dr. Arno Fehm

1 Grundgegriffe der Linearen Algebra

1.1 Logik und Mengen

Wir werden die Grundlagen der Logik und der Mengenlehre kurz ansprechen.

1.1.1 Überblick über die Aussagenlogik

Jede mathematisch sinnvolle Aussage ist entweder wahr oder falsch, aber nie beides!

- "$1+1=2$" $\to$ wahr
- "$1+1=3$" $\to$ falsch
- "Es gibt unendlich viele Primzahlen" $\to$ wahr

Man ordnet jeder mathematischen Aussage A einen Wahrheitswert "wahr" oder "falsch" zu.
Aussagen lassen sich mit logischen Verknüpfungen zu neuen Aussagen zusammensetzen.

- $\vee \to$ oder
- $\wedge \to$ und
- $\neg \to$ nicht
- $\Rightarrow \to$ impliziert
- $\iff \to$ äquivalent

Sind also A und B zwei Aussagen, so ist auch $A \vee B$, $A \wedge B$, $\neg A$, $A \Rightarrow B$ und $A \iff B$ Aussagen. Der Wahrheitswert einer zusammengesetzen Aussage ist eindeutig bestimmt durch die Wahrheitswerte ihrer Einzelaussagen.

- $\neg(1+1=3) \to$ wahr
- "2 ist ungerade" $\Rightarrow$ "3 ist gerade" $\to$ wahr
- "2 ist gerade" $\Rightarrow$ "Es gibt unendlich viele Primzahlen" $\to$ wahr

A	B	$A \vee B$	$A \wedge B$	$\neg A$	$A \Rightarrow B$	$A \iff B$
w	w	w	w	f	w	w
w	f	w	f	f	f	f
f	w	w	f	w	w	f
f	f	f	f	w	w	w

1.1.2 Überblick über die Prädikatenlogik

Wir werden die Quantoren

- $\forall$ (Allquantor, "für alle") und
- $\exists$ (Existenzquantor, "es gibt") verwenden.

Ist $P(x)$ eine Aussage, deren Wahrheitswert von einem unbestimmten x abhängt, so ist
$\forall x : P(x)$ genau dann wahr, wenn $P(x)$ für alle x wahr ist,
$\exists x : P(x)$ genau dann wahr, wenn $P(x)$ für mindestens ein x wahr ist.

Insbesondere ist $\neg\forall x : P(x)$ genau dann wahr, wenn $\exists x : \neg P(x)$ wahr ist.
Analog ist $\neg\exists x : P(x)$ genau dann wahr, wenn $\forall x : \neg P(x)$ wahr ist.

1.1.3 Überblick über die Beweise

Unter einem Beweis verstehen wir die lückenlose Herleitung einer mathematischen Aussage aus einer Menge von Axiomen, Vorraussetzungen und schon früher bewiesenen Aussagen.
Einige Beweismethoden:

- **Widerspruchsbeweis**
  Man nimmt an, dass eine zu beweisende Aussage A falsch sei und leitet daraus ab, dass eine andere Aussage sowohl falsch als auch wahr ist. Formal nutzt man die Gültigkeit der Aussage $\neg A \Rightarrow (B \wedge \neg B) \Rightarrow A$.
- **Kontraposition**
  Ist eine Aussage $A \Rightarrow B$ zu beweisen, kann man stattdessen die Implikation $\neg B \Rightarrow \neg A$ beweisen.
- **vollständige Induktion**
  Will man eine Aussage $P(n)$ für alle natürlichen Zahlen zeigen, so genügt es, zu zeigen, dass $P(1)$ gilt und dass unter der Induktionsbehauptung $P(n)$ stets auch $P(n+1)$ gilt (Induktionschritt). Dann gilt $P(n)$ für alle n.
  Es gilt also das Induktionsschema: $P(1) \wedge \forall n : (P(n) \Rightarrow P(n+1)) \Rightarrow \forall n : P(n)$.

1.1.4 Überblick über die Mengenlehre

Jede Menge ist eine Zusammenfassung bestimmter wohlunterscheidbarer Objekte zu einem Ganzen. Eine Menge enthält also solche Objekte, die Elemente der Menge. Die Menge ist durch ihre Elemente vollständig bestimmt. Diese Objekte können für uns verschiedene mathematische Objekte, wie Zahlen, Funktionen oder andere Mengen sein. Man schreibt $x \in M$ bzw. $x \notin M$, wenn x ein bzw. kein Element der Menge ist.

Ist $P(x)$ ein Prädikat, so bezeichnet man eine Menge mit $X := \{x \mid P(x)\}$. Hierbei muss man vorsichtig sein, denn nicht immer lassen sich alle x für die $P(x)$ gilt, widerspruchsfrei zu einer Menge zusammenfassen.

Beispiel: endliche Mengen
Eine Menge heißt endlich, wenn sie nur endlich viele Elemente enthält. Endliche Mengen notiert man oft in aufzählender Form: $M = \{1; 2; 3; 4; 5; 6\}$. Hierbei ist die Reihenfolge der Elemente nicht relevant, auch nicht die Häufigkeit eines Elements.
Sind die Elemente paarweise verschieden, dann ist die Anzahl der Elemente die Mächtigkeit (oder Kardinalität) der Menge, die wir mit $|M|$ bezeichnen.

Beispiel: unendliche Mengen

- Menge der natürlichen Zahlen: $\mathbb{N} := \{1, 2, 3, 4, ...\}$
- Menge der natürlichen Zahlen mit der 0: $\mathbb{N}_0 := \{0, 1, 2, 3, 4, ...\}$
- Menge der ganzen Zahlen: $\mathbb{Z} := \{..., -2, -1, 0, 1, 2, ...\}$
- Menge der rationalen Zahlen: $\mathbb{Q} := \{\frac{p}{q} \mid p, q \in \mathbb{Z}, q \neq 0\}$

- Menge der reellen Zahlen: $\mathbb{R} := \{x \mid x \text{ ist eine reelle Zahl}\}$

Ist M eine Menge, so gilt $|M| = \infty$

Beispiel: leer Menge
Es gibt genau eine Menge, die keine Elemente hat, die leere Menge $0 := \{\}$.

Definition Teilmenge: Sind X und Y zwei Mengen, so heißt X eine Teilmenge von Y, wenn jedes Element von X auch Element von Y ist, dass heißt wenn für alle x ($x \in X \Rightarrow x \in Y$) gilt.

Da eine Menge durch ihre Elemente bestimmt ist, gilt $X = Y \Rightarrow (X \subset Y) \wedge (Y \subset X)$. Will man Mengengleichheit beweisen, so genügt es, die beiden Inklusionen $X \subset Y$ und $Y \subset X$ zu beweisen.

Ist X eine Menge und $P(x)$ ein Prädikat, so bezeichnet man mit $Y := \{x \in X \mid P(x)\}$ die Teilmenge von X, die das Prädikat $P(x)$ erfüllen.

Definition Mengenoperationen: Seien X und Y Mengen. Man definiert daraus weitere Mengen wie folgt:
- $X \cup Y := \{x \mid x \in X \vee x \in Y\}$
- $X \cap Y := \{x \mid x \in X \wedge x \in Y\}$
- $X \backslash Y := \{x \in X \mid x \notin Y\}$
- $X \times Y := \{(x, y) \mid x \in X \wedge y \in Y\}$
- $\mathcal{P}(X) := \{Y \mid Y \subset X\}$

Neben den offensichtlichen Mengengesetzen, wie dem Kommutaivgesetz, gibt es auch weniger offensichtliche Gesetze, wie die Gesetze von de Morgan: Für $X_1, X_2 \subset X$ gilt:
- $X \backslash (X_1 \cup X_2) = (X \backslash X_1) \cap (X \backslash X_2)$
- $X \backslash (X_1 \cap X_2) = (X \backslash X_1) \cup (X \backslash X_2)$

Sind X und Y endliche Mengen, so gilt:
- $|X \times Y| = |X| \cdot |Y|$
- $|\mathcal{P}(X)| = 2^{|X|}$

1.2 Abbildungen

1.2.1 Überblick über Abbildungen

Eine Abbildung f von eine Menge X in einer Menge Y ist eine Vorschrift, die jedem $x \in X$ auf eindeutige Weise genau ein Element $f(x) \in Y$ zuordnet. Man schreibt dies als

$$f : \begin{cases} X \to Y \\ x \mapsto y \end{cases}$$

oder $f : X \to Y, x \mapsto y$ oder noch einfacher $f : X \to Y$. Dabei heißt X die Definitions- und Y die Zielmenge von f. Zwei Abbildungen heißen gleich, wenn ihre Definitionsmengen und Zielmengen

gleich sind und sie jedem $x \in X$ das selbe Element $y \in Y$ zuordnen. Die Abbildungen von X nach Y bilden wieder eine Menge, welche wir mit $\mathbf{Abb(}X\mathbf{,}Y\mathbf{)}$ bezeichnen.

Beispiele:

- Abbildungen mit Zielmenge $\mathbb{R}$ nennt man Funktion: $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$
- Abbildungen mit Zielmenge $\subset$ Definitionsmenge: $f : \mathbb{R} \to \mathbb{R}_{\leq 0}, x \mapsto x^2$
  $\to$ Diese Abbildungen sind verschieden, da sie nicht die selbe Zielmenge haben.
- $f : \{0, 1\} \to \mathbb{R}, x \mapsto x^2$
- $f : \{0, 1\} \to \mathbb{R}, x \mapsto x$
  $\to$ Diese Funktionen sind gleich. Sie haben die gleichen Definitions- und Zielmengen und sie ordnen jedem Element der Definitionsmenge das gleiche Element der Zielmenge zu.

Beispiele:

- auf jeder Menge X gibt es die identische Abbildung (Identität)
  $id : X \to X, x \mapsto x$
- allgemein kann man zu jeder Teilmenge $A \subset X$ die Inklusionsabbildung zuordnen
  $\iota_A : A \to X, x \mapsto x$
- zu je zwei Mengen X und Y und einem festen $y_0 \in Y$ gibt es die konstante Abbildung
  $c_{y_0} : X \to Y x \mapsto y_0$
- zu jder Menge X und Teilmenge $A \subset X$ definiert man die charakteristische Funktion
  $\chi_A : X \to \mathbb{R}, \begin{cases} x \mapsto 1 & (x \in A) \\ x \mapsto 0 & (x \notin A) \end{cases}$
- zu jeder Menge X gibt es die Abbildung
  $f : X \times X \to \mathbb{R}, (x, y) \mapsto \delta_{x,y} \begin{cases} 1 & (x = y) \\ 0 & (x \neq y) \end{cases}$

Eigenschaften von Funktionen:

- injektiv: Zuordnung ist eindeutig: $F(m_1) = F(m_2) \Rightarrow m_1 = m_2$
  Bsp: x^2 ist nicht injektiv, da $F(-2) = F(2) = 4$
- surjektiv: $F(M) = N$ $(\forall n \in N \; \exists m \in M \mid F(m) = n)$
  Bsp: $sin(x)$ ist nicht surjektiv, da es kein x für $y = 27$ gibt
- bijektiv: injektiv und surjektiv

Definition Einschränkung: Sei $f : x \mapsto y$ eine Abbildung. Für $A \subset X$ definiert man die Einschränkung/Restrikton von f auf A als die Abbildung $f \mid_A A \to Y, a \mapsto f(a)$.
Das Bild von A unter f ist $f(A) := \{f(a) : a \in A\}$.
Das Urbild einer Menge $B \subset Y$ unter f ist $f^{-1} := \{x \in X : f(x) \in B\}$.
Man nennt $Image(f) := f(X)$ das Bild von f.

Bemerkungen zur abstrakteren Betrachtungsweise:
Man ordnet der Abbildung $f : X \to Y$ auch die Abbildungen $\mathcal{P}(X) \to \mathcal{P}(Y)$ und $\mathcal{P}(Y) \to \mathcal{P}(X)$ auf den Potenzmengen zu. Man benutzt hier das gleiche Symbol $f(\dots)$ sowohl für die Abbildung $f : X \to Y$ als auch für $f : P(X) \to P(Y)$, was unvorsichtig ist, aber keine Probleme bereiten sollte.
In anderen Vorlesungen wird für $y \in Y$ auch $f^{-1}(y)$ statt $f^{-1}(\{y\})$ geschrieben.

Bemerkungen:
Genau dann ist $f : X \to Y$ surjektiv, wenn $Image(f) = Y$

Genau dann ist $f : X \to Y \begin{cases} \text{injektiv} \\ \text{surjektiv} \\ \text{bijektiv} \end{cases}$, wenn $|f^{-1}(\{y\})| = \begin{cases} \leq 1 \\ \geq 1 \\ = 1 \end{cases} \quad \forall y \in Y$

Definition Komposition: Sind $f : X \to Y$ und $g : Y \to Z$ Abbildungen, so ist die Komposition $g \circ f$ die Abbildung $g \circ f := X \to Z, x \mapsto g(f(x))$. Man kann die Komposition auffassen als eine Abbildung $\circ : Abb(Y, Z) \times Abb(X, Y) \to Abb(X, Z)$.

Satz: Die Abbildung von Kompositionen ist assotiativ, d.h. es gilt: $h \circ (g \circ f) = (h \circ g) \circ f$.

Definition Umkehrabbildung: Ist $f : X \to Y$ bijektiv, so gibt es zu jedem $y \in Y$ genau ein $x_y \in X$ mit $f(x_y) = y$, durch $f^{-1} : Y \to X, y \mapsto x_y$ wird also eine Abbildung definiert, die Umkehrabbildung zu f.

Satz: Ist die Abbildung $f : X \to Y$ bijektiv, so gilt $f^{-1} \circ f = id_x$ und $f \circ f^{-1} = id_y$.

Bemerkung:
Achtung, wir verwenden hier das selbe Symbol f^{-1} für zwei verschiedene Dinge: Die Abbildung $f^{-1} : \mathcal{P}(X) \to \mathcal{P}(Y)$ existiert für jede Abbildung $f : X \to Y$, aber die Umkehrabbildung $f^{-1} : Y \to X$ existiert nur für bijektive Abbildungen $f : X \to Y$.

Definition Familie: Seien I und X Mengen. Eine Abbildung $x : I \to X, i \mapsto x_i$ nennt man Familie von Elementen von X mit einer Indexmenge I (oder I-Tupel von Elementen von X) und schreibt diese auch als $(x_i)_{i \in I}$. Im Fall $I = \{1, 2, ..., n\}$ identifiziert man die I-Tupel auch mit den n-Tupeln. Ist $(x_i)_{i \in I}$ eine Familie von Teilmengen einer Menge X, so ist

- $\bigcup X_i = \{x \in X \mid \exists i \in I(x \in X)\}$
- $\bigcap X_i = \{x \in X \mid \forall i \in I(x \in X)\}$
- $\prod X_i = \{f \in Abb(I, X) \mid \forall i \in I(f(i) \in X_i)\}$

Die Elemente von $\prod X_i$ schreibt man in der Regel als Familien $(x_i)_{i \in I}$.

Beispiel: Eine Folge ist eine Familie $(x_i)_{i \in I}$ mit der Indexmenge $\mathbb{N}_0$.

Definition Graph: Der Graph einer Abbildung $f : X \to Y$ ist die Menge $\Gamma f : \{(x, y) \in X \times Y \mid y = f(x)\}$.

Bemerkung: Formal korrekte Definition einer Abbildung:
Eine Abbildung f ist ein Tripel (X, Y, Γ), wobei $\Gamma \subset X \times Y \quad \forall x \in X$ genau ein Paar (x, y) mit $y \in Y$ enthält. Die Abbildungsvorschrift schickt dann $x \in X$ auf das eindeutig bestimmte $y \in Y$ mit $(x, y) \in \Gamma$. Es ist dann $\Gamma = \Gamma_f$.

1.3 Gruppen

Definition Gruppe: Sei G eine Menge. Eine (innere, zweistellige) Verknüpfung auf G ist eine Abbildung $* : G \times G \to G, (x, y) \mapsto x * y$. Das Paar $(G, *)$ ist eine Halbgruppe, wenn das folgende Axiom erfüllt ist:
(G1) Für $x, y, z \in G$ ist $(x * y) * z = x * (y * z)$.
Eine Halbgruppe $(G, *)$ ist ein Monoid, wenn zusätzlich das folgende Axiom gilt:
(G2) Es gibt ein Element $e \in G$, welches für alle $x \in G$ die Gleichung $x * e = e * x = x$ erfüllt. Dieses Element heißt dann neutrales Element der Verknüpfung $*$.

Beispiele:

- Für jede Menge X ist $(Abb(X, Y), \circ)$ eine Halbgruppe mit dem neutralen Element id_x, also ein Monoid.
- $\mathbb{N}$ bildet mit der Addition eine Halbgruppe $(\mathbb{N}, +)$, aber kein Monoid, da die 0 nicht in Fehm's Definition der natürlichen Zahlen gehörte
- $\mathbb{N}_0$ bildet mit der Addition ein Monoid $(\mathbb{N}_0, +)$
- $\mathbb{N}$ bildet mit der Multiplikation ein Monoid $(\mathbb{N}, \cdot)$
- $\mathbb{Z}$ bildet mit der Multiplikation ein Monoid $(\mathbb{Z}, \cdot)$

Satz (Eindeutigkeit des neutralen Elements): Ein Monoid $(G, *)$ hat genau ein neutrales Element.

Definition abelsche Gruppe: Eine Gruppe ist ein Monoid $(G, *)$ mit dem neutralen Element e, in dem zusätzlich das folgende Axiom gilt:
(G3) Für jedes $x \in G$ gibt es ein $x' \in G$ mit $x' * x = x * x' = e$.
Gilt weiterhin
(G4) Für alle $x, y \in G$ gilt $x * y = y * x$, so heißt diese Gruppel abelsch.

Ein x' heißt inverses Element zu x.

