Kapitel I: Vorgeplänkel

1 Mengenlehre - die neue Mathematik (Mengen, Abbildungen und Beweise)

A. Was ist eine Menge?

1.1 anschauliche Definition (Georg Cantor, 1845-1918):

Eine Menge ist eine Zusammenfassung wohlunterscheidbarer Elemente zu einem Ganzen.

1.2 exakte Definition:

siehe Zermelo-Fraenkel-Axiomensystem
(Ernst Zermelo, 1907; Abraham Fraenkel, 1921 & 1930)
Schreibweise: $a \in M$ bedeute: "a ist Element der Menge M"

B. Wie kann man eine Menge beschreiben?

(a) explizite Aufzählung: $M_1 = \{2, 4, 6\}$
$M_2 = \{1, 3, 5, 7, \ldots\}$

(b) beschreibende Darstellung: $M_3 = \{a \in A \mid a \text{ hat Eigenschaft } E\}$
z.B. $M_4 = \{\underline{a} \in \mathbb{N} \mid \underline{a} \text{ ist ungerade}\} = M_2$
$2\,\mathbb{Z} = \{\underline{a} \in \mathbb{Z} \mid \underline{a} \text{ ist gerade }\}$
$= \{2\,\underline{a} \mid \underline{a} \in \mathbb{Z}\,\} = \{0, 2, -2, 4, -4, \ldots\}$

C. Welche besonderen Mengen gibt es?

(a) $\emptyset = \{\,\}$ (leere Menge)
(b) $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ (Menge der natürlichen Zahlen)
$\mathbb{N}_+ = \{1, 2, 3, \ldots\}$
(c) $\mathbb{Z} = \{0, 1, -1, 2, -2, \ldots\}$ (Menge der ganzen Zahlen)
(d) $\mathbb{Q} = \{\frac{a}{b} \mid \underline{a} \in \mathbb{Z}, \underline{b} \in \mathbb{N}_+\}$ (Menge der rationalen Zahlen)
(e) $\mathbb{R}$ (Menge der reellen Zahlen, ↗Analysis)
(f) $\mathbb{C} = \{\underline{a} + \underline{b}\mathrm{i} \mid \underline{a}, \underline{b} \in \mathbb{R}\}$ (Menge der komplexen Zahlen)

D. Was kann man mit Mengen so alles machen?

1.3 Definition:

Seien M_1, M_2 Mengen.

(a) $M_1 \cup M_2 = \{\underline{a} \mid \underline{a} \in M_1 \text{ oder } \underline{a} \in M_2 \text{ (oder beides)}\}$
Vereinigungsmenge von M_1 und M_2

(b) $M_1 \cap M_2 = \{\underline{a} \mid \underline{a} \in M_1 \text{ und } \underline{a} \in M_2\}$
Schnittmenge oder Durchschnitt von M_1 und M_2

(c) $M_1 \backslash M_2 = \{\underline{a} \mid \underline{a} \in M_1 \text{ und } \underline{a} \notin M_2\}$
Differenzmenge oder das Komplement von M_1 und M_2

(d) $M_1 \times M_2 = \{(\underline{a}, \underline{b}) \mid \underline{a} \in M_1, \underline{b} \in M_2\}$
Paarmenge oder das kartesische Produkt von M_1 und M_2
(nach Descartes, 1596-1650)

1.4 Bemerkung:

Durch wiederholte Anwendung der obigen Operationen definiert man für
$\underline{n} \in \mathbb{N}_+$ und Mengen $M_1, \ldots, M_n$ die folgenden Mengen:
$M_1 \cup \ldots \cup M_n = \{\underline{a} \mid \underline{a} \in M_i$ für ein $\underline{i} \in \{1, \ldots, n\}\}$
$M_1 \cap \ldots \cap M_n = \{\underline{a} \mid \underline{a} \in M_i$ für alle $\underline{i} \in \{1, \ldots, n\}\}$
$M_1 \times \ldots \times M_n = \{(a_1, \ldots, a_n) \mid a_i \in M_i$ für $\underline{i}$=1, …, n$\}$
($\rightarrow$ "$\underline{i}$=1, …, n"kurz für "für alle $\underline{i} \in \{1, \ldots, n\}$")
Die Elemente $(a_1, \ldots, a_n)$ von $M_1 \times \ldots \times M_n$ heißen n-Tupel.

1.5 Definition:

Besitzt eine Menge M nur endlich viele Elemente, so schreiben wir
$\#M$ für ihre Elementezahl oder Kardinalität.
Andernfalls schreiben wir $\#M = \infty$.

1.6 Satz:

Sei $\underline{n} \geq 2$ und M_1, M_2 endliche Mengen. Dann gilt:

(a) $\#(M_1 \cup M_2) = \#M_1 + \#M_2 - \#(M_1 \cap M_2)$ ("Summenformel")

(b) $\#(M_1 \times \ldots \times M_n) = (\#M_1) \cdot \ldots \cdot (\#M_n)$ ("Produktformel")

E. Was ist eine Abbildung?

1.7 Definition:

(a) Eine Abbildung $\underline{f}$: $M_1 \rightarrow M_2$ ist eine Vorschrift, die jedem Element $\underline{a} \in M_1$ genau ein Element $\underline{f}(\underline{a}) \in M_2$ zuordnet.

(b) Das Element $\underline{f}(\underline{a})$ heißt das Bild von $\underline{a}$ unter $\underline{f}$.

(c) Die Menge M_1 heißt der Definitionsbereich von $\underline{f}$.

(d) Die Menge M_2 heißt der Bildbereich von $\underline{f}$.

1.8 Beispiele:

(a) Die Zuordnung $\begin{array}{rcl} f : \{1,2,3\} & \rightarrow & \{1,2,3\} \\ 1 & \mapsto & 1 \\ 2 & \mapsto & 2 \\ 3 & \mapsto & 3 \end{array}$ ist eine Abbildung.

(b) Die Zuordnung $\begin{array}{rcl} g : \mathbb{R} & \rightarrow & \mathbb{R} \\ x & \mapsto & x^2 \end{array}$ ist eine Abbildung.

Abbildungen mit dem Bildbereich $\mathbb{R}$ heißen auch reelle Funktionen (↗Analysis).

1.9 Definition:

Sei M eine Menge. Die Abbildung $\begin{array}{rcl} id_M : M & \to & M \\ a & \mapsto & a \end{array}$ heißt die identische Abbildung oder die Identität auf M.

F. Welche Eigenschaften können Abbildungen besitzen?

1.10 Definition:

Seien M_1, M_2 Mengen und f: $M_1 \to M_2$ eine Abbildung.

(a) Die Abbildung f heißt injektiv, wenn keine zwei verschiedenen Elemente von M_1 auf das gleiche Element von M_2 abgebildet werden.

(b) Die Abbildung f heißt surjektiv, wenn jedes Element von M_2 Bild eines Elements aus M_1 ist.

(c) Die Abbildung f heißt bijektiv, wenn sie sowohl injektiv als auch surjektiv ist.

1.11 Beispiele:

(a) Die Abbildung $\begin{array}{rcl} f : \{1,2,3\} & \to & \{1,2\} \\ 1 & \mapsto & 1 \\ 2 & \mapsto & 1 \\ 3 & \mapsto & 2 \end{array}$ ist nicht injektiv aber surjektiv.

(b) Die Abbildung $\begin{array}{rcl} g : \mathbb{R} & \to & \mathbb{R} \\ x & \mapsto & x^3 \end{array}$ ist bijektiv.

(c) Sei $\mathbb{Q}_+ = \{ \frac{a}{b} \in \mathbb{Q} \mid a \in \mathbb{N}_+, b \in \mathbb{N}_+ \}$ die Menge der positiven rationalen Zahlen.
Die Abbildung $\begin{array}{rcl} h : \mathbb{Q}_+ & \to & \mathbb{Q}_+ \\ a & \mapsto & a^2 \end{array}$ ist injektiv aber nicht surjektiv.

1.12 Satz:

Seien M_1, M_2 endliche Mengen mit $\#M_1 = \#M_2$ und sei f: $M_1 \to M_2$ eine Abbildung. Dann sind die folgenden Bedingungen äquivalent:

(a) f ist injektiv.

