Lineare Algebra WS2017/18

Dozent: Prof. Dr. Arno Fehm

4. Juni 2018

Inhaltsverzeichnis

Kapitel I
Grundbegriffe der Linearen Algebra

1. Logik und Mengen

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

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 zusammengesetzten 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

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.

Überblick über die Beweise

Unter einem Beweis verstehen wir die lückenlose Herleitung einer mathematischen Aussage aus einer Menge von Axiomen, Voraussetzungen 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: $P(1) \wedge \forall n : (P(n) \Rightarrow P(n+1)) \Rightarrow \forall n : P(n)$.

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 1.1 (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 1.2 (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 1.3 (leere Menge)**
Es gibt genau eine Menge, die keine Elemente hat, die leere Menge $0 := \{\}$.

Definition 1.4 (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 1.5 (Mengenoperationen)
Seien X und Y Mengen. Man definiert daraus weitere Mengen wie folgt (Mengenoperationen):

- $X \cup Y := \{x \mid x \in X \vee x \in Y\}$
- $X \cap Y := \{x \mid x \in X \wedge x \in Y\}$
- $X \backslash Y := \{x \in X \mid x \notin Y\}$
- $X \times Y := \{(x, y) \mid x \in X \wedge y \in Y\}$
- $\mathcal{P}(X) := \{Y \mid Y \subset X\}$

Neben den offensichtlichen Mengengesetzen, wie dem Kommutativgesetz, 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:

- $|X \times Y| = |X| \cdot |Y|$
- $|\mathcal{P}(X)| = 2^{|X|}$

2. Abbildungen

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 Definitionsmenge 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 $\mathrm{Abb}(X, Y)$ bezeichnen.

■ **Beispiel 2.1**

- Abbildungen mit Zielmenge $\mathbb{R}$ nennt man Funktion: $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$
- Abbildungen mit Zielmenge $\supset$ 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.

■ **Beispiel 2.2**

- auf jeder Menge X gibt es die identische Abbildung (Identität)
  $\mathrm{id} : X \to X, x \mapsto x$
- 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
  $f : X \times X \to \mathbb{R}, (x, y) \mapsto \delta_{x,y} \begin{cases} 1 & (x = y) \\ 0 & (x \neq y) \end{cases}$

■ **Beispiel 2.3 (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 2.4 (Einschränkung)
Sei $f : x \mapsto y$ eine Abbildung. Für $A \subset X$ definiert man die Einschränkung/Restrikton von f auf A als die Abbildung

$$f|_A : \begin{cases} A \to Y \\ a \mapsto f(a) \end{cases}$$

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 $\mathrm{Im}(f) := f(X)$ das Bild von f.

▶ **Bemerkung 2.5**
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.

■ **Beispiel 2.6**
Genau dann ist $f : X \to Y$ surjektiv, wenn $\mathrm{Im}(f) = Y$

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 2.7 (Komposition)
Sind $f : X \to Y$ und $g : Y \to Z$ Abbildungen, so ist die Komposition $g \circ f$ die Abbildung

$$g \circ f := \begin{cases} X \to Z \\ x \mapsto g(f(x)) \end{cases}$$

Man kann die Komposition auffassen als eine Abbildung $\circ : \mathrm{Abb}(Y, Z) \times \mathrm{Abb}(X, Y) \to \mathrm{Abb}(X, Z)$.

Satz 2.8
Die Abbildung von Kompositionen ist assoziativ, d.h. es gilt:

$$h \circ (g \circ f) = (h \circ g) \circ f$$

.

Beweis. Sowohl $h \circ (g \circ f)$ als auch $(h \circ g) \circ f$ haben die Definitionsmenge X und die Zielmenge W und für jedes $x \in X$ ist $(h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x))) = (h \circ g)(f(x)) = ((h \circ g) \circ f)(x)$. □

Definition 2.9 (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

$$f^{-1} : \begin{cases} Y \to X \\ y \mapsto x_y \end{cases}$$

wird also eine Abbildung definiert, die Umkehrabbildung zu f.

Satz 2.10
Ist die Abbildung $f : X \to Y$ bijektiv, so gelten

$$f^{-1} \circ f = id_x$$
$$f \circ f^{-1} = id_y$$

Beweis. Es ist $f^{-1} \in \text{Abb}(X, X)$ und $f \circ f^{-1} \in \text{Abb}(Y, Y)$. Für $y \in Y$ ist $(f \circ f^{-1})(x) = f(f^{-1}(y)) = y = id_Y$. Für $x \in X$ ist deshalb $f((f^{-1} \circ f)(x)) = (f \circ (f^{-1} \circ f))(x) = ((f \circ f^{-1}) \circ f)(x) = (id_Y \circ f)(x) = f(x)$. Da f injektiv, folgt $f^{-1} \circ f = id_X$. □

▶ **Bemerkung 2.11**
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 2.12 (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

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

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

■ **Beispiel 2.13**
Eine Folge ist eine Familie $(x_i)_{i \in I}$ mit der Indexmenge $\mathbb{N}_0$.

Definition 2.14 (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 2.15 (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 $\Gamma = \Gamma_f$.