Beispiele:

- $\mathbb{N}_0$ bildet mit der Addition keine Gruppe $(\mathbb{N}_0, +)$
- $\mathbb{Z}$ bildet mit der Addition eine abelsche Gruppe $(\mathbb{Z}, +)$
- Auch $(\mathbb{Q}, +)$ und $(\mathbb{R}, +)$ sind abelsche Gruppen
- $(\mathbb{Q}, \cdot)$ ist keine Gruppe, aber $(\mathbb{Q}\backslash\{0\}, \cdot)$ schon

Satz (Eindeutigkeit des Inversen): Ist $(G, *)$ eine Gruppe, so hat jedes $x \in G$ genau ein inverses Element.

Beispiele:

- Eine triviale Gruppe besteht nur aus ihrem neutralen Element. Tatsächlich ist $G = \{e\}$ mit $e * e = e$ eine Gruppe.
- Sei X eine Menge. Die Menge $Sym(X) := \{f \in Abb(X, X) \mid f \text{ ist bijektiv}\}$ der Permutationen von X bildet mit der Komposition eine Gruppe $(Sym(X), \circ)$, die symmetrsiche Gruppe auf X. Für $n \in \mathbb{N}$ schreibt man $S_n := Sym(\{1, 2, ..., n\})$. Für $n \geq 3$ ist S_n nicht abelsch.

Bemerkung: Häufig benutzte Notationen für die Gruppenverknüpfung $\cdot$:

- In der multiplikativen Notation schreibt man $\cdot$ statt $*$ (oft auch xy statt $x \cdot y$), bezeichnet das neutrale Element mit 1 oder 1_G und das Inverse zu x mit x^{-1}.
- In der additiven Notation schreibt man $+$ für $*$, bezeichnet das neutrale Element mit 0 oder 0_G und das Inverse zu x mit $-x$. Die additive Notation wird nur verwendet, wenn die Gruppe abelsch ist.

In abelschen Gruppen notiert man Ausdrücke auch mit dem Summen- und Produktzeichen.

Satz: Sei $(G, \cdot)$ eine Gruppe. Für $x, y \in G$ gelten $(x^{-1})^{-1} = x$ und $(xy)^{-1} = x^{-1} \cdot x^{-1}$.

Satz: Sei $(G, \cdot)$ eine Gruppe. Für $a, b \in G$ haben die Gleichungen $ax = b$ und $ya = b$ eindeutige Lösungen in G, nämlich $x = a^{-1} \cdot b$ und $y = b \cdot a^{-1}$. Insbesondere gelten die folgenden Kürzungsregeln: $ax = ay \Rightarrow x = y$ und $xa = ya \Rightarrow x = y$.

Beweis:
Es ist $a \cdot a^{-1} \cdot b = 1b = b$, also ist $x = a^{-1} \cdot b$ eine Lösung. Ist umgekehrt $ax = b$ mit $x \in G$, so ist $a^{-1} \cdot b = a^{-1} \cdot ax = 1x = x$ die Lösung und somit eindeutig. Für die zweite Gleichung argumentiert man analog. Den "Insbesondere"-Fall erhält man durch Einsetzen von $b = ay$ bzw. $b = xa$.

Bemerkung:
Wenn aus dem Kontext klar ist, welche Verknüpfung gemeint ist, schreibt man auch einfach G anstatt $(G, \cdot)$ bzw. $(G, +)$. Eine Gruppe G heißt endlich, wenn die Menge G endlich ist. Die Mächtigkeit $|G|$ von G nennt man dann die Ordnung von G. Eine endliche Gruppe kann durch ihre Verknüpfungstafel vollständig beschrieben werden.

Beispiele:
a) die triviale Gruppe $G = \{e\}$

$\cdot$	e
e	e

b) die Gruppe $\mu_2 = \{1, -1\}$ der Ordnung 2

$\cdot$	1	-1
1	1	-1
-1	-1	1

c) die Gruppe $S_2 = Sym(\{1, 2\}) = \{id_{\{1,2\}}, f\}$, wobei $f(1) = 2$ und $f(2) = 1$

$\circ$	$id_{\{1,2\}}$	f
$id_{\{1,2\}}$	$id_{\{1,2\}}$	f
f	f	$id_{\{1,2\}}$

Definition Untergruppe: Eine Untergruppe einer Gruppe $(G, \cdot)$ ist eine nichtleere Teilmenge $H \subset G$, für die gilt:
(UG1) Für alle $x, y \in H$ ist $x \cdot y \in H$ (Abgeschlossenheit unter Multiplikation).
(UG2) Für alle $x \in H$ ist $x^{-1} \in H$ (Abgeschlossenheit unter Inversen).

Satz: Sei $(G, \cdot)$ eine Gruppe und $\emptyset \neq H \subset G$. Genau dann ist H eine Untergruppe von G, wenn sich die Verknüpfung $\cdot : G \times G \to G$ zu einer Abbildung $\cdot_H : H \times H \to H$ einschränken lässt (d.h. $\cdot|_{H \times H} = \iota_H \circ \cdot_H$, wobei $\iota_H \cdot \cdot_H \to G$ die Inklusionsabbildung ist) und $(H, \cdot_H)$ eine Gruppe ist.

Beweis:
Hinrichtung: Sei H eine Untergruppe von G. Nach (UG1) ist $Image(\cdot|_{H \times H}) \subset H$ und somit lässt sich $\cdot$ zu einer Abbildung $\cdot_H : H \times H$ toH einschränken. Wir betrachten jetzt H mit dieser Verknüpfung. Da G (G1) erfüllt, erfüllt auch H (G1). Da $H \neq \emptyset$ existiert ein $x \in H$. Nach (UG1) und (UG2) ist $x \cdot x^{-1} = e \in H$. Da $e_G \cdot y = y \cdot e_G = y$ für alle $y \in G$, insbesondere auch für alle $y \in H$ (G2). Wegen (UG2) erfüllt H auch das Axiom (G3). H ist somit eine Gruppe.
Rückrichtung: Sei nun umgekehrt $(H, \cdot_H)$ eine Gruppe. Für $x, y \in H$ ist dann $xy = x \cdot_H y \in H$, also erüllt H (UG1). Aus $e_H \cdot e_H = e_H = e_H \cdot e_G$ folgt $e_H = e_G$. Ist also x' das Inverse zu x aus der Gruppe H, so ist $x'x = xx' = e_G = e_H$, also $x^{-1} = x' \in H$ und somit erfüllt H auch (UG2). Wir haben gezeigt, dass H eine Untergruppe von G ist.

Bemerkung:
Wir nennen nicht nur die Menge H eine Untergruppe von G, sondern auch die Gruppe $(H, \cdot_H)$. Wir schreiben $H \leq G$.

Beispiele:
- Jede Gruppe G hat die triviale Untergruppe $H = \{e_G\}$ und $H = G$
- Ist $H \leq G$ und $K \leq H$, so ist $K \leq G$ (Transitivität)
- Unter Addition ist $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R}$ eine Kette von Untergruppen
- Unter Multiplikation ist $\mu_2 \leq \mathbb{Q}^+ \leq \mathbb{R}^+$ eine Kette von Untergruppen
- Für $n \in \mathbb{N}_0$ ist $n\mathbb{Z} := \{nx \mid x \in \mathbb{Z}\} \leq \mathbb{Z}$

Lemma: Ist G eine Gruppe und $(H_i)_{i \in I}$ eine Familie von Untergruppen von G, so ist auch $H := \bigcap H_i$ eine Untergruppe von G.

Beweis: Wir haben 3 Dinge zu zeigen
- *$H \neq \emptyset$: Für jedes $i \in I$ ist $e_G \in H$, also auch $e_G \in \bigcap H_i = H$*
- *(UG1): Seien $x, y \in H$. Für jedes $i \in I$ ist $x, y \in H_i$, somit $xy \in H_i$, da $H_i \leq G$. Folglich ist $xy \in \bigcap H_i = H$.*
- *(UG2): Sei $x \in H$. Für jedes $i \in I$ ist $x \in H_i$, somit $x^{-1} \in H_i$, da $H_i \leq G$. Folglich ist $x^{-1} \in \bigcap H_i = H$.*

Satz: Ist G eine Gruppe und $X \subset G$. so gibt es eine eindeutig bestimmte kleinste Untergruppe H von G, die X enthält, d.h. H enthält X und ist H' eine weitere Untergruppe von G, die X enthält, so ist $H \subset H'$.

Beweis:
Sei $\mathcal{H}$ die Menge aller Untergruppen von G, die X enthalten. Nach dem Lemma ist $H := \bigcap \mathcal{H} := \bigcap H$ eine Untergruppe von G. Da $X \subset H'$ für jedes $H' \in \mathcal{H}$ ist auch $X \subset H$. Nach Definition ist H in jedem $H' \leq G$ mit $X \subset H'$ enhalten.

Definition erzeugte Untergruppe: Ist G eine Gruppe und $X \leq G$, so nennt man diese kleinste Untergruppe von G, die X enthält, die von X erzeugte Untergruppe von G und bezeichnet diese mit $< X >$, falls $X = \{x_1, x_2, ..., x_n\}$ enthält auch mit $< x_1, x_2, ..., x_n >$. Gibt es eine endliche Menge $X \subset G$ mit $G =< X >$, so nennt man G endlich erzeugt.

Beispiele:
- Die leere Menge $X = \emptyset \leq G$ erzeugt stets die trivale Untergruppe $< \emptyset >= \{e\} \leq G$
- Jede endliche Gruppe G ist endlich erzeugt $G =< G >$
- Für $n \in \mathbb{N}_0$ ist $n\mathbb{Z} =< n >\leq \mathbb{Z}$. Ist $H \leq \mathbb{Z}$ mit $n \in H$, so ist auch $kn = nk = n + n + ... + n \in H$ und somit auch $n\mathbb{Z} \leq H$.

1.4 Ringe

Definition Ring: Ein Ring ist ein Tripel $(R, +, \cdot)$ bestehend aus einer Menge R, einer Verknüpfung $+ : R \times R \to R$ (Addition) und einer anderen Verknüpfung $\cdot : R \times R \to R$ (Multiplikation), sodass diese zusammen die folgenden Axiome erfüllen:
(R1) $(R, +)$ ist eine abelsche Gruppe.
(R2) $(R, \cdot)$ ist eine Halbgruppe.
(R3) Für $a, x, y \in R$ gelten die Distributivgesetze $a(x + y) = ax + ay$ und $(x + y)a = xa + ya$.
Ein Ring heißt kommutativ, wenn $xy = yx$ für alle $x, y \in R$.
Ein neutrales Element der Multiplikation heißt Einselement von R.
Ein Unterrrig eines Rings $(R, +, \cdot)$ ist eine Teilmenge, die mit der geeigneten Einschränkung von Addition und Multiplikation wieder ein Ring ist.

Bemerkungen:
Hat ein Ring ein Einselement, so ist dieses eindeutig bestimmt. Notationelle Konfektionen: Das neutrale Element der Addition wird häufig mit 0 bezeichnet; die Multiplikation wird nicht immer notiert; Multiplikation bindet stärker als die Addition.
Wenn die Verknüpfungen aus dem Kontext klar sind, schreibt ma R statt $(R, +, \cdot)$.

Beispiele:
- Der Nullring ist $R = \{0\}$ mit den einzig möglichen Verknüpfungen $+$ und $\cdot$ auf R. Der Nullring ist sogar kommutativ und hat ein Einselement, nämlich die 0.
- $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring mit Einselement 1, ebenso $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$.

- $(2\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring, aber ohne Einselement.

Bemerkungen: Ist R ein Ring, dann gelten die folgenden Aussagen für $x, y \in R$
- $0 \cdot x = x \cdot 0 = 0$
- $x \cdot (-y) = (-x) \cdot y = -xy$
- $(-x) \cdot (-y) = xy$

Bemerkung:
Wir führen eine wichtige Klasse endlicher Ringe ein. Hierfür erinnern wir uns an eine der Grundlagen der Arithmetik in $\mathbb{Z}$.

Theorem: Sei $b \neq 0 \in \mathbb{Z}$. Für jedes $a \in \mathbb{Z}$ gibt es eindeutig bestimmte $q, r \in \mathbb{Z}$ (r ist "Rest"), mit $a = qb + r$ und $0 \leq r < |b|$.

Beweis: Existenz und Eindeutigkeit
Existenz: oBdA nehmen wir an, dass $b > 0$ (denn ist $a = qb + r$, so ist auch $a = (-q)(-b) + r$). Sei $q \in \mathbb{Z}$ die größte Zahl mit $q \leq \frac{a}{b}$, und sei $r = a - qb \in \mathbb{Z}$. Dann ist $a \leq \frac{a}{b} - q < 1$, woraus $0 \leq r < b$ folgt.
Eindeutigkeit: Sei $a = qb + r = q'b + r'$ mit $q, q', r, r' \in \mathbb{Z}$ und $0 \leq r, r' < |b|$. Dann ist $(q - q')b = r - r'$ und $|r - r'| < |b|$. Da $q - q' \in \mathbb{Z}$ ist, folgt $r - r' = 0$ und daraus wegen $b \neq 0$, dann $q - q' = 0$.

Beispiel (Restklassenring): Wir fixieren $n \in \mathbb{N}$. Für $a \in \mathbb{Z}$ sei
$\overline{(a)} := a + n\mathbb{Z} := \{a + nx \mid x \in \mathbb{Z}\}$ die Restklasse von "a mod n". Für $a, a' \in \mathbb{Z}$ sind äquivalent:
- $a + n\mathbb{Z} = a' + n\mathbb{Z}$
- $a' \in a + n\mathbb{Z}$
- n teilt $a' - a$ (in Zeichen $n|a' - a$), d.h. $a' = a + nk$ für $k \in \mathbb{Z}$

Beweis:
1) $\Rightarrow$ 2)*: klar, denn $0 \in \mathbb{Z}$*
2) $\Rightarrow$ 3)*: $a' \in a + n\mathbb{Z} \Rightarrow a' = a + nk$ mit $k \in \mathbb{Z}$*
3) $\Rightarrow$ 1)*: $a' = a + nk$ mit*
$k \in \mathbb{Z} \Rightarrow a + n\mathbb{Z} = \{a + nk + nx \mid x \in \mathbb{Z}\} = \{a + n(k + x) \mid x \in \mathbb{Z}\} = a + n\mathbb{Z}$
Insbesondere besteht $a + n\mathbb{Z}$ nur aus den ganzen Zahlen, die bei der Division durch n den selben Rest lassen wie a.

Aus dem Theorem folgt weiter, dass $\mathbb{Z}/n\mathbb{Z} := \{\overline{a} \mid a \in \mathbb{Z}\} = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$ eine Menge der Mächtigkeit n ist (sprich: "$\mathbb{Z}$ mod $n\mathbb{Z}$").

Wir definieren Verknüpfungen auf $\mathbb{Z}/n\mathbb{Z}$ durch $\overline{a} + \overline{b} := \overline{a + b}$, $\overline{a} \cdot \overline{b} := \overline{ab}$ $a, b \in \mathbb{Z}$. Hierbei muss man zeigen, dass diese Verknüpfungen wohldefiniert sind, also nicht von den gewählten Vertretern a, b der Restklassen $\overline{a}$ und $\overline{b}$ abhängen. Ist etwa $\overline{a} = \overline{a'}$ und $\overline{b} = \overline{b'}$, also $a' = a + nk_1$ und $b' = b + nk_2$ mit $k_1, k_2 \in \mathbb{Z}$, so ist
$a' + b' = a + b + n(k_1 + k_2)$, also $\overline{a' + b'} = \overline{a + b}$
$a' \cdot b' = ab + n(bk_1 + ak_2 + nk_1k_2)$, also $\overline{a'b'} = \overline{ab}$

Man prüft nun leicht nach, dass $\mathbb{Z}/n\mathbb{Z}$ mit diesen Verknüpfungen ein kommutativer Ring mit Einselement ist, da dies auch für $(\mathbb{Z}, +, \cdot)$ gilt. Das neutrale Element der Addition ist $\overline{0}$, das Einselement ist $\overline{1}$.

Beispiel: Im Fall $n = 2$ ergeben sich die folgenden Verknüpfungstafeln für $\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{2} = \overline{0}$

$\cdot$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

Definition Charakteristik: Sei R ein Ring mit Einselement. Man definiert die Charakteristik von R als die kleinste natürliche Zahl n mit $1 + 1 + ... + 1 = 0$, falls so ein n existiert, andernfalls ist die Charakteristik 0.

Definition Nullteiler: Sei R ein Ring mit Einselement. Ein $0 \neq x \in R$ ist ein Nullteiler von R, wenn er ein $0 \neq y \in R$ mit $xy = 0$ oder $yx = 0$ gibt. Ein Ring ohne Nullteiler ist nullteilerfrei.

Definition Einheit: Sei R ein Ring mit Einselement. Ein $x \in R$ heißt invertierbar (oder Einheit von R), wenn es ein $x' \in R$ mit $xx' = x'x = 1$ gibt. Wir bezeichnen die invertierten Elemente von R mit $R^\times$.

Beispiele:

- reelle Zahlen sind ein nullteilerfreier Ring der Charakteristik 0 mit $\mathbb{R}^\times = \mathbb{R}\backslash\{0\}$
- $\mathbb{Z}$ ist ein nullteilerfreier Ring der Charakteristik 0 mit $\mathbb{Z}^\times = \{1, -1\}$
- $\mathbb{Z}/n\mathbb{Z}$ ist ein Ring der Charakteristik n. Ist n keine Primzahl, so ist $\mathbb{Z}$ nicht nullteilerfrei.

Satz: Sei R ein Ring mit Einselement.

- Ist $x \in R$ invertierbar, so ist x kein Nullteiler in R.
- Die invertierbaren Elemente von R bilden mit der Multiplikation eine Gruppe.