(b) f ist surjektiv.

(c) f ist bijektiv.

G. Was kann man mit Abbildungen so alles machen?

Man kann Abbildungen komponieren.

1.13 Definition:

Seien M_1, M_2, M_3 Mengen und f: $M_1 \to M_2$ sowie g: $M_2 \to M_3$ Abbildungen.
Dann heißt die Abbildung $\begin{array}{rcl} f \circ g : M_1 & \to & M_3 \\ a & \mapsto & g(f(a)) \end{array}$ die Komposition von f nach g.

1.14 Beispiel:

Sei $\begin{array}{rcl} f : \{1,2\} & \to & \{1,2,3\} \\ 1 & \mapsto & 1 \\ 2 & \mapsto & 2 \end{array}$ die Inklusionsabbildung (d.h. $f(i) = i$, für alle i)

und $\begin{array}{rcl} g : \{1,2,3\} & \to & \{1,2\} \\ 1 & \mapsto & 1 \\ 2 & \mapsto & 2 \\ 3 & \mapsto & 1 \end{array}$ Dann gilt:

(a) $g \circ f = id_{\{1,2\}}$ und somit ist $g \circ f$ bijektiv.

(b) f ist injektiv, aber nicht surjektiv.

(c) g ist surjektiv, aber nicht injektiv.

1.15 Satz:

Seien M_1, M_2 Mengen und sei $f : M_1 \to M_2$ eine Abbildung.
Ist f bijektiv, so gibt es genau eine Abbildung $g : M_2 \to M_1$ mit $g \circ f = id_{M_1}$ und $f \circ g = id_{M_2}$.
Die Abbildung heißt die Inverse von f und wird mit f^{-1} bezeichnet.

H. Was ist Mathematik?

- „Schulmathematik“ ist eigentlich „Rechnen“ .
- Mathematik hat verschiedene Aufgaben:
  (a) Rechnen
  (b) Erforschung komplizierter Strukturen
  (c) Schaffung von „unumstößlichen“ Wissen („Beweisen“)
  (d) Konstruktion neuer Rechenverfahren („Algorithmen“), die schwierige Rechenprobleme effizient lösen
  (e) Klassifikation bestimmter Strukturen

Um diese Aufgaben erfüllen zu können brauchen mathematische Resultate einen Beweis.

I. Was ist ein Beweis?

- Eine (mathematische) Aussage ist ein sprachliches Gebilde, dass entweder wahr oder falsch ist.
- Ein mathematischer Satz enthält zwei Arten von Aussagen:
  Voraussetzungen und Behauptungen.
- Aus den Voraussetzungen sollen die Behauptungen nur die Anwendung der Gesetze der Logik hergeleitet werden. Sind die Voraussetzungen A und die Behauptungen B gegeben, so soll also die allgemeine Gültigkeit von $A \Rightarrow B$ bewiesen werden.

J. Wie kann man etwas beweisen?

Im Folgenden sei stets die Voraussetzung A und die Behauptung B gegeben.

1.16 Bemerkung: (der direkte Beweis)

Wir versuchen eine Schlusskette der Form $A \Rightarrow C_1, C_2 \Rightarrow C_3, \ldots, C_{n-2} \Rightarrow C_{n-1}, C_n \Rightarrow B$ zu bilden.
z.B. versuchen wir nur Satz 1.6.a zu beweisen:

Satz 1.6.a:

Seien M_1 und M_2 endliche Mengen.
Dann gilt $\#(M_1 \cup M_2) = (\#M_1) + (\#M_2) - \#(M_1 \cap M_2)$

Beweis: Wir betrachten 2 Fälle:

1. Fall: Die Vereinigung $M_1 \cup M_2$ sei disjunkt, d.h. es gelte $M_1 \cap M_2 = \emptyset$.
Jedes Element von $M_1 \cup M_2$ ist entweder Element von M_1 oder M_2 und wird daher bei der Berechnung von $\#M_1 + \#M_2$ genau einmal gezählt.

2. Fall: (allgemeiner Fall)
Notation: $N_1 \dot\cup N_2$ bedeute eine disjunkte Vereinigung.
Es gilt: $M_1 = (M_1 \backslash M_2) \dot\cup (M_1 \cap M_2)$
und ebenso: $M_2 = (M_2 \backslash M_1) \dot\cup (M_1 \cap M_2)$
Hieraus folgt: $M_1 \cup M_2 = (M_1 \backslash M_2) \dot\cup (M_2 \backslash M_1) \dot\cup (M_1 \cap M_2)$
Dies liefert mit Hilfe des 1. Falls die Gleichung:
$\#(M_1 \cup M_2) = \#(M_1 \backslash M_2) + \#(M_2 \backslash M_1) + \#(M_1 \cap M_2)$
Nun folgt: $\#(M_1 \cup M_2) = [\#M_1 - \#(M_1 \cap M_2)] + [\#M_2 - \#(M_1 \cap M_2)] + \#(M_1 \cap M_2)$
$= \#M_1 + \#M_2 - \#(M_1 \cap M_2)$. qed.

1.17 Bemerkung: (der indirekte Beweis / Beweis durch Kontraposition)

Wir nehmen an, die Behauptung B gelte nicht, d.h. es gelte $\neg B$. Dann suchen wir eine Schlusskette $\neg B \Rightarrow C_1, \ldots, C_n \Rightarrow \neg A$
Insgesamt beweisen wir also $\neg B \Rightarrow \neg A$.

Wir beweisen nun:

1.12 Satz:

Seien M_1, M_2 endliche Mengen mit $\#M_1 = \#M_2$ und sei f: $M_1 \to M_2$ eine Abbildung. Dann sind die folgenden Bedingungen äquivalent:

(a) f ist injektiv.

(b) f ist surjektiv.

(c) f ist bijektiv.

Beweis: Wir zeigen „a.) ⇒ b.)“ , „b.) ⇒ c.)“ , „c.) ⇒ a.)“ (Ringschluss)

„a.) ⇒ b.)“ (direkter Beweis): Sei $M_1 = \{a_1, \ldots, a_n\}$ mit $n = \#M_1$
Die Menge $Bild(f) = \{f(a_1), \ldots, f(a_n)\}$ besitzt paarweise verschiedene Elemente, denn f ist injektiv.
Wegen $Bild(f) \subseteq M_2$ und $\#Bild(f) = \#M_2 = \#M_1 = n$ folgt somit $Bild(f) = M_2$.
Also ist f surjektiv.

„b.) ⇒ c.)“ (indirekter Beweis) Es genügt zu zeigen, dass f injektiv ist.
Angenommen f ist nicht injektiv.
Schreibe wieder $M_1 = \{a_1, \ldots, a_n\}$ mit $n = \#M_1$.
O.B.d.A seien die Elemente von M_2 so numeriert, dass $f(a_1) = f(a_2)$ gelte.
Dann folgt $Bild(f) = \{f(a_2), \ldots, f(a_n)\}$ und daher $\#Bild(f) < n = \#M_2 \lightning$.
Also ist f nicht surjektiv.

„c.) ⇒ a.)“ Trivial. qed.

1.18 Bemerkung: (der Widerspruchsbeweis)

Wir argumentieren folgendermaßen: Wir nehmen an, dass $\neg B$ wahr ist und suchen dann eine Schlusskette $\neg B \Rightarrow C_1, \ldots, C_{n-1} \Rightarrow C_n$, so dass C_n offensichtlich falsch ist („Widerspruch“ $\lightning$).
Wir beweisen nun:

1.15. Satz:

Seien M_1, M_2 Mengen und sei $f : M_1 \to M_2$ eine Abbildung.
Ist f bijektiv, so gibt es genau eine Abbildung $g : M_2 \to M_1$ mit $g \circ f = id_{M_1}$ und $f \circ g = id_{M_2}$.
Die Abbildung heißt die Inverse von f und wird mit f^{-1} bezeichnet.