3. Gruppen

Definition 3.1 ((Halb-)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 $*$.

Beispiel 3.2

- Für jede Menge X ist $(\mathrm{Abb}(X, Y), \circ)$ 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 3.3 (Eindeutigkeit des neutralen Elements)
Ein Monoid $(G, *)$ hat genau ein neutrales Element.

Beweis. Nach Definition besitzt $(G, *)$ mindestens ein neutrales Element. Seien $e_1, e_2 \in G$ neutrale Elemente. Dann ist $e_1 = e_1 * e_2 = e_2$. Damit besitzt $(G, *)$ höchstens ein neutrales Element, also genau ein neutrales Element. □

Definition 3.4 (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 Gruppe abelsch.

Ein x' heißt inverses Element zu x.

Beispiel 3.5

- $\mathbb{N}_0$ 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 3.6 (Eindeutigkeit des Inversen)
Ist $(G, *)$ eine Gruppe, so hat jedes $x \in G$ genau ein inverses Element.

Beweis. Nach Definition hat jedes $x \in G$ mindestens ein Inverses. Seien $x', x'' \in G$ inverse Elemente zu x. Dann ist $x' = x' * e = x' * (x * x'') = (x' * x) * x'' = e * x'' = x''$. Es gibt also genau ein Inverses zu x. □

Beispiel 3.7

- 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 $Sym(X) := \{f \in \mathrm{Abb}(X,X) \mid f \text{ ist bijektiv}\}$ der Permutationen von X bildet mit der Komposition eine Gruppe $(\mathrm{Sym}(X), \circ)$, die symmetrische Gruppe auf X. Für $n \in \mathbb{N}$ schreibt man $S_n := \mathrm{Sym}(\{1,2,...,n\})$. Für $n \geq 3$ ist S_n nicht abelsch.

▶ **Bemerkung 3.8**
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 3.9
Sei $(G,\cdot)$ eine Gruppe. Für $x, y \in G$ gelten

$$(x^{-1})^{-1} = x$$
$$(xy)^{-1} = x^{-1} \cdot x^{-1}$$

Beweis. Nach Definition erfüllt $z = x$ die Identitäten $x^{-1}z = zx^{-1} = 1$ und somit ist $(x^{-1})^{-1} = z = x$. Ebenso ist $(y^{-1}x^{-1}) \cdot (xy) = y^{-1}(x^{-1}x)y = 1$ und $(xy) \cdot (x^{-1}y^{-1}) = x(yy^{-1})x^{-1} = 1$, also $y^{-1}x^{-1} = (xy)^{-1}$. □

Satz 3.10
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 3.11**
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.

■ **Beispiel 3.12**

- die triviale Gruppe $G = \{e\}$

$\cdot$	e
e	e

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

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

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

$\circ$	$\mathrm{id}_{\{1,2\}}$	f
$\mathrm{id}_{\{1,2\}}$	$\mathrm{id}_{\{1,2\}}$	f
f	f	$\mathrm{id}_{\{1,2\}}$

Definition 3.13 (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 3.14
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 $\iota_H \cdot_H \to G$ die Inklusionsabbildung ist) und $(H, \cdot_H)$ eine Gruppe ist.

Beweis. $\Rightarrow$: Sei H eine Untergruppe von G. Nach (UG1) ist $\mathrm{Im}(\cdot|_{H\times H}) \subset H$ 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.
$\Leftarrow$: Sei nun umgekehrt $(H, \cdot_H)$ eine Gruppe. Für $x, y \in H$ ist dann $xy = x \cdot_H y \in H$, also erfüllt 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 3.15**
Wir nennen nicht nur die Menge H eine Untergruppe von G, sondern auch die Gruppe $(H, \cdot_H)$. Wir schreiben $H \leq G$.

■ **Beispiel 3.16**
- 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 3.17
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 3.18
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 Lemma 3.17 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 3.19 (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 $\langle X \rangle$, falls $X = \{x_1, x_2, ..., x_n\}$ enthält auch mit $\langle x_1, x_2, ..., x_n \rangle$. Gibt es eine endliche Menge $X \subset G$ mit $G = \langle X \rangle$, so nennt man G endlich erzeugt.

■ **Beispiel 3.20**

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

4. Ringe

Definition 4.1 (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 Unterring eines Rings $(R, +, \cdot)$ ist eine Teilmenge, die mit der geeigneten Einschränkung von Addition und Multiplikation wieder ein Ring ist.

▶ **Bemerkung 4.2**
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 $(R, +, \cdot)$.

■ **Beispiel 4.3**

- 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.

▶ **Bemerkung 4.4**
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 4.5**
Wir führen eine wichtige Klasse endlicher Ringe ein. Hierfür erinnern wir uns an eine der Grundlagen der Arithmetik in $\mathbb{Z}$.

Theorem 4.6
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 4.7 (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 Theorem 4.6 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 4.8**
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 4.9 (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 4.10 (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 4.11 (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 $R^\times$.

■ **Beispiel 4.12**
- 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 4.13
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 $x' \in R^\times$. □

5. Körper

Definition 5.1 (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.

▶ **Bemerkung 5.2**
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.