Beweis:

- *Ist* $xx' = x'x = 1$ *und* $xy = 0$ *mit* $x', y \in R$, *so ist* $0 = x' \cdot 0 = x \cdot xy = 1 \cdot y = y$, *aber* $y \neq 0$ *für Nullteiler*
- *Sind* $x, y \in R^\times$, *also* $xx' = x'x = yy' = y'y = 1$. *Dann ist* $(xy)(y'x') = x \cdot 1 \cdot x' = 1$ *und* $(y'x')(xy) = y' \cdot 1 \cdot y = 1$, *somit* $R^\times$ *abgeschlossen unter der Multiplikation. Da* $1 \cdot 1 = 1$ *gilt, ist auch* $1 \in R^\times$. *Nach Definition von* $R^\times$ *hat jedes* $x \in R^\times$ *ein Inverses* $x' \in R^\times$.

1.5 Körper

Definition Körper: Ein Körper ist ein kommutativer Ring $(K, +, \cdot)$ mit Einselement $1 \neq 0$, in dem jedes Element $x \neq x \in K$ invertierbar ist.

Bemerkungen: Ein Körper ist stets nullteilerfrei und $(K\backslash\{0\}, \cdot)$ ist eine abelsche Gruppe. Ein körper ist also ein Tripel $(K, +, \cdot)$ bestehend aus einer Menge K und 2 Verknüpfungen $+ : K \times K \to K$ und $\cdot : K \times K \to K$, für die gelten:
(K1): $(K, +)$ ist eine abelsche Gruppe
(K2): $(K\backslash\{0\}, \cdot)$ ist eine abelsche Gruppe, deren neutrales Element wir mit 1 bezeichnen
(K3): Es gelten die Distributivgesetze.

Bemerkungen: Sei K ein Körper und $a, x, y \in K$. Ist $ax = ay$ und $a \neq 0$, so ist $x = y$.

Definition Teilkörper: Ein Teilkörper eines Körpers $(K, +, \cdot)$ ist die Teilemenge $L \subset K$, die mit der geeigneten Einschränkung von Addition und Multiplikation wieder ein Körper ist.

Beispiele:
- Der Nullring ist kein Körper.
- Der Körper $\mathbb{Q}$ der rationalen Zahlen ist ein Teilkörper des Körpers $\mathbb{R}$ der reellen Zahlen.
- $(\mathbb{Z}, +, \cdot)$ ist kein Körper

Beispiel (Komplexe Zahlen)
Wir definieren die Menge $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ und darauf Verknüpfungen wie folgt: Für $(x_1, y_1), (x_2, y_2) \in \mathbb{C}$ ist:
- $(x_1, y_1) + (x_2, y_2) := (x_1 + x_2, y_1 + y_2)$
- $(x_1, y_1) \cdot (x_2, y_2) := (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1)$

Wie man nachprüfen kann, ist $(\mathbb{C}, +, \cdot)$ ein Körper, genannt Körper der komplexen Zahlen. Da $(x_1, 0) + (x_2, 0) = (x_1 + x_2, 0)$ und $(x_1, 0) \cdot (x_2, 0) = (x_1x_2, 0)$, können wir $\mathbb{R}$ durch "$x = (x, 0)$"mit dem Teilkörper $\mathbb{R} \times \{0\}$ von $\mathbb{C}$ identifizieren.
Die imaginäre Einheit $i = (0, 1)$ erfüllt $i^2 = -1$ und jedes $z \in \mathbb{C}$ kann eindeutig geschrieben werden als $z = x + iy$ mit $x, y \in \mathbb{R}$

Lemma: Sei $a \in \mathbb{Z}$ und sei p eine Primzahl, die a nicht teilt. Dann gibt es $b, k \in \mathbb{Z}$ mit $ab + kp = 1$.

Beweis:
Sei $n \in \mathbb{N}$ die kleinste natürliche Zahl der Form $n = ab + kp$. Angenommen, $n \geq 2$. Schreibe $a = qp + r$ mit $q, r \in \mathbb{Z}$ und $0 \leq r < p$. Aus der Nichtteilbarkeit von a folgt $r \neq 0$, also $r \in \mathbb{N}$. Wegen $r = a \cdot 1 - qp$ ist $n \leq r$. Da p Primzahl ist und $2 \leq n \leq r < p$, gilt n teilt nicht p. Schreibe $p = c \cdot n + m$ mit $c, m \in \mathbb{Z}$ und $0 \leq m < n$. Aus n teilt nicht p folgt $m \neq 0$, also $m \in \mathbb{N}$. Da $m = p - cn = -abc + (1 - kc)p$, ist $m < n$ ein Widerspruch zur Minimalität von n. Die Annahme $n \geq 2$ war somit falsch. Es gilt $n = 1$.

Beispiel (Endliche Primkörper)
Für jede Primzahl p ist $\mathbb{Z}/p\mathbb{Z}$ ein Körper. Ist $\overline{a} \neq \overline{0}$, so gilt p teilt nicht a und somit gibt es $b, k \in \mathbb{Z}$ mit
$ab + kp = 1$
$\overline{(ab + kp)} = \overline{1} = \overline{(ab)} = \overline{a} \cdot \overline{b}$
und somit ist $\overline{a}$ invertierbar in $\mathbb{Z}/p\mathbb{Z}$. Somit sind für $n \in \mathbb{N}$ äquivalent:

- $\mathbb{Z}/n\mathbb{Z}$ ist ein Körper
- $\mathbb{Z}/n\mathbb{Z}$ ist nullteilerfrei
- n ist Primzahl

Beweis: 1 → 2: 4.13; 2 → 3: 4.12; 3 → 1: gegeben
Insbesondere ist $\mathbb{Z}/p\mathbb{Z}$ nullteilerfrei, d.h. aus p teilt ab folgt p teilt a oder p teilt b

1.6 Polynome

In diesem Abschnitt sei R ein kommutativer Ring mit Einselement.

Bemerkung: Unter einem Polynom in der "Unbekannte" x versteht man einen Ausdruck der Form $f(x) = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n = \sum_{k=0}^{n} a_k x^k$ mit $a_0, ..., a_n \in R$. Fasst man x als ein beliebiges Element von R auf, gelten einige offensichtliche Rechenregeln:
Ist $f(x) = \sum_{k=0}^{n} a_k x^k$ und $g(x) = \sum_{k=0}^{n} b_k x^k$ so ist

- $f(x) + g(x) = \sum_{k=0}^{n} (a_k + b_k) x^k$
- $f(x) \cdot g(x) = \sum_{k=0}^{2n} c_k x^k$ mit $c_k = \sum_{j=0}^{k} a_j b_{k-j}$

Dies motiviert die folgende präzise Definition für den Ring der Polynome über R in einer "Unbestimmten" x.

Definition Polynom: Sei $R[X]$ die Menge der Folgen in R, die fast überall 0 sind, also $R[X] := \{(a_k)_{k \in \mathbb{N}_0} \mid \forall k (a_k \in R) \wedge \exists n_0 : \forall k > n_0 (a_k = 0)\}$.

Wir definieren Addition und Multiplikation auf $R[X]$:

- $(a_k)_{k \in \mathbb{N}_0} + (b_k)_{k \in \mathbb{N}_0} = (a_k + b_k)_{k \in \mathbb{N}_0}$
- $(a_k)_{k \in \mathbb{N}_0} \cdot (b_k)_{k \in \mathbb{N}_0} = (c_k)_{k \in \mathbb{N}_0}$ mit $c_k = \sum_{j=0}^{k} a_j b_{k-j}$

Mit diesen Verknüpfungen wird $R[X]$ zu einem kommutativen Ring mit Einselement. Diesen Ring nennt man Polynomring (in einer Variablen X) über R. Ein $(a_k)_{k \in \mathbb{N}_0} \in R[X]$ heißt Polynom mit den Koeffizienten $a_0, ..., a_n$. Wenn wir $a \in R$ mit der Folge $(a, 0, 0, ..., 0) := (a, \delta_{k,0})_{k \in \mathbb{N}_0}$ identifizieren, wird R zu einem Unterrring von $R[X]$.

Definiert man X als die Folge $(0, 1, 0, .., 0) := (\delta_{k,1})_{k \in \mathbb{N}_0}$ (die Folge hat an der k-ten Stelle eine 1, sonst nur Nullen). Jedes $f(a_k)_{k \in \mathbb{N}_0}$ mit $a_k = 0$ für $k > n_0$ lässt sich eindeutig schreiben als $f(X) = \sum_{k=0}^{n_0} a_k X^k$.

Alternativ schreiben wir auch $f = \sum_{k\geq 0} a_k X^k$ mit dem Verständnis, dass diese unendliche Summe nur endlich von 0 verschiedene Summanden enthält.

Sei $0 \neq f(X) = \sum_{k\geq 0} a_k X^k \in R[X]$. Der Grad von f ist das größte k mit $a_k \neq 0$, geschrieben $deg(f) := max\{k \in \mathbb{N}_0 \mid a_k \neq 0\}$. Man definiert den Grad des Nullpolynoms als $deg(0) = -\infty$, wobei $-\infty < k \forall k \in \mathbb{N}_0$ gelten soll. Man nennt a_0 den konstanten Term und $a_{deg(f)}$ den Leitkoeffizienten von f. Hat f den Grad 0, 1 oder 2, so nennt man f konstant, linear bzw. quadratisch.

Beispiel: Das lineare Polynom $f(X) = X - 2 \in R[X]$ hat den Leitkoeffizent 1 und den konstanten Term -2.

Satz: Seien $f, g \in R[X]$
- Es ist $deg(f + g) \leq max\{deg(f), deg(g)\}$.
- Es ist $deg(f \cdot g) \leq deg(f) + deg(g)$.
- Ist R nullteilerfrei, so ist $deg(f \cdot g) = deg(f) + deg(g)$ und auch $R[X]$ ist nullteilerfrei.

Beweis:
- *offenbar*
- *Ist* $deg(f) = n$ *und* $deg(g) = m$, $f = \sum_{i\geq 0} f_i X^i$, $g = \sum_{j\geq 0} g_j X^j$, *so ist auch* $h = fg = \sum_{k\geq 0} h_k X^k$ *mit* $h_k = \sum_{i+j=k} f_i \cdot g_j$ *für alle* $k \geq 0$. *Ist* $k > n + m$ *und* $i + j = k$, *so ist* $i > n$ *oder* $j > m$, *somit* $f_i = 0$ *oder* $g_j = 0$ *und somit* $h_k = 0$. *Folglich ist* $deg(h) \leq n + m$.
- *Ist* $f = 0$ *oder* $g = 0$, *so ist die Aussage klar, wir nehmen als* $n, m \geq 0$ *an. Nach b) ist* $deg(h) \leq n + m$ *und* $h_{m+n} = \sum_{i+j=n+m} f_i g_j = f_n g_m$. *Ist* R *nullteilerfrei, so folgt aus* $f_n \neq 0$ *und* $g_m \neq 0$ *schon* $f_n g_m \neq 0$, *und somit* $deg(h) = n + m$.

Theorem (Polynomdivision): Sei K ein Körper und sei $0 \neq g \in K[X]$. Für jedes Polynom $f \in K[X]$ gibt es eindeutig bestimmte $g, h, r \in K[X]$ mit $f = gh + r$ und $deg(r) < deg(g)$.

Beweis: Existenz und Eindeutigkeit
Existenz: Sei $n = deg(f)$, $m = deg(g)$, $f = \sum_{k=0}^{n} a_k X^k$, $g = \sum_{k=0}^{m} b_k X^k$
Induktion nach n *bei festem* g.
IA: Ist $n < m$, *so wählt man* $h = 0$ *und* $r = f$.
IB: Wir nehmen an, dass die Aussage für alle Polynome vom Grad kleiner als n *gilt.*
IS: Ist $n \geq m$, *so betrachtet man* $f_1 = f - \frac{a_n}{b_m} \cdot X^{n-m} \cdot g(X)$. *Da* $\frac{a_n}{b_m} \cdot X^{n-m} \cdot g(X)$ *ein Polynom vom Grad* $n - m + deg(g) = n$ *mit Leitkoeffizient* $\frac{a_n}{b_m} \cdot b_m = a_n$ *ist, ist* $deg(f_1) < n$. *Nach IB gibt es also* $h_1, r_1 \in K[X]$ *mit* $f_1 = gh_1 + r_1$ *und* $deg(r) < deg(g)$. *Somit ist* $f(X) = f_1(X) + \frac{a_n}{b_m} \cdot X^{n-m} \cdot g(X) = gh + r$ *mit* $h(X) = h_1(X) + \frac{a_n}{b_m} \cdot X^{n-m}, r = r_1$.
Eindeutigkeit: Sei $n = deg(f), m = deg(g)$. *Ist* $f = gh + r = gh' + r'$ *und* $deg(r), deg(r') < m$, *so ist* $(h - h')g = r' - r$ *und* $deg(r' - r) < m$. *Da* $deg(h - h') = deg(h' - h) + m$ *muss* $deg(h - h') < 0$, *also* $h' - h = 0$ *sein. Somit* $h' = h$ *und* $r' = r$

Bemerkung: Der Existenzbeweis durch Induktion liefert uns ein konstruktives Verfahren, diese sogenannte Polynomdivision durchzuführen.

Beispiel: in $\mathbb{Q}[X]$: $(x^3 + x^2 + 1) : (x^2 + 1) = x + 1$ Rest $-x$

Definition Nullstelle: Sei $f(X) = \sum_{k\geq 0} a_k X^k \in \mathbb{R}[X]$. Für $\lambda \in \mathbb{R}$ definiert man die Auswertung von f in λ $f(\lambda) = \sum_{k\geq 0} a_k \lambda^k \in \mathbb{R}$. Das Polynom f liefert auf diese Weise eine Abbildung $\tilde{f} : \mathbb{R} \to \mathbb{R}$ und $\lambda \mapsto f(\lambda)$.
Ein $\lambda \in \mathbb{R}$ $f(\lambda) = 0$ ist eine Nullstelle von f.

Lemma: Für $f, g \in \mathbb{R}[X]$ und $\lambda \in \mathbb{R}$i ist $(f + g)(\lambda) = f(\lambda) + g(\lambda)$ und $(fg)(\lambda) = f(\lambda) \cdot g(\lambda)$.

Beweis: Ist $f = \sum_{k\geq 0} a_k X^k$ *und* $g = \sum_{k\geq 0} b_k X^k$, *so ist*
$f(\lambda) + g(\lambda) = \sum_{k\geq 0} a_k \lambda^k + \sum_{k\geq 0} b_k \lambda^k = \sum_{k\geq 0} (a_k + b_k)\lambda^k = (f + g)(\lambda)$
$f(\lambda) \cdot g(\lambda) = \sum_{k\geq 0} a_k \lambda^k \cdot \sum_{k\geq 0} b_k \lambda^k = \sum_{k\geq 0} \sum_{i+j=k} (a_i + b_j)\lambda^k = (fg)(\lambda)$

Satz: Ist K ein Körper und $\lambda \in K$ eine Nullstelle von $f \in K[X]$ so gibt es ein eindeutig bestimmtes $h \in K[X]$ mit $f(X) = (X - \lambda) \cdot h(x)$.

Beweis:
Es gibt $h, r \in K[X]$ *mit* $f(X) = (X - \lambda) \cdot h(x) + r(x)$ *und* $deg(r) < deg(X - \lambda) = 1$, *also* $r \in K$.
Da λ *Nullstelle von* f *ist, gilt* $0 = f(\lambda) = (\lambda - \lambda) \cdot h(\lambda) + r(\lambda) = r(\lambda)$. *Hieraus folgt* $r = 0$.
Eindeutigkeit folgt aus Eindeutigkeit der Polynomdivision.

Korollar: Sei K ein Körper. Ein Polynom $0 \neq f \in K[X]$ hat höchstens $deg(f)$ viele Nullstellen.

Beweis:
Induktion nach $deg(f) = n$
Ist $n = 0$, *so ist* $f \in K^\times$ *und hat somit keine Nullstellen.*
Ist $n > 0$ *und hat* f *eine Nullstelle* $\lambda \in K$, *so ist* $f(X) = (X - \lambda) * h(x)$ *mit* $h(x) \in K[X]$ *und* $deg(f) = deg(X - \lambda) + deg(h) = n - 1$. *Nach IV besitzt* h *höchstens* $deg(h) = n - 1$ *viele Nullstellen. Ist* λ' *eine Nullstelle von* f, *so ist* $0 = f(\lambda') = (\lambda' - \lambda) * h(\lambda')$, *also* $\lambda' = \lambda$ *oder* λ' *ist Nullstelle von* h. *Somit hat* f *höchstens* n *viele Nullstellen in* K.

Korollar: Ist K ein unendlicher Körper, so ist die Abbildung $K[X] \to Abb(K, K)$ und $f \mapsto \tilde{f}$ injektiv.

Beweis:

Sind $f, g \in K[X]$ mit $\tilde{f} = \tilde{g}$, also $f(\lambda) = g(\lambda)$ für jedes $\lambda \in K$, so ist jedes λ Nullstelle von $h := f - g \in K[X]$. Da $|K| = \infty$ ist, so ist $h = 0$, also $f = g$.

Bemerkung: Dieses Korollar besagt uns, dass man über einem unendlichen Körper Polynome als polynomiale Abbildungen auffassen kann. Ist K aber endlich, so ist dies im Allgemeinen nicht richtig. Beispiel: $K = \mathbb{Z}\backslash 2\mathbb{Z}$, $f(X) = X$, $g(X) = X^2 \Rightarrow f \neq g$, aber $\tilde{f} = \tilde{g}$.

Beispiel: Sei $f(X) = X^2 + 1 \in \mathbb{R}[X] \subset \mathbb{C}[X]$
In $K = \mathbb{R}$ hat f keine Nullstelle: Für $\lambda \in \mathbb{R}$ $f(\lambda) = \lambda^2 + 1 \geq 1 > 0$.
In $K = \mathbb{C}$ hat f die beiden Nullstellen $\lambda_1 = i$ und $\lambda_2 = -i$ und zerfällt dort in Linearfaktoren: $f(X) = (X - i)(X + i)$.