Beweis: „Existenz“ : Sei $b \in M_2$. Da f surjektiv ist, gibt es ein $a \in M_1$ mit $f(a) = b$.
Setze $f^{-1}(b) = a$. Dies ist wohldefiniert (d.h. die Definition von $f^{-1}(b)$ hängt nicht von der Wahl von a ab), denn das Element a ist eindeutig bestimmt, da f injektiv ist.
Man prüft leicht nach, dass die so definierte Abbildung $f^{-1} : M_2 \to M_1$ damit tatsächlich invers zu f ist.
[Sei $a \in M_1$ und $b = f(a)$. Dann gilt $(f^{-1} \circ f)(a) = f^{-1}(f(a)) = f^{-1}(b) = a$
(nach Definition von f^{-1}).
Da $a \in M_1$ beliebig war, folgt $f^{-1} \circ f = id_{M_1}$.
Sei nun $b \in M_2$ und $a \in M_1$ das Element mit $b = f(a)$.
Dann gilt $(f \circ f^{-1})(b) = f(f^{-1}(a)) = b$.
Da $b \in M_2$ beliebig war, folgt $f \circ f^{-1} = id_{M_2}$]
“ Eindeutigkeit“ [Widerspruchsbeweis] Angenommen es gibt zwei verschiedene Abbildungen $f : M_2 \to M_1$ und $\tilde{g} : M_2 \to M_1$ die zu f invers sind. Sei $b \in M_2$ mit $g(b) \neq \tilde{g}(b)$.
Sei $a \in M_1$ das Element mit $f(a) = b$. Dann gilt:
$g(b) = (g \circ f)(a) = (\tilde{g} \circ f)(a) = \tilde{g}(b) \lightning$ qed.

1.19 Bemerkung: (Beweis durch vollständige Induktion)

Die Behauptung B hänge von einer Zahl $n \in \mathbb{N}_+$ ab, d.h. sie sei von der Form: „für alle $n \in \mathbb{N}_+$ gilt $B(n)$“
Prinzip der vollständigen Induktion:

1.) Es gilt $B(1)$
2.) Es gilt $B(n) \Rightarrow B(n+1)$
Wir beweisen nun:

1.6.b Satz:

Für $n \geq 1$ und endliche Mengen $M_1, \ldots, M_n$ gilt:
$\#(M_1 \times \ldots \times M_n) = (\#M_1) \cdot \ldots \cdot (\#M_n)$ ("Produktformel")

Beweis: Wir schließen nun durch vollständige Induktion nach n.

$n = 1$: (Induktionsanfang) $\#M_1 = \#M_1 (\surd)$

$n \to n+1$: (Induktionsschluss) Ein $(n+1)$-Tupel $(a_1, \ldots, a_{n+1}) \in M_1 \times \ldots \times M_{n+1}$ ist eindeutig festgelegt durch das n-Tupel $(a_1, \ldots, a_n) \in M_1 \times \ldots \times M_n$ und das Element $a_{n+1} \in M_{n+1}$.
Verschiedene n-Tupel $(a_1, \ldots, a_n)$ bzw. verschiedene Elemente $a_{n+1} \in M_{n+1}$ liefern dabei $(n+1)$-Tupel $(a_1, \ldots, a_{n+1})$.
Dies zeigt $\#(M_1 \times \ldots \times M_{n+1}) = (\#M_1 \times \ldots \times \#M_n) \cdot (\#M_{n+1})$
Nach Induktionsvoraussetzung gilt: $\#(M_1 \times \ldots \times M_n) = (\#M_1) \cdot \ldots \cdot (\#M_n)$.
Nun ergibt sich: $\#(M_1 \times \ldots \times M_{n+1}) = (\#M_1 \times \ldots \times \#M_n) \cdot (\#M_{n+1})$
$= (\#M_1) \cdot \ldots \cdot (\#M_n) \cdot (\#M_{n+1})$. qed.

2 Unsere lieben Zahlen (Gruppen, Ringe und Körper)

Welche Zahlen gibt es überhaupt?

$\mathbb{N}$, $\mathbb{N}_+$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, ... (vgl. §1)

Was kann mit mit Zahlen so alles machen?

Man kann Zahlen addieren und subtrahieren.
Die zu Grunde liegenden mathematischen Strukturen sind wie folgt definiert:

2.1 Definition:

Sei G eine Menge.

(a) Eine Verknüpfung auf G ist eine Abbildung $\begin{array}{rcl} \circ : G \times G & \to & G \\ (a,b) & \mapsto & a \circ b \end{array}$

(b) Sei $\circ$ eine Verknüpfung auf G. Gilt das Assoziativgesetz $(a \circ b) \circ c = a \circ (b \circ c)$ für alle $a, b, c \in G$ so heißt $(G, \circ)$ eine Halbgruppe.

(c) Ist $(G, \circ)$ eine Halbgruppe und gibt es in G ein neutrales Element $e \in G$, d.h. ein Element mit $e \circ a = a \circ e = a$ für alle $a \in G$, so heißt $(G, \circ)$ ein Monoid.

(d) Ist $(G, \circ)$ ein Monoid und gibt es in G inverse Elemente, d.h. zu jedem $a \in G$ gibt es ein $b \in G$ mit $a \circ b = b \circ a = e$, so heißt $(G, \circ)$ eine Gruppe.

(e) Ist $(G, \circ)$ eine Gruppe und gilt das Kommutativgesetz $a \circ b = b \circ a$ für alle $a, b \in G$, so heißt $(G, \circ)$ eine kommutative Gruppe (oder abelsche Gruppe).
In diesem Fall schreiben wir 0 statt e und $-a$ für das inverse Element von a.

2.2 Beispiele:

(a) $(\mathbb{Z}, +)$ ist eine kommutative Gruppe

(b) $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ sind kommutative Gruppen

(c) $(\mathbb{Q}\backslash\{0\}, \cdot)$ ist eine kommutative Gruppe

2.3 Definition:

Sei $(R, +)$ eine kommutative Gruppe.

(a) Es gebe auf R eine weitere Verknüpfung $\begin{array}{rcl} \cdot : R \times R & \to & R \\ (a,b) & \mapsto & a \cdot b \end{array}$ genannt Multiplikation, so dass gilt:

1.) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ für alle $a, b, c \in R$ (Assoziativität).

2.) Es gibt ein Element $1 \in R$ mit $1 \cdot a = a \cdot 1 = a$ für alle $a \in R$.

3.) Für alle $a, b, c \in R$ gilt:
$a \cdot (b + c) = a \cdot b + a \cdot c$
$(a + b) \cdot c = a \cdot c + b \cdot c$ (Distributivgesetze)

Dann heißt R ein Ring.

(b) Ist $(R, +, \cdot)$ ein Ring und gilt das Kommutativgesetz $a \cdot b = b \cdot a$ für alle $a, b \in R$, so heißt R ein kommutativer Ring (mit Einselement).

(c) Ist R ein kommutativer Ring mit $1 \neq 0$ und gibt es zu jedem Element $a \in R \backslash \{0\}$ ein $b \in R$ mit $a \cdot b = 1$, so heißt R ein Körper (engl. „field“).

2.4 Beispiele:

(a) $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring

(b) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind Körper

C. Gibt es noch weitere Körper?

Ja, es gibt sogar Körper mit nur endlich vielen Elementen.
Im Folgenden wollen wir einige solche endliche Körper konstruieren und untersuchen.

2.5 Satz: (Division mit Rest für ganze Zahlen)

Sei $a \in \mathbb{Z}$ und $b \in \mathbb{N}_+$. Dann gibt es eindeutig bestimmte Zahlen $q, r \in \mathbb{Z}$ mit $a = q \cdot b + r$ und $0 \leq r < b$ (q ist der Quotient, r ist der Rest).

Beweis: später

2.6 Definition:

Sei $a \in \mathbb{Z}$ und $b \in \mathbb{N}_+$.

(a) Für den Rest r in der Darstellung $a = q \cdot b + r$ gemäß Satz 2.5 schreiben wir auch $a(mod\ b)$ und nennen ihn den „Rest von *a modulo b*“ oder einfach „*a modulo b*“ .

(b) Sei $a, b \in \mathbb{Z}$ und $c \in \mathbb{N}_+$. Sind die Reste $a(mod\ c)$ und $b(mod\ c)$ gleich, so heißen a und b *kongruent modulo c* und wir schreiben $a \equiv b(mod\ c)$.