▶ **Bemerkung 5.3**
Sei K ein Körper und $a, x, y \in K$. Ist $ax = ay$ und $a \neq 0$, so ist $x = y$.

Definition 5.4 (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.

■ **Beispiel 5.5**
- 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 5.6 (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:

- $(x_1, y_1) + (x_2, y_2) := (x_1 + x_2, y_1 + y_2)$
- $(x_1, y_1) \cdot (x_2, y_2) := (x_1 x_2 - y_1 y_2, x_1 y_2 + x_2 y_1)$

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 $(x_1, 0) \cdot (x_2, 0) = (x_1 x_2, 0)$, 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 5.7
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 5.8 (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.
- $1 \Rightarrow 2$: Satz 4.13
- $2 \Rightarrow 3$: Beispiel 4.12
- $3 \Rightarrow 1$: gegeben

Insbesondere ist $\mathbb{Z}/p\mathbb{Z}$ nullteilerfrei, d.h. aus $p|ab$ folgt $p|a$ oder $p|b$. □

6. Polynome

In diesem Abschnitt sei R ein kommutativer Ring mit Einselement.

▶ **Bemerkung 6.1**
Unter einem Polynom in der "Unbekannte" x versteht man einen Ausdruck der Form $f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n = \sum_{k=0}^{n} a_kx^k$ mit $a_0, ..., a_n \in R$. Fasst man x als ein beliebiges Element von R auf, gelten einige offensichtliche Rechenregeln:
Ist $f(x) = \sum_{k=0}^{n} a_kx^k$ und $g(x) = \sum_{k=0}^{n} b_kx^k$ so ist

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

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

Definition 6.2 (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 $c_k = \sum_{j=0}^{k} a_jb_{k-j}$

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 $f(X) = \sum_{k=0}^{n_0} a_kX^k$. Alternativ schreiben wir auch $f = \sum_{k\geq 0} a_kX^k$ mit dem Verständnis, dass diese unendliche Summe nur endlich von 0 verschiedene Summanden enthält.

Sei $0 \neq f(X) = \sum_{k\geq 0} a_kX^k \in R[X]$. 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 6.3**
Das lineare Polynom $f(X) = X - 2 \in R[X]$ hat den Leitkoeffizient 1 und den konstanten Term -2.

Satz 6.4
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 6.5 (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 6.6**
Der Existenzbeweis durch Induktion liefert uns ein konstruktives Verfahren, diese sogenannte Polynomdivision durchzuführen.

■ **Beispiel 6.7**
in $\mathbb{Q}[X]$: $(x^3 + x^2 + 1) : (x^2 + 1) = x + 1$ Rest $-x$

Definition 6.8 (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 6.9
Für $f, g \in \mathbb{R}[X]$ und $\lambda \in \mathbb{R}$i ist

$$(f+g)(\lambda) = f(\lambda) + g(\lambda)$$
$$(fg)(\lambda) = f(\lambda) \cdot g(\lambda)$$

Beweis. Ist $f = \sum_{k\geq 0} a_k X^k$ und $g = \sum_{k\geq 0} b_k X^k$, so ist

$$\begin{aligned} f(\lambda) + g(\lambda) &= \sum_{k\geq 0} a_k\lambda^k + \sum_{k\geq 0} b_k\lambda^k \\ &= \sum_{k\geq 0} (a_k + b_k)\lambda^k \\ &= (f+g)(\lambda) \end{aligned}$$

und

$$\begin{aligned} f(\lambda)\cdot g(\lambda) &= \sum_{k\geq 0} a_k\lambda^k \cdot \sum_{k\geq 0} b_k\lambda^k \\ &= \sum_{k\geq 0}\sum_{i+j=k} (a_i + b_j)\lambda^k \\ &= (fg)(\lambda) \end{aligned}$$

□

Satz 6.10
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. □

Folgerung 6.11
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. □

Folgerung 6.12
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 6.13**
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 6.14**
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 6.15
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 6.16 (algebraisch abgeschlossen)
Ein Körper K heißt algebraisch abgeschlossen, wenn er eine der äquivalenten Bedingungen erfüllt.

Theorem 6.17 (Fundamentalsatz der Algebra)
Der Körper $\mathbb{C}$ ist algebraisch abgeschlossen.

▶ **Bemerkung 6.18**
Wir werden das Theorem zwar benutzen, aber nicht beweisen.

Kapitel II

Vektorräume

1. Definition und Beispiele

2. Linearkombinationen

3. Basis und Dimension

4. Summen von VR

Kapitel III

Lineare Abbildungen

1. Matrizen

2. Homomorphismen von Gruppen

3. Homomorphismen von Ringen

4. Homomorphismen von VR

5. Der VR der linearen Abbildungen

6. Koordinatendarstellung linearer Abbildungen

7. Quotientenräume

8. Rang

9. Lineare Gleichungssysteme

Kapitel IV

Determinanten

1. Das Vorzeichen einer Permutation

2. Determinante einer Matrix

3. Minoren

4. Determinante und Spur von Endomorphismen

Anhang

Anhang A: Listen

A.1. Liste der Theoreme

A.2. Liste der benannten Sätze

Index