Satz: Für einen Körper K sind äquivalent:

- Jedes Polynom $f \in K[X]$ mit $deg(f) > 0$ hat eine Nullstelle in K.
- Jedes Polynom $f \in K[X]$ zerfällt in Linearfaktoren, also $f(X) = a \cdot \prod_{i=1}^{n} (X - \lambda_i)$ mit $n = deg(f), a, \lambda_i \in K$.

Beweis:
$1 \Rightarrow 2$: *Induktion nach $n = deg(f)$*
Ist $n \leq 0$, so ist nichts zu zeigen.
Ist $n > 0$, so hat f eine Nullstelle $\lambda_n \in K$, somit $f(X) = (X - \lambda_n) \cdot g(X)$ mit $g(X) \in K[X]$ und $deg(g) = n - 1$, Nach IV ist $g(X) = a \cdot \prod_{i=1}^{n} (X - \lambda_i)$. Somit ist $f(X) = a \cdot \prod_{i=1}^{n} (X - \lambda_i)$.
$2 \Rightarrow 1$: *Sei $f \in K[X]$ mit $n = deg(f) > 0$. Damit gilt $f(X) = a \cdot \prod_{i=1}^{n} (X - \lambda_i)$. Da $n > 0$, hat f z.B. die Nullstelle λ_1.*

Definition algebraisch abgeschlossen: Ein Körper K heißt algebraisch abgeschlossen, wenn er eine der äquivalenten Bedingungen erfüllt.

Theorem (Fundamentalsatz der Algebra): Der Körper $\mathbb{C}$ ist algebraisch abgeschlossen.

Bemerkung: Wir werden das Theorem zwar benutzen, aber nicht beweisen.

2 Vektorräume

In diesem Kapitel sei K ein Körper.

2.1 Definition und Beispiele

Beispiel: Ist $K = \mathbb{R}$, so haben wir für $K^3 = \mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R} = \{(a, b, c) | a, b, c \in \mathbb{R}\}$ eine geometrische Anschauung, nämlich den euklidischen Raum. Welche algebraische Struktur können wir hierauf sinnvollerweise definieren?

Definition K-Vektorraum: Ein K-Vektorraum (auch Vektorraum über K) ist ein Tripel $(V, +, \cdot)$ bestehend aus einer Menge V, einer Verknüpfung $+ : V \times V \to V$, genannt Addition, und einer Abbildung $\cdot : K \times V \to V$, genannt Skalarmultiplikation, für die gelten:
(V1): $(V, +)$ ist eine abelsche Gruppe
(V2): Addition und Skalarmultiplikation sind verträglich:

- $\lambda(x + y) = (\lambda \cdot x) + (\lambda \cdot y)$
- $(\lambda + \mu) \cdot x = (\lambda \cdot x) + (\mu \cdot x)$
- $\lambda(\mu \cdot x) = (\lambda \cdot \mu) \cdot x$
- $1 \cdot x = x$

Bemerkung: Wir haben sowohl im Körper K als auch im Vektorraum V eine Addition definiert, die wir mit dem selben Symbol + notieren. Ebenso benutzen wir das Symbol $\cdot$ sowohl für die Multiplikation im Körper K als auch für die Skalarmultiplikation. Zur Unterscheidung nennt man die Elemente von V Vektoren und die Elemente von K Skalare. Wir werden bald auch den Nullvektor mit 0 bezeichnen, also mit dem selben Symbol wie das neutrale Element im Körper K. Auch für Vektorräume gibt es notationelle Konvektionen: So bindet die Skalarmultiplikation stärker als die Addition und wird manchmal nicht notiert.

Beispiel: Für $n \in \mathbb{N}$ ist $V = K^n := \prod_{i=1}^{n} K = \{(x_1, x_2, ..., x_n) \mid x_1, x_2, .., x_n \in K\}$ mit komponentenweiser Addition und Skalarmultiplikation $\lambda(x_1, ..., x_n) = (\lambda \cdot x_1, ..., \lambda \cdot x_n)$ ein K-Vektorraum, genannt der (n-dimensionale) Standardraum über K.
Insbesondere (Spezialfall $n = 1$) ist K ein K-Vektorraum.
Für $n = 0$ definiert man K^0 als Nullraum $V = \{0\}$, der einzig möglichen Addition und Skalarmultiplikation einen K-Vektorraum bildet.

Satz: Ist V ein K-Vektorraum, so gelten für $\lambda \in K$ und $x \in V$:

- $0 \cdot x = 0$
- $\lambda \cdot 0 = 0$
- $(-\lambda) \cdot x = \lambda \cdot (-x) = -\lambda \cdot x$. Insbesondere $(-1)x = -x$
- Ist $\lambda \cdot x = 0$, so ist $\lambda = 0$ oder $x = 0$

Beweis:

- *Es ist* $0 \cdot x = (0 + 0) \cdot x = 0 \cdot x + 0 \cdot x$, *woraus* $0 = 0 \cdot x$
- *Es ist* $\lambda \cdot 0 = \lambda(0 + 0) = \lambda \cdot 0 + 0 \cdot \lambda$, *woraus* $0 = \lambda \cdot 0$
- *Es ist* $\lambda \cdot x + (-\lambda \cdot x) = (\lambda + (-\lambda)) \cdot x = 0 \cdot x = 0$, *also* $(-\lambda)x = -(\lambda x)$
- *Ist* $\lambda \cdot x = 0$ *und* $\lambda \neq 0$, *so ist* $0 = \lambda^{-1} \cdot \lambda \cdot x = 1 \cdot x = x$

Beispiele:

- Schränkt man die Multiplikation im Polynomring $K[X] \times K[X] \to K[X]$ zu einer Abbildung $K \times K[X] \to K[X]$ ein, so wird $K[X]$ mit dieser Skalarmultipliaktion zu einem K-VR. Die Skalarmultiplikation ist also gegen $\lambda \cdot \sum_{k \geq 0} a_k \cdot X^k = \sum_{k \geq 0} \lambda \cdot a_k \cdot X^k$ ersetzt wurden.
- Schränkt man die komplexe Multiplikation $\mathbb{C} \times \mathbb{C} \to \mathbb{C}$ zu einer Abbildung $\mathbb{R} \times \mathbb{C} \to \mathbb{C}$ ein, so wird $\mathbb{C}$ mit dieser Skalarmultipliaktion zu einem $\mathbb{R}$-VR. Die Skalarmultipliaktion ist gegeben durch $\lambda(x + iy) = \lambda \cdot x + i \cdot \lambda \cdot y$.

- Verallgemeinerung von 1 und 2: Ist der Körper K ein Unterring eines kommutativen Rings R mit Einselement $1_K \in K$, so wird R durch Einschränkung der Multiplikation $R \times R \to R$ zu einer Abbildung $K \times R \to R$ zu einem K-VR.
- Ist X eine Menge, so wird die Menge der Abbildungen $Abb(X, K)$ durch punktweise Addition $(f + g)(x) = f(x) + g(x)$ und die Skalarmultiplikation $(\lambda \cdot f)(x) = \lambda \cdot f(x)$ zu einem K-VR. Im Spezialfall $X = \{1, 2, ..., n\}$ erhält man den Standardraum K^n.

Definition Untervektorraum: Sei V ein K-VR. Ein Untervektorraum (UVR) von V ist eine nichtleere Teilmenge $W \subset V$ mit:
(UV1): Für $x, y \in W$ ist $x + y \in W$.
(UV2): Für $x \in W$ und $\lambda \in K$ ist $\lambda \cdot x \in W$.

Satz: Sei V ein K-VR und $W \subset V$. Genau dann ist W ein UVR von V, wenn W mit geeigneter Einschränkung der Addition und Skalarmultiplikation wieder ein K-VR ist.

Beweis:
Rückrichtung: Lassen sich $+: V \times V \to V$ *und* $\cdot: K \times V \to V$ *einschränken zur Abbildung* $+_w$*:* $W \times W \to W$, $\cdot_w$*:* $K \times W \to W$ *so gilt für* $x, y \in W$ *und* $\lambda \in K$*:* $x + y = x +_w y \in W$ *und* $\lambda \cdot x = \lambda \cdot_w x \in W$*. Ist* $(W, +_w, \cdot_w)$ *ein* K*-VR, so ist insbesodere* W *nicht leer. Somit ist* W *ein UVR.*
Hinrichtung: Nach (UV1) und (UV2) lassen sich $+$ *und* $\cdot$ *einchränken zu Abbildungen* $+_w$*:* $W \times W \to W$ *und* $\cdot_w$*:* $K \times W \to W$*. Nach (UV1) ist abgeschlossen und unter der Addition und für* $x \in W$ *ist auch* $-x = (-1)x \in W$ *nach (UV2),* W *ist somit Untergruppe von* $(V, +)$*. Insbesondere ist* $(W, +)$ *eine abelsche Gruppe, erfüllt also (V1). Die Verträglichkeit (V2) ist für* $\lambda, \mu \in K$ *und* $x, y \in W$ *gegeben, da sie auch für* $x, y \in V$ *erfüllt ist. Somit ist* $(W, +_w, \cdot_w)$ *ein* K*-VR.*

Beispiele:
- Jder K-VR hat triviale UVR $W = \{0\}$ und $W = V$
- Ist V ein K-VR und $x \in V$, so ist $W = K \cdot x = \{\lambda \cdot x \mid \lambda \in K\}$ ein UVR von V. Insbesondere besitzt z.B. der $\mathbb{R}$-VR $\mathbb{R}^2$ unendlich viele UVR, nämlich alle Ursprungsgeraden. Hieran sehen wir auch, dass die Vereinigung zweier UVR im Allgemeinen kein UVR ist. $\mathbb{R} \cdot (1, 0) \cup \mathbb{R} \cdot (1, 0) \subset \mathbb{R}^2$ verletzt (UV1).
- Der K-VR $K[X]$ hat unter anderem die folgenden UVR:
  - Den Raum K der konstanten Polynome
  - Den Raum $K[X]_{\leq 1} = \{aX + b \mid a, b \in K\}$ der linearen (oder konstanten) Polynome
  - allgemeiner den Raum $K[X]_{\leq n} = \{f \in K[X] \mid deg(f) \leq n\}$ der Polynome von höchstens Grad n
- In der Analysis werden Sie verschiedene UVR des $\mathbb{R}$-VR $Abb(\mathbb{R}, \mathbb{R})$ kennenlernen, etwa den Raum $\mathcal{C}(\mathbb{R}, \mathbb{R})$ der stetigen Funktionen und den Raum $\mathcal{C}^{-1}(\mathbb{R}, \mathbb{R})$ der stetig differenzierbaren Funktionen. Die Menge der Polynomfunktionen $\{\tilde{f} \mid \tilde{f} \in \mathbb{R}[X]\}$ bildet einen UVR des $\mathbb{R}$-VR $\mathcal{C}^{-1}(\mathbb{R}, \mathbb{R})$

Lemma: Ist V ein Vektorraum und $(W_i)_{i \in I}$ eine Familie von UVR von V, so ist auch $W = \bigcap W_i$ ein UVR von V.

Beweis:
Da $0 \in W_i$ *ist auch* $0 \in W$*, insbesondere* $W \neq \emptyset$*.*

- *(UV1): Sind $x, y \in W$, so ist auch $x, y \in W_i$ und deshalb $x + y \in \bigcap W_i = W$.*
- *(UV2): Ist $x \in W$ und $\lambda \in K$, so ist auch $x \in W_i$ und somit $\lambda x \in \bigcap W_i = W$.*

Satz: Ist V ein K-VR und $X \subset V$, so gibt es einen eindeutig bestimmten kleinsten UVR W von V mit $X \subset W$.

Beweis:
Sei $\mathcal{V}$ die Menge aller UVR von X, die X enthalten. Sei $W = \bigcap \mathcal{V}$. Damit ist W ein UVR von V der X enthält.

Definition Erzeugendensystem: Ist V ein K-VR und $X \subset V$, so nennt man den kleinsten UVR von V, der X enthält den von X erzeugten UVR von V und bezeichnet diesen mit $< X >$. Eine Mengen $X \subset V$ mit $< X >= V$ heißt Erzeugendensystem von V. Der VR V heißt endlich erzeugt, wenn er ein endliches Erzeugendensystem besitzt.

2.2 Linearkombination und lineare Abhängigkeit

Sei V ein K-VR.

Definition Linearkombination:
- Sei $n \in \mathbb{N}_0$. Ein $x \in V$ ist eine Linearkombination eines n-Tupels $(x_1, ..., x_n)$ von Elementen von V, wenn es $\lambda_1, ..., \lambda_n \in K$ gibt mit $x = \lambda_1 \cdot x_1, ..., \lambda_n \cdot x_n$. Der Nullvektor ist stets eine Linearkombination von $(x_1, ..., x_n)$ auch wenn $n = 0$.
- Ein $x \in V$ ist eine Linearkombination einer Familie (x_i) von Elementen von V, wenn es $n \in \mathbb{N}_0$ und $i_1, ..., i_n \in I$ gibt, für die x Linearkombination von $(x \cdot i_1, ..., x \cdot i_n)$ ist.
- Die Menge aller $x \in V$, die Linearkombination von $\mathcal{F} = (x_i)$ sind, wird mit $span_K(\mathcal{F})$ bezeichnet.

Bemerkungen:
- Offenbar hängt die Menge der Linearkombinationen von $(x_1, ..., x_n)$ nicht von der Reihenfolge der x_i ab. Wegen (V2)(ii) hängt sie sogar nur von der Menge $\{x_1, ..., x_n\}$ ab.
- Deshalb stimmt 2. für endliche Familien $(x_1, ..., x_n)$ mit 1. überein.
- Auch die Menge der Linearkombinationen einer Familie $\mathcal{F} = (x_1, ..., x_n)$ hängt nur von der Menge $X = \{x_i \mid i \in I\}$ ab. Man sagt deshalb auch, x ist Linearkombination von X und schreibt $span_K(X) = span_K(\mathcal{F})$, also
  $span_K(X) = \{\sum_{i=1}^{n} \lambda_i \cdot n_i \mid n \in \mathbb{N}_0, x_i \in X, \lambda_1, ..., \lambda_n \in K\}$. Nach Definition in $0 \in span_K(X)$ auch für $X = \emptyset$.
- Wie schon bei Polynomen schreibt man hier gerne formal unendliche Summen $x = \sum_{i \in I} \lambda_i \cdot x_i$, bei denen nur endlich viele λ_i von 0 verschieden sind.

Lemma: Für jede Teilmenge $X \subset V$ ist $span_K(X)$ ein UVR von V.

Beweis:
- *Sei $W = span_K(X)$. Nach Definition ist $0 \in W$, insbesondere $W \neq \emptyset$*

- *(UV1): Sind $x, y \in W$, also $x = \lambda_1 \cdot x + ... + \lambda_n \cdot x_n$ und $y = \mu_1 \cdot x + ... + \mu_n \cdot x_n$, so ist $x + y = (\lambda_1 + \mu_1)x_1 + ... + (\lambda_n + \mu_n)x_n \in W$*
- *(UV2): Ist $\lambda \in K$ und $x \in W$, so ist $\lambda x = \lambda \cdot \sum_{i=1}^{n} \lambda_i \cdot x_i = \sum_{i=1}^{n} (\lambda \cdot \lambda_i)x_i \in W$*

Satz: Für jede Teilmenge $X \subset V$ ist $span_K(X) =< X >$.

Beweis:
- *$span_K(X)$ ist UVR von V, der wegen $x = x \cdot 1$ die Menge X enthält, und $< X >$ ist der kleinste solche.*
- *Ist $W \subset V$ ein UVR von V, der X enthält, so enthält er auch wegen (UV2) alle Elemente der Form $\lambda \cdot x$, und wegen (UV1) dann auch alle Linearkombinationen aus X. Insbesondere gilt dies auch für $W =< X >$*

Bemerkung: Wir erhalten $span_K(X) =< X >$ auf 2 verschiedenen Wegen. Erstens "von oben" als Schnitt über alle UVR von V, die X enthalten und zweitens "von unten" als Menge der Linearkombinationen. Man nennt $span_K(X)$ auch den von X aufgespannten UVR oder die lineare Hülle von X.

Beispiele:
- Sei $V = K^n$ der Standardraum. Für $i = 1, ..., n$ sei $e_i = (\delta_{i,1}, ..., \delta_{i,n})$, also $e_1 = (1, 0, ...0)$, $e_2 = (0, 1, 0, ..., 0), ..., e_n = (0, ..., 1)$. Für $x = (x_1, ..., x_n) \in V$ ist $x = \sum_{i=1}^{n} x_i \cdot e_1$, folglich $span_K(e_1, .., e_n) = V$. Insbesondere ist K^n eindeutig erzeugt. Man nennt $(e_1, ..., e_n)$ die Standardbasis des Standardraums K^n.
- Sei $V = K[X]$ Polynomring über K. Da $f = \sum_{i=1}^{n} a_i \cdot X^i$ ist $span_K((X^i)_{i \in I}) = K[X]$. Genauer ist $span_K(1, X, X^2, ..., X^n) = K[X]_{\leq n}$. Tatsächlich ist der K-VR $K[X]$ nicht endlich erzeugt. Sind $f_1, ..., f_r \in K[X]$ und ist $d = max\{deg(f_1), ..., deg(f_r)\}$, so sind $f_1, ..., f_r \in K[X]_{\leq d}$ und somit $span_K(f_1, ..., f_r) \subset K[X]_{\leq d}$, aber es gibt Polynome, deren Grad größer d ist.
- Für $x \in V$ ist $< x >= span_K(x) = K \cdot x$. Im Fall $K = \mathbb{R}$, $V = \mathbb{R}^3$, $x \neq 0$ ist dies eine Ursprungsgerade.
- Im $\mathbb{R}$-VR $\mathbb{C}$ ist $span_{\mathbb{R}}(1) = \mathbb{R} \cdot 1 = \mathbb{R}$, aber im $\mathbb{C}$-VR $\mathbb{C}$ ist $span_{\mathbb{C}}(1) = \mathbb{C} \cdot 1 = \mathbb{C}$

Definition linear (un)abhängig:
- Sei $n \in \mathbb{N}_0$. Ein n-Tupel $(x_1, ..., x_n)$ von Elementen von V ist linear abhängig, wenn es $\lambda_1, ..., \lambda_n \in K$ gibt, die nicht alle 0 sind und $\lambda_1 \cdot x_1 + ... + \lambda_n \cdot x_n = 0$ (*) erfüllen. Andernfalls heißt das Tupel linear unabhängig.
- Eine Familie (x_i) von Elementen von V ist linear abhängig, wenn es $n \in \mathbb{N}_0$ und paarweise verschiedene $i_1, ..., i_n \in I$ gibt, für die $(x_{i_1}, ..., x_{i_n})$ linear abhängig ist. Andernfalls linear unabhängig.