2.7 Beispiele:

(a) $3 \equiv 18(mod\ 5)$

(b) $17 \equiv 27(mod\ 10)$

2.8 Bemerkung: (Rechnen mit Resten)

Nun sei $n \geq 2$. Wir bezeichnen die Reste *modulo n* auch mit $\overline{1}, \overline{2}, \ldots, \overline{n-1}$.
Die Menge dieser Reste bezeichnen wir mit $\mathbb{Z}/n\mathbb{Z} = \{\overline{1}, \overline{2}, \ldots, \overline{n-1}\}$ („$\mathbb{Z}$ *modulo* $n\mathbb{Z}$“)

2.9 Satz: (Der Ring $\mathbb{Z}/n\mathbb{Z}$)

(a) Die Abbildungen $+ : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $(\overline{a}, \overline{b}) \mapsto (a+b)(mod\ n) = \overline{a+b}$
und $\cdot : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $(\overline{a}, \overline{b}) \mapsto (a \cdot b)(mod\ n) = \overline{a \cdot b}$ sind wohldefiniert.

(b) Durch diese Definitionen wird die Menge der Reste $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ zu einem kommutativen Ring.

Beweis: (2.9.a)

Das Ergebnis $\overline{a+b}$ soll unabhängig von der Wahl von a und b sein.
Dazu seien $a_1, a_2 \in \mathbb{Z}$ mit $\overline{a_1} = \overline{a_2}$ (also $a_1 \equiv a_2(mod\ n)$) und $b_1, b_2 \in \mathbb{Z}$ mit $\overline{b_1} = \overline{b_2}$.
Dann gibt es $c_1, c_2 \in \mathbb{Z}$ mit $a_1 - a_2 = c_1 \cdot n$ und $b_1 - b_2 = c_2 \cdot n$.
Hieraus folgt: $(a_1 + b_1) - (a_2 + b_2) = (c_1 + c_2) \cdot n$, also $a_1 + b_1 \equiv a_2 + b_2(mod\ n)$.
Somit ist die +-Verknüpfung wohldefiniert.
Der Beweis der Wohldefiniertheit von $\cdot$ verläuft analog.

Beweis: (2.9.b)

Man kann alle Axiome leicht nachrechnen, z.B. gilt:
$(\overline{a} + \overline{b}) + \overline{c} = (a+b)(mod\ n) + \overline{c} = ((a+b)(mod\ n) + c)(mod\ n) = (a+b+c)(mod\ n)$.
denn: $a + b = q_1 \cdot n + r_1$ und $c = q_2 \cdot n + r_2$ liefert
$(a+b)(mod\ n) + c(mod\ n) = (r_1 + c)(mod\ n) = (r_1 + r_2)(mod\ n)$.
$a + b + c = (q_1 + q_2)n + \underbrace{q_3 n + (r_1 + r_2)(mod\ n)}_{= r_1 + r_2}$ zeigt $(a+b+c)(mod\ n) = (r_1 + r_2)(mod\ n)$
$\overline{a} + (\overline{b} + \overline{c}) = \ldots = (a+b+c)(mod\ n)$ folgt ebenso. qed.

2.10 Beispiel:

Für den Ring $\mathbb{Z}/4\mathbb{Z}$ gilt:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{1}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Hier erkennt man, dass $\mathbb{Z}/4\mathbb{Z}$ kein Körper ist, denn es gibt kein $\overline{a} \in \mathbb{Z}/4\mathbb{Z}$ mit $\overline{2a} = \overline{1}$.
Gäbe es $(\overline{2})^{-1}$, so wäre $\overline{0} = \overline{0} \cdot (\overline{2})^{-1} \cdot (\overline{2})^{-1} = \overline{2} \cdot (\overline{2})^{-1} \cdot \overline{2} \cdot (\overline{2})^{-1} = \overline{1} \cdot \overline{1} = \overline{1}$ ↯
In einem Körper darf für Elemente $a, b \neq 0$ niemals $a \cdot b = 0$ gelten!

2.11 Satz:

Der Ring $\mathbb{Z}/n\mathbb{Z}$ ist genau dann ein Körper, wenn n eine Primzahl ist.
Schreibweise: p sei eine Primzahl. Dann heißt $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ der Körper mit p Elementen. ($\mathbb{F}$ für „field“).

Beweis: „⇒“ Angenommen, n ist keine Primzahl. Sei also $n = k \cdot l$ mit $k, l \geq 2$. Dann gilt in $\mathbb{Z}/n\mathbb{Z}$ die Gleichung $\overline{k} \cdot \overline{l} = \overline{0}$ und es ist $\overline{k} \neq \overline{0}, \overline{l} \neq \overline{0}$. Wie in Beispiel 2.10 liefert dies den Widerspruch $\overline{0} = \overline{1}$.

„⇐“ Zu zeigen ist, dass ein beliebiges Element $\overline{a} \in (\mathbb{Z}/n\mathbb{Z}) \backslash \{\overline{0}\}$ ein multiplikatives Inverses besitzt.
Die Multiplikation $\mu_{\overline{a}} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ ist injektiv, denn:

$$\overline{b} \mapsto \overline{a \cdot b}$$

1.) Aus $\overline{a \cdot b} = 0$ folgt $\overline{a} = 0$ oder $\overline{b} = 0$, denn wenn eine Primzahl n das Produkt ab teilt, muss sie einen der Faktoren a oder b teilen.
Wegen $\overline{a} \neq 0$ muss dann $\overline{b} = 0$ sein.

2.) Gilt nun $\overline{a \cdot b_1} = \overline{a \cdot b_2}$ so folgt $\overline{a}(\overline{b_1} - \overline{b_2}) = \overline{0}$, also $\overline{b_1} - \overline{b_2} = 0$, also $\overline{b_1} = \overline{b_2}$.
Damit ist $\mu_{\overline{a}}$ injektiv.

Da $\mu_{\overline{a}}$ injektiv ist, zeigt Satz 1.15, dass $\mu_{\overline{a}}$ bijektiv ist.
Somit gibt es ein $\overline{b} \in \mathbb{Z}/n\mathbb{Z}$ mit $\overline{a \cdot b} = \overline{1}$. qed.

2.12 Beispiel:

Wir berechnen das Inverse zu $\overline{5} \in \mathbb{F}_{11}$.

Gesucht ist also eine Restklasse $\overline{a} \in \{\overline{0}, \ldots, \overline{10}\}$ mit $\overline{5 \cdot a} = \overline{1}$.
Also brauchen wir eine Zahl $a \in \{0, 1, \ldots, 10\}$ so dass es ein $b \in \mathbb{Z}$ gibt mit $5 \cdot a - 1 = b \cdot 11$.

1.) Raten / Probieren:

$\overline{a}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\ldots$	$\overline{9}$
$\overline{5a}$	$\overline{0}$	$\overline{5}$	$\overline{10}$	$\overline{4}$	$\ldots$	$\overline{1}$

Also gilt $a = 9$ und $\overline{5 \cdot 9} = \overline{1}$.

2.) Der erweiterte euklidische Algorithmus berechnet a, b mit $5a - 11b = 1$ (vgl. später).

3 m lineare Gleichungen in n Unbestimmten

A. Was ist ein lineares Gleichungssystem?

Im Folgenden sei K ein Körper.

3.1 Definition:

Seien $m, n \in \mathbb{N}_+$ und $a_{ij} \in K$ für $i = 1, \ldots, m$ und $j = 1, \ldots, n$. Weiter seien $b_1, \ldots, b_n \in K$.