Bemerkungen:
- Offenbar hängt die Bedingung (*) nicht von der Reihenfolge der $x_1, ..., x_n$ ab und ist $(x_1, ..., x_k)$ linear abhängig für ein $k \leq n$, so ist auch $(x_1, ..., x_n)$ linear abhängig. Deshalb stimmt die 2. Definition für endliche Familien mit der 1. überein und (x_i) ist genau dann linear abhängig, wenn es eine endliche Teilmenge $J \subset I$ gibt, für die (x_j) linear abhängig ist.

- Eine Familie ist genau dann linear unabhängig, wenn für jede endliche Teilmenge $J \subset I$ und für jede Wahl an Skalaren $(\lambda_i)_{i \in J}$ aus $\sum \lambda_i \cdot x_i = 0$ schon $\lambda_i = 0$ folgt, also wenn sich der Nullvektor nur trivial linear kombinieren lässt.

Satz: Genau dann ist (x_i) linear abhängig, wenn es $i_0 \in I$ gibt mit $x_{i_0} \in span_K((x_i)_{i \in I \setminus \{i_0\}})$. In diesem Fall ist $span_K((x_i)_{i \in I}) = span_K((x_i)_{i \in I \setminus \{i_0\}})$.

Beweis: Es reicht, die Aussage für $I = \{1, ..., n\}$ zu beweisen.
Hinrichtung: Ist $(x_1, ..., x_n)$ linear anhängig, so existieren $\lambda_1, ..., \lambda_n$ mit $\sum_{i=1}^{n} \lambda_i \cdot x_i = 0$. oBdA sei $\lambda_n \neq 0$. Dann ist $x_n = \lambda_n^{-1} \cdot \sum_{i=1}^{n-1} \lambda_i \cdot x_i = \sum_{i=1}^{n-1} \lambda_n^{-1} \cdot \lambda_i \cdot x_i \in span_K(x_1, ..., x_n)$.
Rückrichtung: oBdA. $i_0 = n$, also $\sum_{i=0}^{n-1} \lambda_i \cdot x_i$. Mit $\lambda_n = -1$ ist $\sum_{i=1}^{n} \lambda_i \cdot x_i = 0$, was zeigt, dass $(x_1, ..., x_n)$ linear abhängig ist.
Sei nun $x_n = \sum_{i=1}^{n-1} \lambda_i \cdot x_i \in span_K(x_1, ..., x_{n-1})$. Wir zeigen, dass $span_K(x_1, ..., x_{n-1}) = span_K(x_1, ..., x_n)$

- *klar, da bei mehr Elementen die Anzahl der Linearkombinationen nicht abnimmt*
- *Ist $y = \sum_{i=1}^{n} \mu_i \cdot x_i \in span_K(x_1, ..., x_n)$, so ist $y = \sum_{i=1}^{n-1} \mu_i + \mu_n \cdot \lambda_i \cdot x_i \in span_K(x_1, ..., x_n)$*

Satz: Genau dann ist (x_i) linear unabhängig, wenn sich jedes $x \in span_K((x_i))$ in eindeutiger Weise als Linearkombination der (x_i) schreiben lässt, d.h. $x = \sum_{i \in I} \lambda_i \cdot x_i = \sum_{i \in I} \lambda_i' \cdot x_i$, so ist $\lambda_i = \lambda_i'$

Beweis: Es reicht, die Aussage für $I = \{1, ..., n\}$ zu beweisen.
Hinrichtung: Ist $(x_,..., x_n)$ linear unabhängig und $x = \sum_{i \in I} \lambda_i \cdot x_i = \sum_{i \in I} \lambda_i' \cdot x_i$, so folgt daraus $\sum_{i \in I} (\lambda_i - \lambda_i') x_i = 0$ wegen der linearen Unabhängigkeit der x_i, dass $\lambda_i = \lambda_i' = 0$
Rückrichtung: Lässt sich jedes $x \in span_K(x_1, ..., x_n)$ in eindeutiger Weise als Linearkombination der x_i schreiben, so gilt dies insbesondere für $x = 0$. Ist also $\sum_{i=1}^{n} \lambda_i \cdot x_i = 0$, so folgt schon $\sum_{i=1}^{n} 0 \cdot x_i = 0$ schon $\lambda_i = 0$

Beispiele:

- Die Standardbasis $(e_1, ..., e_n)$ des K^n ist linear unabhängig. Es ist $\sum_{i=1}^{n} \lambda_i \cdot e_i = (\lambda_1, ..., \lambda_n)$
- Im K-VR $K[X]$ sind die Monome (X^i) linear unabhängig.
- Ein einzelner Vektor $x \in V$ ist genau dann linear abhängig, wenn $x = 0$.
- Ein Paar (x_1, x_2) von Elementen von V ist linear abhängig, wenn es ein skalares Vielfaches des anderen ist, also z.B. $x_1 = \lambda \cdot x_2$.
- Im $\mathbb{R}$-VR $\mathbb{R}^2$ sind die beiden Vektoren $(1, 2)$ und $(2, 1)$ linear unabhängig.
  Im $\mathbb{Z}\backslash 3\mathbb{Z}$-VR $(\mathbb{Z}\backslash 3\mathbb{Z})^2$ sind diese Vektoren linear unabhängig, da $x_1 + x_2 = (1, 2) + (2, 1) = (3, 3) = (0, 0) = 0$.
- Im $\mathbb{R}$-VR $\mathbb{C}$ ist $(1, i)$ linear unabhängig, aber im $\mathbb{C}$-VR $\mathbb{C}$ ist $(1, i)$ linear abhängig, denn $\lambda_1 \cdot 1 + \lambda_2 \cdot i = 0$ für $\lambda_1 = 1$ und $\lambda_2 = i$.

Bemerkungen:

- Ist $x_{i_0} = 0$, ist (x_i) linear abhängig: $1 \cdot x_{i_0} = 0$
- Gibt es $i, j \in I$ mit $i \neq j$, aber $x_i = x_j$, so ist (x_i) linear abhängig: $x_i - x_j = 0$
- Dennoch sagt man auch "die Teilmenge $X \subset V$ ist linear abhängig" und meint damit, dass die Familie $(x_x)_{x \in X}$ linear abhängig ist, d.h. es gibt ein $n \in \mathbb{N}_0$, $x_1, ..., x_n \in X$ paarweise verschieden, mit $\sum_{i=1}^{n} \lambda_i \cdot x_i = 0$.

2.3 Basis und Dimension

Definition Basis: Eine Familie (x_i) von Elementen von V ist eine Basis von V, wenn gilt:
(B1): Die Familie ist linear unabhängig.
(B2): Die Familie erzeugt V, also $span_K(x_i) = V$.

Bemerkung: Kurz gesagt ist eine Basis ein linear unabhängiges Erzeugendensystem.

Satz: Sei (x_i) eine Familie von Elementen von V. Genau dann ist (x_i) eine Basis von V, wenn sich jedes $x \in V$ auf eindeutige Weise als Linearkombination der (x_i) schreiben lässt.

Beispiele:

- Die leere Familie ist eine Basis des Nullraums.
- Die Standardbasis $(e_1, ..., e_n)$ ist eine Basis des Standardraums.
- Die Monome (X^i) bilden eine Basis des K-VR $K[X]$.
- Die Basis des $\mathbb{R}$-VR $\mathbb{C}$ ist gegeben durch $(1, i)$, eine Basis des $\mathbb{C}$- VR $\mathbb{C}$ ist gegeben durch (1)
- Der $\mathbb{C}$-VR $\mathbb{C}$ hat viele weitere Basen.

Satz: Für eine Familie (x_i) von Elementen von V sind äquivalent:

- B ist eine Basis von V.
- B ist ein minimales Erzeugendensystem.
- B ist maximal linear unabhängig, d.h. B ist linear unabhängig, aber wenn Elemente zur Basis hinzugefügt werden, ist diese nicht mehr linear unabhängig.

Beweis:
$1 \Rightarrow 2$*: Sei B eine Basis von V und J eine echte Teilmenge von I. Nach Definition ist B ein Erzeugendensystem. Wähle $i_0 \in I \backslash J$. Da (x_i) linear unabhängig ist, ist x_{i_0} keine Element $span_K((x_i)_{i \in I \backslash \{i_0\}}) \geq span_K((x_i)_{i \in J})$. Insbesondere ist $(x_i)_{i \in J}$ kein Erzeugendensystem von V.*
$2 \Rightarrow 3$*: Sei B ein minimales Erzeugendensystem und $(x_i)_{i \in J}$ eine Familie mit J echter Obermenge von I. Wäre (x_i) linear abhängig, so gäbe es ein i_0 mit $span_K((x_i)_{i \in I \backslash \{i_0\}}) = span_K((x_i)_{i \in I}) = V$ im Widerspruch zur Minimalität von B. Also ist $B = (x_i)$ linear unabhängig. Wähle $j_0 \in J \backslash I$. Dann ist $x_{j_0} \in V = span_K(x_i) \leq span_K((x_i)_{i \in J \backslash \{j_0\}})$ und somit ist $(x_i)_{i \in J}$ linear abhängig.*
$3 \Rightarrow 1$*: Sei B nun maximal linear unabhängig. Angenommen B wäre kein Erzeugendensystem. Dann gibt es ein $x \in V \backslash span_K(x_i)$. Definiere $J = I \cup \{j_0\}$ mit $j_0 \notin I$ und $x_{j_0} := x$. Aufgrund der Maximalität von B ist (x_i) linear abhängig, es gibt als Skalare λ, (λ_i), nicht alle gleich 0, mit $\lambda \cdot x + \sum_{i \in I} \lambda_i \cdot x_i = 0$. Da (x_i) linear abhängig ist, muss $\lambda \neq 0$ sein, woraus der Widerspruch $x = \lambda^{-1} \cdot \sum_{i \in I} \lambda_i \cdot x_i \in span_K(x_i)$. Somit ist B ein Erzeugendensystem.*

Theorem (Basisauswahlsatz): Jedes endliche Erzeugendensystem von V besitzt eine Basis als Teilfamilie: Ist (x_i) ein endliches Erzeugendensystem von V, so gibt es eine Teilmenge $J \subset I$, für die $(x_i)_{i\in J}$ eine Basis von V ist.

Beweis:
Sei (x_i) ein endliches Erzeugendensystem von V. Definiere
$\mathcal{J} := \{J \subset I \mid (x_i)_{i\in J}$ J ist Erzeugendensystem von $V\}$. Da I endlich ist, ist auch $\mathcal{J}$ endlich. Da (x_i) Erzeugendensystem ist, ist $I \in J$, insbesondere $\mathcal{J} \neq \emptyset$. Es gibt deshalb ein bezüglich Inklusion minimales $J_0 \in \mathcal{J}$, d.h. $J_1 \in \mathcal{J}$ so gilt nicht $J_1 \subsetneq J_0$. Deshalb ist $(x_i)_{i\in J_0}$ eine Basis von V.

Korollar: Jeder endlich erzeugte K-VR besitzt eine endliche Basis.

Bemerkungen:

- Der Beweis des Theorems liefert ein konstruktives Verfahren: Ist $(x_1, ..., x_n)$ ein endliches Erzeugendensystem von V, so prüfe man, ob es ein i_0 mit $x_{i_0} \in span_K((x_i)_{i\neq i_0})$ gibt. Falls Nein, ist $(x_1, ..., x_n)$ eine Basis von V. Falls Ja, macht man mit $(x_1, ..., x_{i_{0-1}}, x_{i_{0+1}}, ..., x_n)$ weiter.
- Man kann jedoch zeigen, dass jeder Vektorraum eine Basis besitzt. Die Gültigkeit der Aussage hängt jedoch von bestimmten mengentheoretischen Axoimen ab, auf die wir an dieser Stelle nicht eingegehen werden. Siehe dazu LAAG 2. Semester.

(Austausch-)Lemma: Sei $B = (x_1, ..., x_n)$ eine Basis von V. Sind $\lambda_1, ..., \lambda_n \in K$ und $y = \sum_{i=1}^{n} \lambda_i \cdot x_i$, so ist für jedes $j \in \{1, 2, ..., n\}$ mit $\lambda_j \neq 0$ auch $B' = (x_1, ..., x_{j-1}, y, x_{j+1}, ..., x_n)$ eine Basis von V.

Beweis:
o.B.d.A. sei $j = 1$, also $B' = (y, x_2, ..., x_n)$. Wegen $\lambda_1 \neq 0$ ist
$x_1 = \lambda_1^{-1} \cdot y - \sum_{i=2}^{n} \lambda_i \cdot x_i \in span_K(y, x_2, ..., x_n)$ und somit ist B' ein Erzeugendensystem. Sind
$\mu_1, ..., \mu_n \in K$ mit $\mu_1 \cdot y - \sum_{i=2}^{n} \mu_i \cdot x_i = 0$, so folgt
$0 = \mu_1(\sum_{i=1}^{n} \lambda_i \cdot x_i + \sum_{i=2}^{n} \mu_i \cdot x_i) = \mu_1 \cdot \lambda_1 \cdot x_1 + \sum_{i=2}^{n}(\mu_1 \cdot \lambda_i + \mu_i)x_i$ und aus der linearen
Unabhängigkeit von B somit $\mu_1 \cdot \lambda_1 = 0$, $\mu_1 \cdot \lambda_2 + \mu_2 = 0$, ..., $\mu_1 \cdot \lambda_n + \mu_n = 0$. Wegen $\lambda_1 \neq 0$ folgt $\mu_1 = 0$ und daraus $\mu_i = 0$. Folglich ist B' linear unabhängig.

Theorem (Steinitz'scher Austauschsatz): Sei $B = (x_1, ..., x_n)$ eine Basis von V und $\mathcal{F} = (y_1, ..., y_r)$ eine linear unabhängige Familie in V. Dann ist $r \leq n$ und es gibt $i_1, ..., i_{n-r} \in \{1, ..., n\}$, für die $B' = (y_1, ..., y_r, x_{i_1}, ..., x_{i_{n-r}})$ eine Basis von V ist.

Beweis: Induktion nach r
Für $r = 0$ ist nichts zu zeigen.
Sei nun $r \geq 1$ und gelte die Aussage für $(y_1, ..., y_{r-1})$. Insbesondere ist $r - 1 \leq n$ und es gibt $i_1, .., i_{n-(r-1)} \in \{1, ..., n\}$ für die $B' = (y_1, ..., y_r, x_{i_1}, ..., x_{i_{n-(r-1)}})$ eine Basis von V ist. Da

$y_r \in V = span_K(B')$ *ist* $y_r = \sum_{i=1}^{r-1} \lambda_i \cdot y_1 + \sum_{j=0}^{n-(r-1)} \mu_j \cdot x_{i_j}$. *Da* $(y_1, ..., y_r)$ *linear unabhängig, ist* $y_r \notin span_K(y_1, ..., y_{r-1})$. *Folglich gibt es* $j_0 \in \{1, ..., n-(r-1)\}$ *mit* $\mu_{j_0} \neq 0$. *Insbesondere ist* $n-(r-1) \geq 1$, *also* $r \leq n$. *o.B.d.A.* $j_0 = 1$, *dann ergibt sich mit dem Austasuchlemma, dass auch* $(y_1, ..., y_{r-1}, y_r, x_{i_2}, ..., x_{i_{n-(r-1)}})$ *eine Basis von* V *ist.*

Korollar: Ist V endlich erzeugt, so lässt sich jede linear unabhängige Familie zu einer Basis ergänzen: Ist $(x_1, ..., x_n)$ linear unabhängig, so gibt es $m \geq n$ und $x_{n+1}, x_{n+2}, ..., x_m$ für die $(x_1, ..., x_n, x_{n+1}, ..., x_m)$ eine Basis von V ist.

Beweis:
Nach dem Basisauswahlsatz besitzt V *eine endliche Basis, die Behauptung folgt somit aus dem Steinitz'schen Austauschsatz.*

Korollar: Sind (x_i) und (x_j) Basen von V und ist I endlich, so ist $|I| = |J|$.

Beweis:
Da (y_r) *linear unabhängig ist, ist* $|J| \leq |I|$ *nach dem Steinitz'schen Austauschsatz. Insbesondere ist* J *endlich, also* $|I| \leq |J|$ *nach dem Austauschsatz.*

Korollar: Ist V endlich erzeugt, so haben alle Basen von V die gleiche Mächtigkeit.

Beweis:
Besitzt V *eine endliche Basis, so folgt deshalb die Behauptung aus dem vorherigen Korollar.*

Definition Dimension: Ist V endlich erzeugt, so ist die Dimension des VR V die Mächtigkeit $dim_K(V)$ einer Basis von V. Anderfalls sagt man, dass V unendliche Dimensionen hat und schreibt $dim_K(V) = \infty$.

Beispiele:
- $dim_K(K^n) = n$
- $dim_K(K[X]) = \infty$
- $dim_K(K[X]_{\leq n}) = n + 1$
- $dim_{\mathbb{R}}(\mathbb{C}) = 2$
- $dim_{\mathbb{C}}(\mathbb{C}) = 1$

Bemerkungen:
- V ist genau dann endlich erzeugt, wenn $dim_K(V) < \infty$.
- $dim_K(V) = min\{|B| \mid span_K(B) = V\} = max\{|B| \mid \text{B linear unabhängig}\}$

Satz: Sei V endlich erzeugt und $W \leq V$ ein UVR.
- Es ist $dim_K(W) \leq dim_K(V)$. Insbesondere ist W endlich erzeugt.
- Ist $dim_K(W) = dim_K(V)$, so ist auch $W = V$.