(a) Ein lineares Gleichungssystem (LGS) über K bestehend aus m Gleichungen in n Unbestimmten ist ein System der Form:

$$(*) \begin{cases} a_{11}x_1 + a_{21}x_2 + \ldots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = b_2 \\ \vdots \qquad\quad \vdots \qquad\qquad\quad \vdots = \vdots \\ a_{m1}x_1 + a_{22}x_2 + \ldots + a_{mn}x_n = b_m \end{cases}$$

(b) Die Lösungsmenge des LGS ist die Menge
$\mathbb{L} = \{(c_1, \ldots, c_n) \in K^n \mid a_{i1}c_1 + a_{i2}c_2 + \ldots + a_{in}c_n = b_i \text{ für } i = 1, \ldots, n\}$
($K^n = K \times K \times \ldots \times K$ (n-mal))

Fragen:

- Wie kann man die Lösungsmenge eines LGS bestimmen?
- Welche Gestalt besitzt die Lösungsmenge?
- Welche Anwendungen besitzt das Lösen von LGS

3.2 Beispiel:

Gegeben sei folgendes LGS:

$$\begin{cases} 3x - y = 1 \\ 6x - 2y = 3 \end{cases} \text{ über dem Körper } \mathbb{Q}$$

Notation: Statt x_1, x_2 schreiben wir oft auf x, y (im Fall $n = 2$).
Statt x_1, x_2, x_3 schreiben wir oft auf x, y, z (im Fall $n = 3$).

1.) Dividieren der zweiten Gleichung durch 2 liefert:

$$\begin{cases} 3x - y = 1 \\ 3x - y = \frac{3}{2} \end{cases} \text{ Hieraus erkennt man } \mathbb{L} = \emptyset$$

Ein LGS mit $\mathbb{L} = \emptyset$ heißt unlösbar oder inkonsistent.

3.3 Beispiel:

Gegeben sei folgendes LGS:

$$\begin{cases} 3x - \sqrt{2}y = 0 \\ \sqrt{3}x + 2y = 0 \end{cases} \text{ über dem Körper } \mathbb{R}$$

1.) Multipliziere die zweite Gleichung mit $\sqrt{3}$

$$\begin{cases} 3x - \sqrt{2}y = 0 \\ 3x + 2\sqrt{3}y = 0 \end{cases}$$

2.) Subtrahiere die erste Gleichung von der zweiten.

$$\begin{cases} 3x - \sqrt{2}y = 0 \\ (2\sqrt{3}+\sqrt{2})y = 0 \end{cases}$$

3.) Dividiere die zweite Gleichung durch $(2\sqrt{3}+\sqrt{2})$.

$$\begin{cases} 3x - \sqrt{2}y = 0 \\ y = 0 \end{cases}$$

4.) Setze dies in die erste Gleichung ein.

$$\begin{cases} 3x = 0 \\ y = 0 \end{cases}$$

5.) Dividiere die erste Gleichung durch 3.

$$\begin{cases} x = 0 \\ y = 0 \end{cases} \Rightarrow \mathbb{L} = \{(0,0)\}$$

Ein LGS mit $b_1 = \ldots = b_m = 0$ heißt ein homogenes LGS. Ein homogenes LGS besitzt immer mindestens die Lösung $(0, 0, \ldots, 0)$.

3.4 Beispiel:

Gegeben sei folgendes LGS:

$\{4x + 3y = 1$ über dem Körper $\mathbb{Q}$
Man kann für x einen belieben Wert aus $\mathbb{Q}$ wählen und nach y auflösen.
Setze also $x = c \in \mathbb{Q}$ und rechne:
$4c + 3y = 1 \Rightarrow 3y = 1 - 4c \Rightarrow y = \frac{1}{3} - \frac{4}{3}c$
Also ergibt sich: $\mathbb{L} = \{(c, \frac{1}{3} - \frac{4}{3}c) \mid c \in \mathbb{R}\}$
Ein LGS kann somit unendlich viele Lösungen besitzen.
Die Lösungsmenge besitzt (hier) eine Parameterdarstellung oder Parametisierung.

3.5 Beispiel:

Gegeben sei folgendes LGS:

$$\begin{cases} \overline{2}x + \overline{3}y = \overline{1} \\ x + \overline{4}y = \overline{3} \end{cases}$$ über dem Körper $\mathbb{F}_5$.

1.) Multipliziere die zweite Gleichung mit $\overline{2}$

$$\begin{cases} \overline{2}x + \overline{3}y = \overline{1} \\ \overline{2}x + \overline{3}y = \overline{1} \end{cases}$$

2.) Wir subtrahieren die erste Gleichung von der zweiten.

$$\begin{cases} \overline{2}x + \overline{3}y = \overline{1} \\ \qquad\quad \overline{0} = \overline{0} \end{cases}$$

3.) Setze $x = c \in \mathbb{F}_5$ und berechne:
$\overline{3}y = \overline{1} - \overline{2}c = \overline{1} + \overline{3}c$ also $y = \overline{2} + c$
$\Rightarrow$ Insgesamt erhalten wir $\mathbb{L} = \{(c, \overline{2} + c) \mid c \in \mathbb{F}_5\}$

B. Wie kann man ein LGS systematisch lösen?

3.6 Bemerkung:

Es gibt folgende elementare Gleichungsumformungen:

Typ P: Vertauschen von zwei Gleichugen
Typ D: Multiplikation einer Gleichung mit einer Zahl $d \in K\backslash\{0\}$
Typ E: Addition eines Vielfachen einer Gleichung zu einer anderen

3.7 Satz:

Gegeben sei das LGS $(*)$

Eine elementare Gleichungsumformungen ändert die Lösungsmenge nicht.

Beweis:

Typ P: klar.

Typ D: Sei $d \in K\backslash\{0\}$ und sei $a_{i1}x_1 + \ldots + a_{in}x_n = b_i$ die zu multiplizierende Gleichung.
Sei $(c_1, \ldots, c_n) \in K^n$ mit $a_{i1}c_1 + \ldots + a_{in}c_n = b_i$. Dann gilt auch $da_{i1}c_1 + \ldots + da_{in}c_n = db_i$
Somit erfüllt $(c_1, \ldots, c_n)$ auch die Gleichung $da_{i1}c_1x_1 + \ldots + da_{in}c_nx_n = db_i$.
Sei umgekehrt $(c_1, \ldots, c_n) \in K^n$ mit $da_{i1}c_1 + \ldots + da_{in}c_n = db_i$.
Dann folgt durch Multiplikation mit d^{-1}, dass auch $a_{i1}c_1 + \ldots + a_{in}c_n = b_i$ gilt.
Also ist $(c_1, \ldots, c_n)$ auch eine Lösung von $a_{i1}x_1 + \ldots + a_{in}x_n = b_i$.

Typ E: Dies prüft man entsprechend nach. qed.

3.8 Definiton:

Ein LGS $(*)$ ist in Zeilenstufenform, wenn gilt:

(a) Gleichungen $0 = 0$ stehen in den untersten Zeilen des LGS.

(b) Ist eine Gleichung ungleich $0 = 0$, so ist sie entweder $0 = 1$ oder von der Form $a_{i1}x_1 + \ldots + a_{in}x_n = b_i$, wobei das erste $a_{ij} \neq 0$ die Bedingung $a_{ij} = 1$ erfüllt. [Dieses a_{ij} heißt Leitkoeffizient oder Pirotelement]

(c) Kommt eine Gleichung $0 = 1$ vor, so steht sie unter den Gleichungen $0 = 0$ ganz unten.

(d) Sind zwei untereinander stehende Gleichungen ungleich $0 = 0$ und $0 = 1$, so steht der Leitkoeffizient der unteren Gleichung weiter rechts als der der oberen , d.h. bei einem x_j mit größerem j.

3.9 Beispiel:

Betrachte das LGS

$$(**)\quad \begin{cases} x + y - z = 0 \\ x - y + z = 0 \\ -x + y + z = 0 \end{cases} \text{ über dem Körper } \mathbb{Q}$$

1.) Subtrahiere die erste Gleichung von der zweiten und addiere sie dann zu dritten.

$$\begin{cases} x + y - z = 0 \\ -2y + 2z = 0 \\ 2y = 0 \end{cases}$$

2.) Addiere die zweite Gleichung zur dritten und normiere beide (d.h. multipliziere beide so, dass der Leitkoeffizient 1 wird).

$$\begin{cases} x + y - z = 0 \\ y - z = 0 \\ z = 0 \end{cases}$$

Den nächsten Schritt nennt man Ausräumen.