Beweis:

- *Ist F eine linear unabhängige Familie in W, so ist auch F linear unabhängig in V und somit $|F| \leq dim_K(V)$. Insbesondere gibt es eine maximal linear unabhängige Familie B in W und es folgt $dim_K(W) = |B| \leq dim_K(V)$.*
- *Sei B eine Basis von W. Dann ist B auch in V linear unabhängig. Ist $dim_K(W) = dim_K(V)$, so muss auch B in V maximal linear unabhängig sein. Insbesondere ist $W = span_K(B) = V$.*

2.4 Summen von Vektorräumen

Sei V ein K-VR und (W_i) eine Familie von UVR von V.

Definition Summe von VR: Die Summe der W_i ist der UVR $\sum_{i \in I} W_i := span_K(\bigcup W_i)$. Im Fall $I = \{1, ..., n\}$ schreibt man auch $W_1 + ... + W_n$ für $\sum_{i=1}^{n} W_i$.

Lemma: Es ist $\sum_{i \in I} W_i = \{\sum_{i \in I} x_i \mid x_i \in W_i$, fast alle gleich $0\}$.

Beweis:
" $\geq$ ": *klar,* $\sum x_i \in span_K(\bigcup W_i)$
" $\leq$ ": *Die rechte Seite enthält jedes W_i und ist ein UVR von V:*
Für $x_i, x_i' \in W$, fast alle gleich 0 und $\lambda \in K$ ist $\sum x_i + \sum x_i' = \sum(x_i + x_i')$, $\lambda \cdot \sum x_i = \sum \lambda \cdot x_i \rightarrow$ UVR

Definition direkte Summe: Ist jedes $x \in \sum W_i$ eindeutig als Summe von x_i mit $x_i \in W_i$ darstellbar, so sagt man, dass $\sum W_i$ die direkte Summe der UVR W_i ist und schreibt $\oplus W_i$ für $\sum W_i$. Im Fall $I = \{1, ..., n\}$ schreibt man auch $W_1 \oplus W_2 \oplus ... \oplus W_n$ für $\oplus W_i$.

Beispiel: Ist $(x_1, ..., x_n)$ eine Basis von V, so ist $V = Kx_1 \oplus ... \oplus Kx_n$.

Bemerkung: Wir wollen uns näher mit dem wichtigen Spezialfall $I = \{1, 2\}$ beschäftigen und schreiben noch mal auf:
- $V = W_1 \oplus W_2$
- $V = W_1 + W_2$ und $W_1 \cap W_2 = \{0\}$

Satz: Sind W_1, W_2 UVR von V mit Basen $(x_i)_{i \in I_1}$ bzw. $(x_i)_{i \in I_2}$, wobei $I_1 \cap I_2 = \emptyset$, so sind äquivalent:
- $V = W_1 \oplus W_2$
- $(x_i)_{i \in I_1 \cap I_2}$ ist eine Basis von V

Beweis: Sei $I = I_1 \cup I_2$
$1 \Rightarrow 2$*: Da $span_K((x_i)_{i \in I_1}) = W_1$ und $span_K((x_i)_{i \in I_2}) = W_2$ ist $span_K((x_i)_{i \in I}) = W_1 + W_2 = V$. Ist $\sum \lambda_i x_i = 0$, so ist $\sum_{i \in I_1} \lambda_i x_i = -\sum_{i \in I_2} \lambda_i x_i \in W_1 \cap W_2 = \{0\}$. Da $(x_i)_{i \in I_1}$ linear unabhängig ist, ist $\lambda_i = 0$, analog für $i \in I_2$.*

$2 \Rightarrow 1$: *$W_1 + W_2 = span_K((x_i)_{i\in I_1}) + span_K((x_i)_{i\in I_2}) = span_K((x_i)_{i\in I}) = V$. Ist $x \in W_1 \cap W_2$, so ist $x = \sum_{i\in I_1} \lambda_i x_i = \sum_{i\in I_2} \lambda_i x_i$. Somit $0 = \sum_{i\in I_1} \lambda_i x_i - \sum_{i\in I_2} \lambda_i x_i$, woraus wegen $(x_i)_{i\in I}$ linear unabhängig schon $\lambda_i = 0$ folgt. Somit ist $x = 0$.*

Korllar: Ist $dim_K(V) < \infty$, so ist jeder UVR ein direkter Summand: Ist W ein UVR von V, so gibt es einen UVR W' von V mit $V = W \oplus W'$ (W' heißt das **lineare Komplement** von W in V). Es ist $dim_K(W') = dim_K(V) - dim_K(W)$.

Beweis:
Sei $(x_1, ..., x_m)$ eine Basis von W. Nach dem Basisergänzungssatz lässt sich diese zu einer Basis $(x_1, ..., x_n)$ von V ergänzen. Mit $W' := span_K(x_{m+1}, ..., x_n)$ ist dann $V = W \oplus W'$.

Bemerkung: Ist $dim_K(V) < \infty$, so folgt aus $W_1 \cap W_2 = \{0\}$ also insbesondere $dim_K(W_1 + W_2) = dim_K(W_1) + dim_K(W_2)$.

Theorem (Dimensionsformel): Sei $dim_K(V) < \infty$. Für UVR W_1, W_2 von V gilt: $dim_K(W_1 + W_2) + dim_K(W_1 \cap W_2) = dim_K(W_1) + dim_K(W_2)$.

Beweis:
Da $dim_K(V) < \infty$ haben alle UVR von V Basen. Sei also $B_0 = (X_1, ..., x_n)$ eine Basis von $W_1 \cap W_2$. Nach dem Basisergänzungssatz können wir B_0 zu den Basen $B_1 = (x_1, ..., x_n, y_1, ..., y_p)$ von W_1 und $B_2 = (x_1, ..., x_n, z_1, ..., z_q)$ von W_2 ergänzen. Wir behaupten, dass $B = (x_1, ..., x_n, y_1, ..., y_p, z_1, ..., z_q)$ eine Basis von $W_1 + W_2$ ist. Offenbar ist B ein Erzeugendensystem von $W_1 + W_2$. Seien nun $\lambda_1, ..., \lambda_n, \mu_1, ..., \mu_p, \eta_1, ..., \eta_q \in K$ mit $\sum_{i=1}^{n} \lambda_i x_i + \sum_{j=1}^{p} \mu_j y_j + \sum_{k=1}^{q} \eta_k z_k = 0$. Dann ist $\sum_{i=1}^{n} \lambda_i x_i + \sum_{j=1}^{p} \mu_j y_j = -\sum_{k=1}^{q} \eta_k z_k \in W_1 \cap W_2$. Da $span_K(B_0) = W_1 \cap W_2$ und B_1 linear unabhängig ist, ist $\mu_j = 0$. Analog zeigt man auch, dass $\eta_k = 0$. Aus B_0 linear unabhängig folgt dann auch, dass $\lambda_i = 0$. Somit ist B linear unabhängig. Wir haben gezeigt, dass B eine Basis von $W_1 + W_2$ ist.
$\Rightarrow dim_K(W_1) + dim_K(W_2) = |B_1| + |B_2| = (n + p) + (n - q) = (n + p + q) + n = |B| + |B_0| = dim_K(W_1 + W_2) + dim_K(W_1 \cap W_2)$.

Definition (externes) Produkt: Das (externe) Produkt einer Familie (V_i) von K-VR ist der K-VR $\prod V_i$ bestehend aus dem kartesischen Produkt der V_i mit komponentenweiser Addition und Skalarmultiplikation, $(x_i) + (x_i') := (x_i + x_i')$ und $\lambda(x_i) := (\lambda x_i)$.

Definition (externe) Summe: Die (externe) Summe einer Familie (V_i) von K-VR ist der UVR $\oplus V_i := \{(x_i) \in \prod V_i \mid x_i = 0$; für fast alle $i\}$ des K-VR $\prod V_i$.

Bemerkung: Man prüft sofort nach, dass $\prod V_i$ ein K-VR ist und $\oplus V_i$ ein UVR davon ist. Für endliche Indexmengen ist $\prod V_i = \oplus V_i$, z.B. $K^n = \prod_{i=1}^{n} K = \oplus K$.

Lemma: Sei (V_i) eine Familie von K-VR und sei $V = \oplus V_i$. Für jedes $j \in I$ ist $\tilde{V}_j := V \times \prod_{i \in I \setminus \{j\}} \{0\}$ ein UVR von V und $V = \oplus \tilde{V}_j$

Beweis:
Ist $x = (x_i) \in V$ mit $x_i \in V_i$, fast alle $x_i = 0$, so ist $x = \sum \tilde{x}_i$ mit $\tilde{x} := (x_i \delta_{ij}) \in \tilde{V}_j$. Somit ist $V = \sum \tilde{V}_i$. Die Gleichung $\tilde{V}_i \cap \sum_{j \neq i} \tilde{V}_j = \{0\}$ folgt aus Definition der $\tilde{V}_i$.

3 Lineare Abbildungen

Sei K ein Körper.

3.1 Matrizen

Definition Matrix: Seien $m, n \in \mathbb{N}_0$. Eine $m \times n$-Matrix über K ist ein rechteckiges Schema:

$$\begin{pmatrix} a_{11} & ... & a_{1n} \\ ... & & ... \\ a_{m1} & ... & a_{mn} \end{pmatrix}$$

Man schreibt dies auch als $A = (a_{ij})_{i=1,...,n\ j=1,...,m}$ oder $A = (a_{ij})_{i,j}$, wenn m und n aus dem Kontext hervorgehen. Die a_{ij} heißen die Koeffizienten der Matrix A und wir definieren $A_{i,j} = a_{ij}$. Die Menge der $m \times n$-Matrizen über K wird mit $Mat_{m \times n}(K)$ oder $K^{m \times n}$ bezeichnet. Man nennt das Paar (m, n) auch den Typ von A. Ist $m = n$, so spricht man von quadratischen Matrizen und schreibt $Mat_n(K)$. Zu einer Matrix $A = (a_{ij}) \in Mat_{m \times n}(K)$ definiert man die zu A transponierte Matrix $A^t := (a_{ij})_{j,i} \in Mat_{n \times m}(K)$.

Beispiele:
- Die Nullmatrix ist $0 = (0)_{i,j} \in Mat_{m \times n}(K)$.
- Für $k, l \in \{1, ..., n\}$ ist die (k, l)-Basismatrix gegeben durch $E_{kl} = (\delta_{jk} \delta_{jl}) \in Mat_{m \times n}(K)$.
- Die Einheitsmatrix ist $1_n = (\delta_{ii}) \in Mat_n(K)$.
- Für $a_i, ..., a_n \in K$ definiert man eine Diagonalmatrix $diag(a_1, ..., a_n) = (\delta_{ij} \cdot a_i)$.
- Für eine Permutation $\sigma \in S_n$ definiert man die Permutationsmatrix $P_\sigma := (\delta_{\sigma(i),j})$.
- Für $a_1, ..., a_n$ definiert man einen Zeilenvektor $(a_1, ..., a_n) \in Mat_{1 \times n}(K)$ bzw. einen Spaltenvektor $(a_1, ..., a_n)^t$.

Definition Addition und Skalarmultiplikation: Seien $A = (a_{ij})$ und $B = (b_{ij})$ desselben Typs und $\lambda \in K$. Man definiert auf $Mat_{m \times n}(K)$ eine koeffizientenweise Addition und Skalarmultiplikation.

Satz: $(Mat_{m \times n}, +, \cdot)$ ist ein K-VR der Dimension $dim_K(Mat_{m \times n}) = n \cdot m$ mit Basismatrix als Basis.

Beweis:

Dies ist klar, weil wir $Mat_{m\times n}$ mit dem Standardraum K^{mn} identifizieren können. Wir haben die Elemente nur als $m \times n$-Matrix statt als mn-Tupel geschrieben.

Definition Matrizenmultiplikation: Seien $m, n, r \in \mathbb{N}_0$. Sind $A = (a_{ij}) \in Mat_{m\times n}(K)$, $B = (b_{jk}) \in Mat_{n\times r}(K)$ so definieren wir $C = AB$ als die Matrix $C = (c_{ik}) \in Mat_{m\times r}(K)$ mit $c_{ik} = \sum_{j=1}^{n} a_{ij} \cdot b_{jk}$. Kurz geschrieben "Zeile · Spalte".

Beispiele:

- Für $A \in Mat_n(K)$ ist $0 \cdot A = 0$ und $1 \cdot A = A$.
- Für $\sigma \in S_n$ und $A \in Mat_{n\times r}(K)$ geht $P_\sigma \cdot A$ aus A durch Permutation der Zeilen hervor.

Lemma: Für $m, n, r \in \mathbb{N}_0$ und $A = (a_{ij}) \in Mat_{m\times n}(K)$, $B = (b_{jk}) \in Mat_{n\times r}(K)$ und $\lambda \in K$ gilt: $A(\lambda B) = (\lambda A)B = \lambda(AB)$.

Beweis:
Schreibe $A = (a_{ij})$, $B = (b_{jk})$. Dann ist
$A(\lambda B) = \sum_{j=1}^{n} a_{ij} \cdot \lambda b_{jk} = \sum_{j=1}^{n} \lambda a_{ij} \cdot b_{jk} = (\lambda A)B = \lambda \cdot \sum_{j=1}^{n} a_{ij} b_{jk} = \lambda(AB).$

Lemma: Matrizenmultiplikation ist assoziativ: $A(BC) = (AB)C$.

Beweis:
Sei $D = BC \in Mat_{n\times s}(K)$, $E = AB \in Mat_{m\times r}(K)$. Schreibe $A = (a_{ij})$ usw. Für i, l ist
$(AD) = \sum_{j=1}^{n} a_{ij} d_{jl} = \sum_{j=1}^{n} a_{ij} \cdot \sum_{k=1}^{r} b_{jk} c_{kl} = \sum_{j=1}^{n} \sum_{k=1}^{n} a_{ij} b_{jk} c_{kl}.$
$(EC) = \sum_{k=1}^{n} e_{ik} c_{kl} = \sum_{k=1}^{r} \sum_{j=1}^{n} a_{ij} b_{jk} c_{kl}.$ *Also ist $AD = EC$.*

Lemma: Für $m, n, r \in \mathbb{N}_0$ und $A, A' \in Mat_{m\times n}(K)$, $B, B' \in Mat_{n\times r}(K)$ ist
$(A + A')B = AB + A'B$ und $A(B' + B) = AB' + AB$.

Beweis:
Schreibe $A = (a_{ij})$ etc. Dann ist
$(A + A')B = \sum_{j=1}^{n} (a_{ij} + a'ij) b_{jk} = \sum_{j=1}^{n} a_{ij} + b_{jk} + \sum_{j=1}^{n} a'_{ij} + b_{jk} = (AB + A'B).$ *Rest analog.*

Satz: Mit der Matrizenmultiplikation wird $Mat_n(K)$ zu einem Ring mit Einselement 1.

Beweis:
Die vorherigen Sätze und Lemmas.

Beispiele:

- Für $n = 1$ können wir dem Ring $Mat_n(K)$ mit K identifizieren, der Ring ist also ein Körper, insbesondere ist er kommutativ.
- Für $n \geq 2$ ist $Mat_n(K)$ nicht kommutativ.

Definition invertierbar: Eine Matrix $A \in Mat_n(K)$ heißt invertierbar oder regulär, wenn sie im Ring $Mat_n(K)$ invertierbar ist, sonst singulär. Die Gruppe $GL_n(K) = Mat_n(K)^\times$ der invertierbaren $n \times n$ -Matrizen heißt allgemeine Gruppe.

Beispiel: Sei $n = 2$. Zu $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Mat_2(K)$ definiert man $\tilde{A} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \in Mat_2(K)$.
Man prüft nach, dass $A \cdot \tilde{A} = \tilde{A} \cdot A = (ad - bc) \cdot 1_2$. Definiert man nun $det(A) = ad - bc$ so sieht man: Ist $det(A) \neq 0$, so ist A invertierbar mit $A^{-1} = det(A)^{-1} \cdot \tilde{A}$. Ist $det(A) = 0$ so A ist Nullteiler und somit nicht invertierbar.

Lemma: Für $A, A_1, A_2 \in Mat_{m\times n}(K)$ und $B = Mat_{n\times r}(K)$ ist
- $(A^t)^t = A$
- $(A_1 + A_2)^t = A_1^t + A_2^t$
- $(AB)^t = B^t A^t$

Beweis:
Übung

Satz: Für $A \in Gl_n(K)$ ist $A^t \in GL_n(K)$ und $(A^{-1})^t = (A^t)^{-1}$

Beweis:
Aus $AA^{-1} = 1$ folgt, dass $(A^{-1})^t A^t = 1_n^t = 1_n$. Somit ist $(A^{-1})^t$ das Inverse zu A^t.

3.2 Homomorphismen von Gruppen

Seien G, H zwei multiplikativ geschriebene Gruppen.

Definition Gruppenhomomorphismus: Eine Abbildung $f : G \to H$ ist ein Gruppenhomomorphismus, wenn gilt:
(GH): $f(xy) = f(x) \cdot f(y)$
Die Menge der Homomorphismen $f : G \to H$ bezeichnet man mit $Hom(G, H)$.

Bemerkung: Ein Gruppenhomomorphismus ist also eine Abbildung, welche mit der Verknüpfung, also der Struktur der Gruppe, verträglich ist. Man beachte: für additiv geschriebe Gruppen lautet die Bedingung: $f(x + y) = f(x) + f(y)$.