3.10 Definition:

Ein LGS befinde sich in Zeilenstufenform.
Wir sagen, es sei in reduzierter Zeilenstufenform wenn jeder Leitterm, d.h. jede führende Variable x_j genau einmal im ganzen LGS vorkommt.

3.11 Beispiel:

Wir überführen das LGS $(**)$ in reduzierter Zeilenstufenform.

1.) Addiere die dritte Gleichung zur ersten und zur zweiten.

$$\begin{cases} x + y = 0 \\ y = 0 \\ z = 0 \end{cases}$$

2.) Subtrahiere die zweite Gleichung von der ersten.

$$\begin{cases} x = 0 \\ y = 0 \\ z = 0 \end{cases} \text{ Offensichtlich folgt } \mathbb{L} = \{(0,0,0)\}$$

3.12 Satz: (das Gaußsche Eliminationsverfahren (Carl-Friedrich Gauß, 1777-1855))

Gegeben sei das LGS $(*)$. Betrachte die folgenden Instruktionen/Schritte:

(a) Finde eine Gleichung in der die Unbestimmte x_j mit dem kleinsten j vorkommt. Vertausche die Gleichung so, dass dies die erste Gleichung ist.

(b) Ist der Koeffizient a_{ij} von x_j in der ersten Gleichung ungleich 1, so teile die erste Gleichung durch a_{ij}.

(c) Addiere passende Vielfache der ersten Gleichung zu den darunter stehenden Gleichungen, so dass der Koeffizient von x_j dort überall verschwindet.

(d) Wende die Schritte a) bis c) auf die Gleichungen 2 bis m an und wiederhole dieses Verfahren, solange bis das LGS in Zeilenstufenform ist.

Dies ist ein Algorithmus, der das LGS $(*)$ in Zeilenstufenform überführt, ohne die Lösungsmenge zu verändern.

Beweis: *Endlichkeit: ... Korrektheit: ...*

3.13 Korollar: (Das Gauß-Jordan Verfahren)

Sei das LGS $(*)$ gegeben. Führe das Gauß-Verfahren (3.12) durch und schließe folgenden Schritt an: Beginnend mit der letzten von 0=0 verschiedenen Gleichung: Addiere geeignete Vielfache jeder Gleichung j zu den darüber stehenden Gleichungen um die Koeffizienten des Leitterms von Gleichung j in den darüber stehenden Gleichungen zu eliminieren („Ausräumen“).

Dies ist eine Algorithmus, der das LGS $(*)$ in ein LGS überführt, dass sich in reduzierter Zeilenstufenform befindet, ohne die Lösungsmenge zu verändern.

3.14 Beispiel:

Gegeben sei das LGS

$$\begin{cases} x + y + 2z = 9 \\ 2x + 4y - 3z = 1 \\ 3x + 6y - 5z = 1 \end{cases} \text{ über dem Körper } \mathbb{Q}$$

(a) Gauß-Verfahren:
(c) $(-2)\cdot$I + II und $(-3)\cdot$I + III

$$\begin{cases} x + y + 2z = 9 \\ 2y - 7z = -17 \\ 3y - 11z = -26 \end{cases}$$

(b) $\frac{1}{2}\cdot$II

$$\begin{cases} x + y + 2z = 9 \\ y - \frac{7}{2}z = -\frac{17}{2} \\ 3y - 11z = -26 \end{cases}$$

(c) $(-3)\cdot$II + III

$$\begin{cases} x + y + 2z = 9 \\ \quad y - \frac{7}{2}z = -\frac{17}{2} \\ \quad\quad - \frac{1}{2}z = -\frac{1}{2} \end{cases}$$

(b) $(-2)\cdot$III

$$\begin{cases} x + y + 2z = 9 \\ \quad y - \frac{7}{2}z = -\frac{17}{2} \\ \quad\quad z = 1 \end{cases}$$

Dieses LGS ist in Zeilenstufenform. Rücksubstitution liefert:
$z = 1, y = -5, x = 12$, also die Lösungsmenge: $\mathbb{L} = \{(12, -5, 1)\}$

(b) Gauß-Jordan-Verfahren:

(e) $\frac{7}{2}\cdot$III + II und $(-2)\cdot$III + I

$$\begin{cases} x + y = 7 \\ \quad y = -5 \\ \quad\quad z = 1 \end{cases}$$

(e) $(-1)\cdot$II + I

$$\begin{cases} x = 12 \\ \quad y = -5 \\ \quad\quad z = 1 \end{cases}$$

Wieder folgt: $\mathbb{L} = \{(12, -5, 1)\}$

C. Was nützt uns die reduzierte Zeilenstufenform eines LGS?

3.15 Bemerkung:

Sei das LGS $(*)$ gegeben. Man kann die reduzierte Zeilenstufenform wie folgt mit CoCoA berechnen:

(a) Wechsle in den korrekten Grundring, z.b.:
Use S::=Q[x[1..5]]; (die Unbestimmten sind x[1]. . .x[5])
oder: Use T::=Z/(101)[x,y,z];

(b) Definiere Polynome, die die Gleichungen repräsentieren, wobei der konstante Term b_i auf die linke Seite gebracht wurde. z.B.:
F1:=x+y+2z-9;
F2:=2x+4y-3z-1;
F3:=3x+6y-5z-1;

(c) Definiere das Polynomideal aus F1, F2, F3:
I:=Ideal(F1,F2,F3);

(d) Berechne die Gleichungen der reduzierten Zeilenstufenform mit:
ReducedGBasis(I);

3.16 Satz: (Ablesen der Lösungsmenge aus der reduzierten Zeilenstufenform)

Sei das LGS $(*)$ gegeben und sei

$$(**)\begin{cases} x_{i1} & \dots & 0 & \dots & 0 & + & c_{1l}x_l & + & \dots & + & c_{1n}x_n & = & d1 \\ 0 & & x_{i2} & \dots & 0 & + & c_{2l}x_l & + & \dots & + & c_{2n}x_n & = & d2 \\ \vdots & & \vdots & \ddots & \vdots & & \vdots & & & & \vdots & & \vdots \\ 0 & \dots & 0 & \dots & x_{ik} & + & c_{kl}x_l & + & \dots & + & c_{kn}x_n & = & d_k \\ 0 & \dots & 0 & \dots & 0 & & 0 & & \dots & & 0 & = & 0 \end{cases}$$

mit Indizes $1 \le i_1 < i_2 < \ldots < i_k \le n$ und $l = i_k + 1$ und $c_{ij}, d_m \in K$.

Dann kann man die Lösungsmenge von (*) wie folgt parametisieren:
$\mathbb{L} = \{(e_1, \ldots, e_n) \in K^n \mid e_j \in K$ beliebig für $j \notin \{i_1, \ldots, i_k\}$
und $e_j = d_\mu - c_{\mu l}e_l - \ldots - c_{\mu n}e_n$ für $j = i_\mu \in \{i_1, \ldots, i_k\}\}$

Beweis:
„$\supseteq$“ Durch Einsetzen in $(**)$ prüft man leicht nach, dass die angegebenen Tupel tatsächlich das LGS $(**)$ lösen.

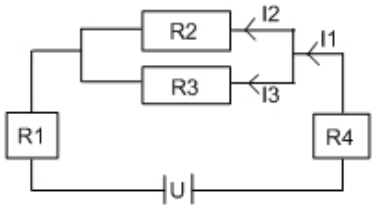
„$\subseteq$“ Umgekehrt erfüllt jede Lösung von$(**)$ wegen der ersten k Gleichungen auch die Bedingungen $e_j = d_\mu - c_{\mu l}e_l - \ldots - c_{\mu n}e_n$ für $j = i_\mu$. Somit ist die rechte Seite die Lösungsmenge von $(**)$. Nach Satz 3.7 ist sie auch die Lösungsmenge von $(*)$. qed.

D. Welche Anwendungen besitzt das Lösen von LGS?

(a) Graphentheorie / Logik (vgl. Blatt 2 / Aufg. 4)

(b) Computertomographie (vgl. Blatt 3 / Aufg. 1)

3.17 Beispiel: (Elektrische Schaltkreise)



Die Widerstände R_1, R_2, R_3, R_4 seien gegeben.
Zeige: Die fließenden Ströme I_1, I_2, I_3 sind proportional zur angelegten Spannung U.
Man bestimme die Proportionskonstante.

Ohmsches Gesetz: $U = R \cdot I$

1. Kirchhoffsches Gesetz: An jedem Knoten ist die Summe der zu- und abfließenden Ströme gleich Null.

2. Kirchhoffsches Gesetz: In jedem Kreis ist die Summe der Spannungen gleich Null.

Hier ergibt sich:

$$\begin{cases} I_1 - I_2 - I_3 = 0 \\ R_2I_2 - R_3I_3 = 0 \\ (R_1 + R_4)I_1 + R_2I_2 = 0 \end{cases}$$

Hier ergibt sich ein LGS über $\mathbb{R}$ für die Unbestimmten I_1, I_2, I_3.

Es ergibt sich ein Lösungstupel der Form:
$I_1 = c_1 \cdot U$
$I_2 = c_2 \cdot U$ wobei die c_i Funktionen von R_1, R_2, R_3, R_4 abhängen.
$I_3 = c_3 \cdot U$

3.18 Beispiel: (Wahrscheinlichkeitsrechnung)

Bei einem Spiel werden zwei Würfel geworfen und die Augenzahlen addiert. Abhängig von der Summe wählen die Spieler entsprechend ihrer (geheimen) Strategie eine der Aktionen $A_1, \ldots, A_k$. Ein Beobachter protokolliert das Verhalten der Spieler bei einer großen Anzahl von Spielen und bestimmt $P_i(A_j)$, die Wahrscheinlichkeit dafür, dass Spieler i die Aktion A_j wählt. Wie kann der Beobachter die Strategie der Spieler bestimmen?
Unter Verwendung der bekannten Wahrscheinlichkeiten $P(B_l)$ für die Würfelsumme $l \in \{2, 3, \ldots, 12\}$ und der (Unbekannten) bedingten Wahrscheinlichkeiten $P_i(A_j/B_l)$ („Wahrscheinlichkeit dafür, dass Spieler i die Aktion A_j wählt, wenn die Würfelsumme l ist“) erhalten wir das LGS:

$$P_i(B_2) \cdot \underbrace{P_i(A_i/B_2)}_{\text{Unbestimmte}} + \ldots + P_i(B_{12}) \cdot \underbrace{P_i(A_j/B_{12})}_{\text{Unbestimmte}} = P_i(A_j)$$

für $i = 1, \ldots, \#Spieler$ und $j = 1, \ldots, k$.
Hieraus kann man die Lösungsmenge $\{P_i(A_j/B_l) \mid j = 1, \ldots, k \text{ und } l = 2, \ldots, 12\}$ für die Strategie von Spieler i berechnen.

E. Wie kann man LGS effektiv lösen?

3.19 Definition:

Ist ein LGS $(*)$ gegeben, so heißt

$$(+) \left\{ \begin{array}{ccccccc} a_{11}x_1 & + & \ldots & + & a_{1n}x_n & = & 0 \\ \vdots & & & & \vdots & = & \vdots \\ a_{m1}x_1 & + & \ldots & + & a_{mn}x_n & = & 0 \end{array} \right. \quad \text{das assoziierte homogene LGS.}$$

3.20 Satz: (Reduktion auf homogene LGS)

Sei $\mathbb{L}$ die Lösungsmenge von $(*)$ und $\tilde{\mathbb{L}}$ die Lösungsmenge von $(+)$. Ferner sei $(c_1, \ldots, c_n) \in \mathbb{L}$ eine feste Lösung von $(*)$. Dann gilt
$\mathbb{L} = (c_1, \ldots, c_n) + \tilde{\mathbb{L}} = \{(c_1 + d_1, \ldots, c_n + d_n) \mid (d_1, \ldots, d_n) \in \tilde{\mathbb{L}}\}$

Beweis:
„$\subseteq$“ Sei $(e_1, \ldots, e_n) \in \mathbb{L}$. Dann gilt $a_{i1}e_1 + \ldots + a_{in}e_n = b_i$ und $a_{i1}c_1 + \ldots + a_{in}c_n = b_i$ für $i = 1, \ldots, m$
Die Differenzgleichung $a_{i1}(e_1 - c_1) + \ldots + a_{in}(e_n + c_n) = 0$ für $i = 1, \ldots, m$ zeigt, dass das Tupel $(d_1, \ldots, d_n) = (e_1 - c_1, \ldots, e_n - c_n)$ eine Lösung von $(+)$ ist.
Nun liefert $(e_1, \ldots, e_n) = (c_1, \ldots, c_n) + (d_1, \ldots, d_n) \in (c_1, \ldots, c_n) + \tilde{\mathbb{L}}$ die Behauptung.

„$\supseteq$ Sei $(d_1, \ldots, d_n) \in \tilde{\mathbb{L}}$ d.h. es gelte $a_{i1}d_1 + \ldots + a_{in}d_n = 0$ für $i = 1, \ldots, m$.
Dann folgt:
$a_{i1}(c_1 + d_1) + \ldots + a_{in}(c_n + d_n) = (a_{i1}c_1 + \ldots + a_{in}c_n) + (a_{i1}d_1 + \ldots + a_{in}d_n) = b_i + 0 = b_i$ für $i = 1, \ldots, m$ und somit $(c_1 + d_2, \ldots, c_n + d_n) \in \mathbb{L}$. qed.

3.21 Bemerkung:

Wir werden später sehen, dass man eine Lösung $(c_1, \ldots, c_n)$ von $(*)$ mit einer Formel berechnen kann („Cramersche Regel“). Also kann man das Lösen des LGS $(*)$ mit Satz 3.20 auf den homogenen Fall zurückführen.

3.22 Definition: (Matrizen Notation)

Um die Durchführung der Gaußschen Elimination übersichtlicher zu gestalten, führen wir folgende Notation ein:

(a) eine $m \times n$-Matrix über K ist ein rechteckiges Zahlenschema

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \text{ mit } a_{ij} \in K$$

(b) Fassen wir die Koeffizienten a_{ij} zu einer Matrix

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$$

über K zusammen, so heißt A die Koeffizientenmatrix des LGS $(*)$

(c) Die Matrix

$$B = \left(\begin{array}{ccc|c} a_{11} & \cdots & a_{1n} & b_1 \\ \vdots & & \vdots & \vdots \\ a_{m1} & \cdots & a_{mn} & b_m \end{array}\right)$$

heißt die erweiterte Koeffizientenmatrix des LGS $(*)$

(d) Schreibweise des LGS:

$$A \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$$

3.23 Bemerkung:

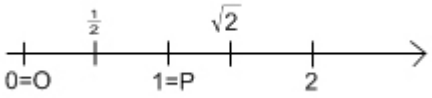
Man kann die Schritte des Gauß-Verfahrens bzw. des Gauß-Jordan-Verfahrens auch direkt mit der erweiterten Koeffizientenmatrix des LGS durchzuführen. Ist das LGS homogen, so kann man auch mit der Koeffizientenmatrix selbst arbeiten.
Die sogenannte Matrizenrechnung wird später behandelt.

4 Blick in den n-Dimensionalen Raum

(Affine Räume - der $\mathbb{R}^n$)
Rene Descartes hatte folgende Idee, wie man die Zeichenebene durch die Tupel im $\mathbb{R}^2$ darstellen kann:

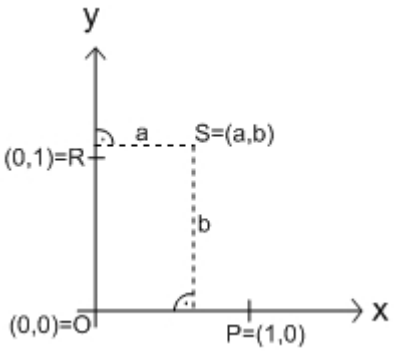
4.1 Bemerkung:

(a) In der Zeichenebene wählt man zwei „ausgezeichnete“ Punkte O und P. Wir identifizieren O mit der reellen Zahl 0 und P mit 1. Jeder Punkt auf der Geraden $\overline{OP}$ entspricht dann genau einer reellen Zahl.