Beispiele von Gruppenhomomorphismen:
- $id_G : G \to G$
- $c_1 : G \to H$ mit $x \mapsto 1_H$
- $G_0 \leq G$ Untergruppe, $\iota : G_0 \to G$

- $(A, +)$ abelsche Gruppe, $k \in \mathbb{Z}$, $A \to A$ mit $a \mapsto ka$
- $\mathbb{Z} \to \mathbb{Z}\backslash n\mathbb{Z}$ mit $\overline{a} \mapsto a + n\mathbb{Z}$
- $\mathbb{R} \to \mathbb{R}^\times$ mit $x \mapsto e^x$
- $Mat_n(K) \to Mat_n(K)$ mit $A \mapsto A^t$
- $\mathbb{C} \to \mathbb{R}^\times$ mit $z \mapsto |z|$

Satz: Sei $f \in Hom(G, H)$. Dann gilt:
- $f(1_G) \to 1_H$
- Für $x \in G$ ist $f(x^{-1}) = (f(x))^{-1}$.
- Für $x_1, ..., x_n \in G$ ist $f(x_1, ..., x_n) = f(x_1) \cdot ... \cdot f(x_n)$.
- Ist $G_0 \leq G$, so ist $f(G_0) \leq H$.
- Ist $H_0 \leq H$, so ist $f^{-1}(H_0) \leq G$.

Beweis:
- $f(1) = f(1 \cdot 1) = f(1) \cdot f(1) \Rightarrow$ *kürzen, weil* H *Gruppe* $\Rightarrow 1 = f(1)$
- $f(x) \cdot f(x^{-1}) = f(x \cdot x^{-1}) = f(1) = 1$
- *Induktion nach* n
- $x, y \in G_0 \Rightarrow f(x) \cdot f(y) = f(xy) \in f(G_0)$, $f^{-1}(x) = f(x^{-1}) \in f(G_0)$
- $x, y \in f^{-1}(H_0) \Rightarrow f(x) \cdot f(y) = f(xy) \in H_0 \Rightarrow xy \in f^{-1}(H_0)$, $f(x^{-1}) = (f(x))^{-1} \in H_0 \Rightarrow x^{-1} \in f^{-1}(H_0)$, $f(1) = 1 \in H_0 \Rightarrow 1 \in f^{-1}(H_0)$, *insbesondere* $f^{-1}(H_0) \neq \emptyset$

Satz: Seien G_1, G_2, G_3 Gruppen. Sind $f_1 : G_1 \to G_2$, $f_2 : G_2 \to G_3$ Homomorphismen, so ist auch $f_2 \circ f_1 : G_1 \to G_3$.

Beweis:
Für $x, y \in G_1$ *ist*
$(f_2 \circ f_1)(xy) = f_2(f_1(xy)) = f_2(f_1(x) \cdot f_1(y)) = f_2(f_1(x)) \cdot f_2(f_1(y)) = (f_2 \circ f_1)(x) \cdot (f_2 \circ f_1)(y)$

Definition Arten von Homomorphismen: Ein Homomorphismus ist
ein Monomorphismus, wenn f injektiv ist,
ein Epimorphismus, wenn f surjektiv ist,
ein Isomorphismus, wenn f bijektiv ist. Die Gruppen G und H heißen isomorph, in Zeichen $G \cong H$, wenn es einen Isomorphismus $G \to H$ gibt.

Lemma: Ist $f : G \to H$ ein Isomorphismus, so ist auch $f^{-1} : H \to G$ ein Isomorphismus.

Beweis:
Da f^{-1} *wieder bijektiv ist, müssen wir nur zeigen, dass* f^{-1} *ein Homomorphismus ist. Seien* $x, y \in H$. *Dann ist* $f(f^{-1}(x) \cdot f^{-1}(y)) = f(f^{-1}(x)) \cdot f(f^{-1}(y)) = xy$, *somit*
$f^{-1}(xy) = f^{-1}(x) \cdot f^{-1}(y)$.

Satz: Sei $f : G \to H$ ein Homomorphismus. Genau dann ist f ein Isomorphismus, wenn es einen Homomorphismus $f' : H \to G$ mit $f' \circ f = id_G$ und $f \circ f' = id_H$ gibt.

Beweis:
Ist f ein Isomorphismus, so erfüllt $f' := f^{-1}$ das Gewünschte. Ist umgekehrt f' wie angegeben, so muss f bijektiv sein:

- *$f' \circ f = id_G$ injektiv $\Rightarrow$ f injektiv*
- *$f \circ f' = id_H$ surjektiv $\Rightarrow$ f surjektiv*

Korollar: Isomorphie von Gruppen ist eine Äquivalenzrelation: Sind G, G_1, G_2, G_3 Gruppen, so gilt:

- $G \cong G$ (Reflexivität)
- Ist $G_1 \cong G_2$, so ist auch $G_2 \cong G_1$ (Symmetrie)
- Ist $G_1 \cong G_2$ und $G_2 \cong G_3$, dann ist auch $G_1 \cong G_3$ (Transitivität)

Beweis:

- *id_G ist ein Isomorphismus*
- *vorheriges Lemma*
- *vorletzer Satz und A18*

Bemerkung: Der letzte Satz erklärt die Bedeutung des Isomorphismus: Eine mit der Struktur verträgliche Abbildung, die eine mit der Struktur verträgliche Umkehrabbildung besitzt, also eine strukturerhaltende Abbildung. Tatsächlich können wir uns einen Isomorphismus $f : G \to H$ so vorstellen, dass wir nur die Elemente von G umbenennen. Alle Aussagen, die sich nur aus der Struktur selbst ergeben, bleiben damit wahr. Zum Beispiel: Ist $G \cong H$ und ist G abelsch, so auch H und umgekehrt.

Beispiele:

- Es ist $\mathbb{Z}^\times = \mu_2 \cong \mathbb{Z}\backslash 2\mathbb{Z} \cong (\mathbb{Z}\backslash 3\mathbb{Z})^\times \cong S_2$. Je zwei beliebige Gruppen der Ordnung 2 sind zueinander isomorph.
- $e : \mathbb{R} \to \mathbb{R}_{>0}$, $x \mapsto e^x$ liefert einen Isomorphismus, da $(\mathbb{R}, +) \to (\mathbb{R}, \cdot)$.

Definition Kern: Der Kern eines Gruppenhomomorphismus $f : G \to H$ ist
$Ker(f) := f^{-1}(\{1\}) = \{x \in G \mid f(x) = 1_H\}$.

Lemma: Ist $f : G \to H$ ein Homomorphismus, so ist $N := Ker(f)$ eine Untergruppe von G mit $x \cdot y \cdot x^{-1} \in N$ für alle $x \in G$ und $y \in N$.

Beweis:
Es ist $N \leq G$. Für $x \in G$ und $y \in N$ ist
$f(xyx^{-1}) = f(x) \cdot f(y) \cdot f(x^{-1}) = f(x) \cdot f(x^{-1}) \cdot 1 = f(x) \cdot f(x^{-1}) = 1$, *also* $xyx^{-1} \in N$.

Satz: Sei $f \in Hom(G, H)$. Genau dann ist f injektiv, wenn $Ker(f) = \{1_G\}$.

Beweis:
Schreibe $N = Ker(f)$.
Hinrichtung: Ist f injetiv, so ist $N \leq G$ mit $|N| \leq 1$, also $N = \{1_G\}$.
Rückrichtung: Sei $N = \{1_G\}$. Sind $x, y \in G$ mir $f(x) = f(y)$, so ist
$1 = (f(x))^{-1} \cdot f(y) = f(x^{-1} \cdot y)$, *also* $x^{-1} \cdot y \in N = \{1\}$ *und somit* $x = y$. *Folglich ist f injetiv.*

Definition Normalteiler: Ist $N \leq G$ mit $x^{-1}y \in N$ für alle $x \in G$ und $y \in N$, so nennt man N einen Normalteiler von G und schreibt $N \lhd G$.

3.3 Homomorphismen von Ringen

Seien R, S und T Ringe.

Definition Ringhomomorphismus: Eine Abbildung $f : R \to S$ ist ein Ringhomomorphismus, wenn für $x, y \in R$ gilt:
(RH1:) $f(x + y) = f(x) + f(y)$
(RH2:) $f(xy) = f(x) \cdot f(y)$
Die Menge der Ringhomomorhismen $f : R \to R$ wird mit $Hom(R, S)$ bezeichnet. Ein Homomorphismus $f : R \to S$ ist ein Mono-, Epi- oder Isomorphismus, wenn f injektiv, surjektiv oder bijektiv ist. Gibt es einen Isomorphismus $f : R \to S$, so nennt man R und S isomorph und schreibt $R \cong S$. Die Elemente von $End(R) := Hom(R, R)$ nennt man Endomorphismen. Der Kern eines Ringhomorphismus $f : R \to S$ ist $Ker(f) := f^{-1}(\{0\})$.

Bemerkung: Ein Ringhomomorphismus $f : R \to S$ ist ein Gruppenhomomorphismus der abelschen Gruppen $(R, +)$ und $(S, +)$, der mit der Multiplikation verträglich ist, also eine strukturverträgliche Abbildung zwischen Ringen.

Beispiele:

- $id_R : R \to R$ ist ein Ringisomorphismus
- Ist $R_0 \leq R$ ein Unterring von R, so ist $\iota : R_0 \to R$ ein Ringmonomorphismus
- $\mathbb{Z} \to \mathbb{Z}\backslash n\mathbb{Z}$ mit $\overline{a} \mapsto a + n\mathbb{Z}$ it ein Ringepimorphismus
- Sei R kommutativ mit Einselement. Für $\lambda \in R$ ist die Auswertungsabbildung $R[X] \to R$ mit $f \mapsto f(\lambda)$ ein Ringepimorphismus.
- $\mathbb{C} \to \mathbb{C}$ mit $z \mapsto \overline{z}$ ist ein Ringisomorphismus

Satz: Sind $f : R \to S$ und $g : S \to T$ Ringhomomorphismen, so auch $g \circ f : R \to T$.

Beweis:
Übung, analog zu Gruppen

Lemma: Ist $f : R \to S$ ein Ringisomorphismus, so auch $f^{-1} : S \to R$.

Beweis:
Von den Gruppen wissen wir: f^{-1} ist ein Isomorphismus der abelschen Gruppen $(S, +) \to (R, +)$. Die Verträglichkeit mit der Multiplikation zeigt man analog.

Satz: Sei $f \in Hom(R, S)$. Genau dann ist f ein Ringisomorphismus, wenn es $f' \in Hom(S, R)$ mit $f' \circ f = id_R$ und $f \circ f' = id_S$ gibt.

Beweis:
analog zu Gruppen

Lemma: Der Kern $I := Ker(f)$ eines Ringhomomorphismus $f : R \to S$ ist eine Untergruppe von $(R, +)$ mit $x \cdot a, a \cdot x \in I$ für alle $a \in I$ und $x \in R$.

Beweis:
Von den Gruppen wissen wir: I ist eine Untergruppe von $(R, +)$. Für $x \in R$ und $a \in I$ ist $f(xa) = f(x) \cdot f(a) = f(x) \cdot 0 = 0$. Somit ist $xa \in I$. Analog ist $ax \in I$.

Satz: Sei $f \in Hom(R, S)$. Genau dann ist f injektiv, wenn $Ker(f) = \{0\}$.

Beweis:
Die Aussage folgt aus dem entsprechenden Satz für Gruppen, da $f : (R, +) \to (S, +)$ ein Gruppenhomomorphismus ist.

Definition Ideal: Ist I eine Untergruppe von $(R, +)$ und $xa, ax \in I$ mit $x \in R$ und $a \in I$, so nennt man I ein Ideal von R und schreibt $I \lhd R$.

Beispiel: Der Kern des Ringhomomorphismus $\mathbb{Z} \to \mathbb{Z}\backslash n\mathbb{Z}$ mit $a \mapsto \overline{a}$ ist das Ideal $I = n\mathbb{Z} \lhd \mathbb{Z}$.

3.4 Homomorphismen von Vektorräumen

Seien U, V, W drei K-VR.

Definition K-linear: Eine Abbildung $f : V \to W$ heißt K-linearer Homomorphismus von K-VR, wenn für alle $x, y \in V$ und $\lambda \in K$ gilt:
(L1): $f(x + y) = f(x) + f(y)$
(L2): $f(\lambda x) = \lambda \cdot f(x)$
Die Menge der K-linearen Abbildungen $f : V \to W$ wird mit $Hom_K(V, W)$ bezeichnet. Die Elemente von $End_K(V) := Hom_K(V, V)$ nennt man die Endomorphismen von V. Ein $f \in Hom_K(V, W)$ ist ein Mono-, Epi- bzw. Isomorphismus, falls f injektiv, surjektiv bzw. bijektiv ist. Einen Endomorphismus der auch ein Isomorphismus ist, nennt man Automorphismus von V und bezeichnet die Menge der Automorphismen von V mit $Aut_K(V)$. Der Kern einer linearen Abbildung $f : V \to W$ ist $Ker(f) := f^{-1}(\{0\})$.

Bemerkung: Eine K-lineare Abbildung $f : V \to W$ ist also ein Homomorphismus der abelschen Gruppen $(V, +) \to (W, +)$, der mit der Skalarmultiplikation verträglich ist, d.h. eine strukturverträgliche Abbildung zwischen VR.

Satz: Eine Abbildung $f : V \to W$ ist genau dann K-linear, wenn für alle $x, y \in V$ und $\lambda, \mu \in K$ gilt:
(L): $f(\lambda x + \mu y) = \lambda f(x) + \mu f(y)$.

Beweis:

Hinrichtung: $f(\lambda x + \mu y) = f(\lambda x) + f(\mu y) = \lambda f(x) + \mu f(y)$
Rückrichtung: (L1): $f(x+y) = f(1x + 1y) = 1f(x) + 1f(y)$*, (L2):* $f(\lambda x) = f(\lambda x + 0y) = \lambda f(x)$.

Beispiele:

- $id_V : V \to V$ ist ein Automorphismus von V
- $c_0 : V \to W$ mit $x \mapsto 0$ ist K-linear
- Für einen UVR $V_0 \leq V$ ist $\iota : V_0 \to V$ ein Monomorphismus
- Im K-VR $K[X]$ kann man die (formale) Ableitung definieren: $(\sum_{i=0}^{n} a_i X^i)' := \sum_{i=1}^{n} i a_i X^{i-1}$. Diese Abbildung $K[X] \to K[X]$ mit $f \mapsto f'$ ist ein K-Endomorphismus von $K[X]$.

Beispiel: Sei $V = K^n$ und $W = K^m$. Wir fassen die Elemente von V und W als Spaltenvektoren auf. Zu einer Matrix $A \in Mat_{m\times n}(K)$ definieren wir die Abbildung $f_A : V \to W$ mit $x \mapsto Ax$. Ausgeschrieben: Ist $A = (a_{ij})$ und $x = (x_1, ..., x_n)^t$ so ist

$f_A(x) = Ax = \begin{pmatrix} a_{11} & ... & a_{1n} \\ ... & & ... \\ a_{m1} & ... & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ ... \\ x_n \end{pmatrix} = \begin{pmatrix} a_{11} \cdot x_1 + ... + a_{1n} \cdot x_n \\ ... \\ a_{m1} \cdot x_1 + ... + a_{mn} \cdot x_n \end{pmatrix}$. Diese Abbildung ist K-linear.

Satz: Für ein $f \in Hom_K(V, W)$. Dann gilt:

- $f(0) = 0$
- Für $x, y \in V$ ist $f(x - y) = f(x) - f(y)$.
- Sind (x_1) aus V, (λ_i) aus K, fast alle gleich 0, so ist $f(\sum_{i\in I} \lambda_i \cdot x_i) = \sum_{i\in I} \lambda_i \cdot f(x)$.
- Ist (x_i) linear abhängig in V, so ist $f(x_i)$ linear abhängig in W.
- Ist $V_0 \leq V$ ein UVR von V, so ist $f(V_0) \leq W$ ein UVR.
- Ist $W_0 \leq W$ ein UVR von W, so ist $f^{-1}(W_0) \leq V$ ein UVR.

Beweis:

- *klar*
- *klar*
- *Induktion*
- $\sum \lambda_i \cdot x_i = 0 \Rightarrow 0 = f(0) = f(\sum \lambda_i \cdot x_i) = \sum \lambda_i \cdot f(x_i)$
- $x, y \in V_0 \Rightarrow f(x) + f(y) = f(x + y) \in f(V_0)$
  $x \in V_0, \lambda \in K \Rightarrow f(x \cdot \lambda = f(\lambda x) \in f(V_0))$
- $f(0) = 0 \in W_0 \Rightarrow 0 \in f^{-1}(W_0)$*, insbesondere ist* $f^{-1}(W_0) \neq \emptyset$
  $x, y \in f^{-1}(W_0) \Rightarrow f(x + y) = f(x) + f(y) \in W_0$*, also* $x + y \in f^{-1}(W_0)$
  $x \in f^{-1}(W_0)$ *und* $\lambda \in K \Rightarrow f(\lambda x) = \lambda f(x) \in W_0$*, also* $\lambda x \in f^{-1}(W_0)$

Satz: Sind $f : V \to W$ und $g : W \to U$ K-linear, so auch $g \circ f : V \to U$.

Beweis:
Für $x, y \in V$ *und* $\lambda, \mu \in K$ *ist*
$(g \circ f)(\lambda x + \mu y) = g(f(\lambda x + \mu y)) = g(\lambda f(x) + \mu f(y)) = \lambda(g \circ f)(x) + \mu(g \circ f)(y)$.

Lemma: Ist $f : V \to W$ ein Isomorphismus, so auch $f^{-1} : W \to V$.

Beweis:
Wir müssen nur zeigen, dass f^{-1} linear ist. Für $x, y \in V$ und $\lambda, \mu \in K$ ist
$f(\lambda f^{-1}(x) + \mu f^{-1}(y)) = \lambda(f \circ f^{-1})(x) + \mu(f \circ f^{-1})(y) = \lambda x + \mu y$, *also*
$f^{-1}(\lambda x + \mu y) = \lambda f^{-1}(x) + \mu f^{-1}(y)$.

Satz: Sei $f : V \to W$ linear. Genau dann ist f ein Isomorphismus, wenn es eine lineare Abbildung $f' : W \to V$ gibt mit $(f' \circ f) = id_V$ und $(f \circ f') = id_W$.

Beweis:
Ist f ein Isomorphismus, so erfüllt $f' = f^{-1}$ die Behauptung. Existiert umgekehrt f' wie angegeben, so muss f bijektiv sein.

Bemerkung: Wie auch bei Gruppen sehen wir hier bei VR, dass Isomorphismen genau die strukturerhaltenden Abbildungen sind. Wieder können wir uns einen Isomorphismus $f : V \to W$ so vorstellen, dass wir nur die Elemente von V umbennen. Alle Aussagen, die sich nur aus der Struktur selbst ergeben, bleiben damit wahr, wie z.B. $dim_K(V) = dim_K(W) \iff V = W$. Insbesondere ist $K^n \cong K^m$ für $n = m$.

Satz: Ist $f : V \to W$ eine lineare Abbildung, so ist $Ker(f)$ ein UVR von V. Genau dann ist f ein Monomorphismus, wenn $Ker(f) = \{0\}$.

Beweis:
Der erste Teil folgt aus dem letzten Beispiel, der zweite folgt aus den Gruppen, da $f : (V, +) \to (W, +)$ ein Gruppenhomomorphismus ist.

3.5 Der Vektorraum der linearen Abbildungen

Seien V und W zwei K-VR.

Satz: Sei (x_i) eine Basis von V und (y_i) eine Familie in W. Dann gibt es genau eine lineare Abbildung $f : V \to W$ mit $f(x_i) = y_i$. Diese Abbildung ist durch $f(\sum \lambda_i x_i) = \sum \lambda_i y_i$ (*) ($\lambda_i \in K$, fast alle gleich 0) gegeben und erfüllt

- $Image(f) = span_K(y_i)$
- genau dann ist f injektiv, wenn (y_i) linear unabhängig ist

Beweis:
Ist $f : V \to W$ linear mit $f(x_i) = y_i$, so folgt $f(\sum \lambda_i x_i) = \sum \lambda_i y_i$. Da sich jedes $x \in V$ als $x = \sum \lambda_i x_i$ schreiben lässt, ist f dadurch schon eindeutig bestimmt. Andererseits wird durch (*) eine wohldefinierte Abbildung beschrieben, da die Darstellung von x eindeutig ist (denn x_i sind linear unabhängig). Es bleibt zu zeigen, dass die durch (*) definierte Abbildung $f : V \to W$ tatsächlich linear ist. Ist $x = \sum \lambda_i x_i$ und $x' = \sum \lambda'_i x_i$ so ist
$f(x + x') = f(\sum(\lambda_i + \lambda'_i)x_i) = \sum(\lambda_i + \lambda'_i)y_i = \sum \lambda_i y_i + \sum \lambda'_i y_i = f(x) + f(x')$.
$f(\lambda x) = f(\sum \lambda\lambda_i x_i) = \sum \lambda\lambda_i y_i = \lambda \sum \lambda_i y_i = \lambda f(x)$.

- *$Image(f)$ ist ein UVR von W und $\{y_i\} \subset Image(f) \subset span_K(y_i)$, somit $Image(f) = span_K(y_i)$*
- *f ist injektiv* $\iff Ker(f) = \{0\}$
  $\iff$ *$\lambda_i \in K$ gilt:* $f(\sum \lambda_i x_i) = 0 \Rightarrow \sum \lambda_i x_i = 0$
  $\iff$ *$\lambda_i \in K$ gilt:* $\sum \lambda_i y_i = 0 \Rightarrow \lambda_i = 0$
  $\iff$ *(y_i) linear unabhängig.*

Korollar: Sei $dim_K < \infty$. Ist $(x_1, ..., x_n)$ eine linear unabhängige Familie in V und $(y_1, ..., y_n)$ eine Familie in W, so gibt es eine lineare Abbildung $f : V \to W$ mit $f(x_i) = y_i$

Beweis:
Nach dem Basisergänzungssatz können wir die Familie (x_i) zu einer Basis $x_1, ..., x_m$ ergänzen. Die Behauptung folgt aus dem vorherigen Satz für beliebige $y_{n+1}, ..., y_m \in W$.

Korollar: Ist (x_i) eine Basis von V und (y_i) eine Basis in W, so gibt es genau einen Isomorphismus $f : V \to W$ mit $f(x_i) = y_i$.

Beweis:
Sei f wie im ersten Satz. (y_i) ist Erzeugendensystem $\Rightarrow Image(f) = span_K(y_i) = W$, also f surjektiv. (y_i) linear abhängig $\Rightarrow f$ ist injektiv.

Korollar: Zwei endlichdimensionale K-VR sind genau dann isomorph, wenn sie dieselbe Dimension haben.

Beweis:
letztes Korllar und letztes Kapitel

Korollar: Ist $B = (v_1, ..., v_n)$ eine Basis von V, so gibt es genau einen Isomorphismus $\Phi_B : K^n \to V$ mit $f(e_i) = v_i$. Insbesondere ist jeder endlichdimensionale K-VR zu einem Standardraum isomorph, nämlich zu K^n für $n = dim_K(V)$.

Definition Koordinatensystem: Die Abbildung Φ_B heißt Koordinatensystem zu B. Für $v \in V$ ist $(x_1, ..., x_n)^t = \Phi_B^{-1}(v) \in K^n$ der Koordinatenvekor zu v bezüglich B und $(x_1, ..., x_n)$ sind die Koordinaten von v bezüglich B.

Satz: Die Menge $Hom_K(V, W)$ ist eine UVR des K-VR $Abb(V, W)$.

Beweis:
Seien $f, g \in Hom_K(V, W)$ und $\eta \in K$.
- *$f + g \in Hom_K(V, W)$: Für $x, y \in V$ und $\lambda, \mu \in K$ ist $(f + g)(\lambda x + \mu y) = f(\lambda x + \mu y) + g(\lambda x + \mu y) = \lambda f(x) + \mu f(y) + \lambda g(x) + \mu g(y) = \lambda(f + g)(x) + \mu(f + g)(y)$*
- *$\eta f \in Hom_K(V, W)$: Für $x, y \in V$ und $\lambda, \mu \in K$ ist $(\eta f)(\lambda x + \mu y) = \eta \cdot f(\lambda x + \mu y) = \eta(\lambda f(x) + \mu f(y)) = \lambda(\eta f)(x) + \mu(\eta f)(y)$*

- $Hom_K(V,W) \neq \emptyset$: $c_0 \in Hom_K(V,W)$

Lemma: Sei U ein weiterer K-VR. Sind $f, f_1, f_2 \in Hom_K(V,W)$ und $g, g_1, g_2 \in Hom_K(U,V)$, so ist $f \circ (g_1 + g_2) = f \circ g_1 + f \circ g_2$ und $(f_1 + f_2) \circ g = f_1 \circ g + f_2 \circ g$.

Beweis:
Für $x \in U$ ist
- $(f \circ (g_1 + g_2))(x) = f((g_1 + g_2)(x)) = f(g_1(x) + g_2(x)) = f(g_1(x)) + f(g_2(x)) = (f \circ g_1 + f \circ g_2)(x)$
- $((f_1 + f_2) \circ g)(x) = (f_1 + f_2)(g(x)) = f_1(g(x)) + f_2(g(x)) = (f_1 \circ g + f_2 \circ g)(x)$

Korollar: Unter der Komposition wird $End_K(V)$ zu einem Ring mit Einselement id_V und $End_K(V)^\times = Aut_K(V)$.

Beweis:
$(End_K(V), +)$ ist eine abelsche Gruppe, die Komposition eine Verknüpfung auf $End_K(V)$ ist assoziativ und die Distributivgesetze gelten (vorheriges Lemma).

Bemerkung: Die Menge der strukturverträglichen Abbildungen zwischen K-VR trägt also wieder die Struktur eines K-VR. Wir können diesen mit unseren Mitteln untersuchen und z.B. nach Dimension und Basis fragen.

Lemma: Seien $m, n, r \in \mathbb{N}$, $A \in Mat_{m \times n}(K)$, $B \in Mat_{n \times r}(K)$. Für die linearen Abbildungen $f_A \in Hom_K(K^n, K^m)$, $f_B \in Hom_K(K^r, K^n)$ gilt dann $f_{AB} = f_A \circ f_B$.

Beweis:
Sind $A = (a_{ij})$ und $B = (b_{jk})$, so ist $(f_A \circ f_B)(e_k) = f_A(f_B(e_k)) = f_A(Be_k) = f_A(b_{1k}, ..., b_{nk})^t = A \cdot (b_{1k}, ..., b_{nk})^t = (\sum_{j=1}^{n} a_{ij} b_{jk}, ..., \sum_{j=1}^{n} a_{mj} b_{jk})^t = AB \cdot e_k = f_{AB}(e_k)$ für $k = 1, ..., r$, also
$f_A \circ f_B = f_{AB}$.

Satz: Die Abbildung $A \to f_A$ liefert einen Isomorphismus von K-VR $F_{m \times n} : Mat_{m \times n}(K) \to Hom_K(K^n, K^m)$ sowie einen Ringisomorphismus $F_n : Mat_n(F) \to End_K(K^n)$ der $GL_n(K)$ auf $Aut_K(K^n)$ abbildet.

Beweis: Wir schreiben F für $F_{m \times n}$
- *F ist linear: Sind $A, B \in Mat - n \times m(K)$ und $\lambda, \mu \in K$, so ist $F(\lambda A + \mu B)(x) = f_{\lambda A + \mu B}(x) = (\lambda A + \mu B)x = \lambda Ax + \mu Bx = \lambda f_A(x) + \mu f_B(x) = (\lambda F(A) + \mu F(B))(x)$, also ist F linear.*
- *F ist injektiv: Es genügt zu zeigen, dass $Ker(f) = \{0\}$. Ist $A = (a_{ij}) \in Mat_{n \times m}(K)$ mit $F(A) = 0$, so insbesondere $0 = F(A)(e_j) = f_A(e_j) = Ae_j = (a_{1j}, ..., a_{mj})^t$, also $A = 0$.*
- *F ist surjektiv: Sei $f \in Hom_K(V,W)$. Schreibe $f(e_j) = (a_{1j}, ..., a_{mj})^t$ und setze $A = (a_{ij}) \in Mat_{n \times m}(K)$. Dann ist $f_A \in Hom_K(K^n, K^m)$ mit $f_A(e_j) = Ae_j = f(e_j)$, also $f = f_A = F(A) \in Image(f)$.*
- *F_n ist eine Ringhomomorphismus:*
  (RH1) aus (L1)
  (RH2) aus $f_{AB} = f_A \circ f_B$.

- *Somit ist F_n eine Ringisomorphismus $\Rightarrow F_n(Mat_n(K)^\times) = End_K(V)^\times$, also $F_n(GL_n(K)) = Aut_K(V)$.*

3.6 Koordinatendarstellung linearer Abbildungen

Seien V, W endlichdimensionale K-VR mit den Basen $B = (x_1, ..., x_n)$ und $C = (y_1, ..., y_m)$.

Definition darstellende Matrix: Sei $f \in Hom_K(V, W)$. Für $j = 1, ..., n$ schreiben wir $f(x_j) = \sum_{i=1}^{m} a_{ij} y_i$ mit eindeutig bestimmten $a_{ij} \in K$. Die Matrix $M_C^B(f) = (a_{ij}) \in Mat_{m \times n}(K)$ heißt die darstellende Matrix von f bezüglich der Basen B und C.

Satz: Sei $f \in Hom_K(V, W)$. Die darstellende Matrix $M_C^B(f)$ ist die eindeutig bestimmte Matrix $A \in Mat_{n \times m}(K)$, für die das folgenden Diagramm kommutiert:

$$\begin{array}{ccc} K^n & \xrightarrow{f_A} & K^m \\ {\scriptstyle \Phi_B}\downarrow & & \downarrow{\scriptstyle \Phi_C} \\ V & \xrightarrow[f]{} & W \end{array}$$

d.h. $f \circ \Phi_B = \Phi_C \circ f_A$.

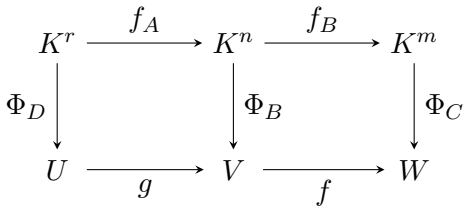
Beweis:
Sei zunächst $A = M_C^B(f)$. Für $j = 1, ..., n$ ist
$\Phi_C(f_A(e_j)) = \Phi_C((a_{1j}, ..., a_{mj})^t) = \sum_{i=1}^{m} a_{ij} \cdot y_i = f(x_j) = f(\Phi_B(e_j))$, *also $\Phi_C \circ f_A = f \circ \Phi_B$.*
Sei umgekehrt $A \in Mat_{m \times n}(K)$ mit $\Phi_C \circ f_A = f \circ \Phi_B$. Da Φ_B und Φ_C Isomorphismen sind, ist f_A eindeutig bestimmt: $f_A = \Phi_C^{-1} \circ f \circ \Phi_B$ und deshalb auch A.

Korollar: Die Abbildung M_C^B: $Hom_K(V, W) \to Mat_{m \times n}(K)$ ist ein Isomorphismus von K-VR.

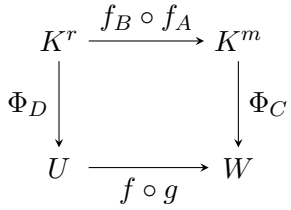
Beweis:
Definiere A: $Hom_K(V, W) \to Mat_{m \times n}(K)$ mit $f \mapsto \Phi_C^{-1} \circ f \circ \Phi_B$. $A(f) = F_{m \times n}(M_C^B(f))$, also $A = F_{m \times n} \circ M_C^B$. Die Abbildung ist bijektiv, da Φ_B und Φ_C bijektiv sind, und linear, da Φ_B und Φ_C linear sind. Also ist A ein Isomorphismus. Da auch $F_{m \times n}^{-1}$ ein Isomorphismus ist, ist folglich auch $M_C^B = F_{m \times n}^{-1} \circ A$.

Lemma: Sei U ein weitere K-VR mit endlicher Basis D. Für $f \in Hom_K(V, W)$ und $g \in Hom_K(U, V)$ ist $M_C^B(f) \cdot M_B^D(g) = M_C^D(f \circ g)$.

Beweis:
Sei $r = dim_K(U)$ und $A = M_B^D(g)$ und $B = M_C^B(f)$. Nach dem letzen Satz kommutieren die beiden kleinen Quadrate in:



Deshalb kommutiert auch:



Die Eindeutigkeit impliziert deshalb, dass $F_{m\times n}(M_C^B(f)) \circ F_{r\times m}(M_B^D(g)) = F_{r\times n}(M_C^D(f \circ g))$. *Da* $F_{r\times n}$ *injektiv ist, folgt* $M_C^B(f) \cdot M_B^D(g) = M_C^D(f \circ g)$.

Korollar: Sei $f \in Hom_K(V, W)$. Genau dann ist f ein Isomorphismus, wenn $m = n$ und $M_C^B(f) = GL_n(K)$. In diesem Fall ist $M_B^C(f^{-1}) = M_C^B(f)^{-1}$.

Beweis:
Sei $A = M_C^B(f)$. f *ist genau dann ein Isomorphismus, wenn* f_A *einer ist, und in diesem Fall ist* $m = n$. *Zudem ist* f_A *genau dann ein Isomorphimus, wenn* $A \in GL_n(K)$. *Ist* f *ein Isomorphismus, so ist* $M_B^C(f^{-1}) \cdot M_C^B(f) = M_C^C(f^{-1} \circ f) = 1_n$, *also* $M_B^C(f^{-1}) = M_C^B(f)^{-1}$.

Korollar: Die Abbildung $M_B := M_B^B$: $End_K(V) \to Mat_n(K)$ ist ein Ringisomorphismus, der $Aut_K(V)$ auf $GL_n(K)$ abbildet.

Beweis:
Die vorherigen Korollare und das Lemma.

Definition Transformationsmatrix: Sind B und B' Basen von V, so nennt man $T_B^{\prime B} := M_{B'}^B(id_V) \in GL_n(K)$ die Transformationsmatrix des Basiswechsels von B nach B'.

Bemerkung: Nach dem letzen Satz ist $T_{B'}^B$, also die Matrix A, die $f_A = \Phi_B^{-1} \circ \Phi_B$ erfüllt. Ist $x = \Phi_B^{-1}(v) \in K^n$ der Koordinatenvektor von v bezüglich B, so ist $T_{B'}^B \cdot x = f_{T_{B'}^B}(x) = (\Phi_{B'} \circ \Phi_B)(\Phi_B^{-1}(v)) = \Phi_{B'}^{-1}(v)$ der Koordinatenvektor von v bezüglich B'.

Satz (Transformationsformel): Seien B, B' Basen von V und C, C' Basen von W. Für $f \in Hom_K(V, W)$ ist $M_C^{\prime B}(f) = T_C^{\prime C} \cdot M_C^B(f) \cdot (T_B^{\prime B})^{-1}$.

Beweis:
$f = id_W \circ f \circ id_V$ *mit den Basen* B', B, C, C' *und erhält*
$M_{C'}^{B'}(f) = M_{C'}^C(id_W) \cdot M_C^B(f) \cdot M_B^{B'}(id_V) = T_{C'}^C \cdot M_C^B(f) \cdot T_B^{B'}$ *und*
$T_B^{B'} = M_B^{B'}(id_V) = M_B^{B'}(id_V^{-1}) = M_{B'}^B(id_V)^{-1} = (T_{B'}^B)^{-1}$.

Korollar: Sind B und B' Basen von V und $f \in End_K(V)$, so gilt
$M_{B'}(f) = T^B_{B'} \cdot M_B(f) \cdot (T^B_{B'})^{-1}$.

Beweis:
später