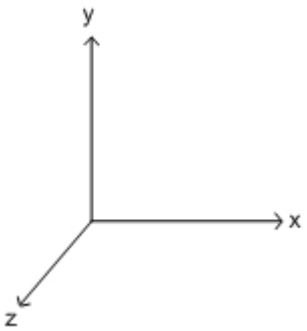
Diese Gerade heißt die x-Achse.

Dann bildet man die Senkrechte zur x-Achse durch O und nennt sie y-Achse. Dreht man den Punkt P um 90 um O, so wird der resultierende Punkt R auf der y-Achse mit $R = (0, 1)$ bezeichnet. Statt O schreiben wir auch $(0, 0)$ und statt P auch $(1, 0)$.
Skizze:



Ist eine beliebiger Punkt S gegeben, so fällen wir das Lot auf die x-Achse und erhalten eine Zahl $a \in \mathbb{R}$. Ebenso fällen wir das Lot auf die y-Achse und erhalten $b \in \mathbb{R}$. Dann wir S mit dem Tupel (a, b) identifiziert. Auf diese Weise können wir die Zeichenebene mit $\mathbb{R}^2$ identifizieren.

(b) Auf diese Wiese kann man auch den Anschauungsraum mit $\mathbb{R}^3$ identifizieren.
Skizze:



Die positive x-Achse, positive y-Achse und positive z-Achse sind dabei nach der rechte-Hand-Regel angeordnet.

(c) Eine Gerade G in der Zeichenebene kann auf mehrere Weisen mit einer Teilmenge von $\mathbb{R}^2$ identifiziert werden:

1.) Ist die Gerade durch zwei Punkte $P_1 = (a, b)$ und $P_2 = (c, d)$ gegeben, also $G = \overline{P_1P_2}$, so gilt:
$G = \{\underbrace{(a, b) + \lambda(c - a, d - b)}_{= a + \lambda(c-a), b + \lambda(d-b)} \mid \lambda \in \mathbb{R}\}$
„Parameterdarstellung“ einer Geraden in $\mathbb{R}^2$

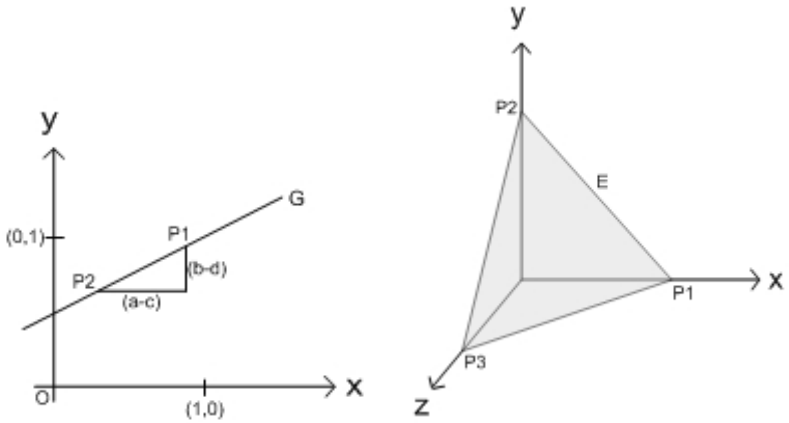
2.) Es gilt auch $G = \{(c_1, c_2) \in \mathbb{R} \mid (c_1 - a)(d - b) - (c_2 - b)(c - a) = 0\}$
d.h. G ist die Lösungsmenge einer linearen Gleichung
$\alpha x + \beta y = \gamma$ mit $\alpha, \beta, \gamma \in \mathbb{R}$ und $(\alpha, \beta) \neq (0, 0)$

(d) Entsprechend kann man auch eine Ebene im $\mathbb{R}^3$ darstellen:

1.) Sind $P_1 = (a_1, a_2, a_3), P_2 = (b_1, b_2, b_3), P_3 = (c_1, c_2, c_3)$ drei Punkte in E, die nicht auf einer Geraden liegen, so gilt:
$E = \{(a_1, a_2, a_3) + \lambda(b_1 - a_1, b_2 - a_2, b_3 - a_3) + \mu(c_1 - a_1, c_2 - a_2, c_3 - a_3) \mid \lambda, \mu \in \mathbb{R}\}$
„Parameterdarstellung“ einer Ebene $E \subseteq \mathbb{R}^3$

2.) Eine Ebene E ist auch die Lösungsmenge einer linearen Gleichung
$\alpha x + \beta y + \gamma z = \delta$ mit $\alpha, \beta, \gamma, \delta \in \mathbb{R}$ und $(\alpha, \beta, \gamma) \neq (0, 0, 0)$

Skizze:



4.2 Definition:

Sei $n \geq 1$.

(a) Die Menge $\mathbb{R}^n$ heißt der n-dimensionale affine Raum über $\mathbb{R}$.

(b) Eine Teilmenge $G \subseteq \mathbb{R}^n$ der Form $G = \{(a_1, \ldots, a_n) + \lambda(b_1, \ldots, b_n) \mid \lambda \in \mathbb{R}\}$ von $\mathbb{R}^n$ mit fest gewählten $a_i, b_j \in \mathbb{R}$, wobei $(b_1, \ldots, b_n) \neq (0, \ldots, 0)$ sein muss, heißt eine Gerade im $\mathbb{R}^n$.

(c) Eine Teilmenge $E \subseteq \mathbb{R}^n$ der Form
$E = \{(a_1, \ldots, a_n) + \lambda(b_1, \ldots, b_n) + \mu(c_1, \ldots, c_n) \mid \lambda, \mu \in \mathbb{R}\}$ mit fest gewählten $a_i, b_j, c_k \in \mathbb{R}$ und $(b_1, \ldots, b_n) \neq (0, \ldots, 0)$ und $(c_1, \ldots, c_n) \neq (0, \ldots, 0)$, die nicht in $\{\lambda(b_1, \ldots, b_n) \mid \lambda \in \mathbb{R}\}$ liegt, heißt eine Ebene im $\mathbb{R}^{\aleph}$.

(d) Die Lösungsmenge einer linearen Gleichung $H = \{(c_1, \ldots, c_n) \in \mathbb{R}^n \mid a_1c_1 + \ldots + a_nc_n = b\}$ mit fest gewählten $a_1, \ldots, a_n, b \in \mathbb{R}$ und $(a_1, \ldots, a_n) \neq (0, \ldots, 0)$ heißt eine Hyperebene im $\mathbb{R}^n$.

4.3 Beispiele:

(a) Sei $i \in \{1, \ldots, n\}$. Die x_i-Achse ist die Gerade
$G_i = \{[0, \ldots, 0) + \lambda(0, \ldots, 0, \underbrace{1}_{\text{i-te Stelle}}, 0, \ldots, 0) \mid \lambda \in \mathbb{R}\}$
$= \{(0, \ldots, 0, \overbrace{\lambda}, 0, \ldots, 0) \mid \lambda \in \mathbb{R}\}$ im $\mathbb{R}^n$.

(b) Die Menge $H_n = \{(c_1, \ldots, c_n) \in \mathbb{R}^n \mid c_1 + \ldots + c_n = 1\}$ ist eine Hyperebene im $\mathbb{R}^n$.

1.) Bild im $\mathbb{R}^2$:

2.) Bild im $\mathbb{R}^3$

A. Was kann man mit den Punkten im $\mathbb{R}^n$ so alles machen?

Man kann die Punkte im $\mathbb{R}^n$ (oder Tupel) addieren und mit Skalaren (d.h. Elementen von $\mathbb{R}$ multiplizieren.

4.4 Definition:

(a) Die Verknüpfung
$$\begin{array}{rcl} + : \mathbb{R}^n \times \mathbb{R}^n & \to & \mathbb{R}^n \\ ((a_1, \ldots, a_n), (b_1, \ldots, b_n)) & \mapsto & (a_1 + b_1, \ldots, a_n + b_n) \end{array}$$
macht $\mathbb{R}^n$ zu einer abelschen Gruppe. Diese Verknüpfung heißt die Addition (oder Vektoraddition) im $\mathbb{R}^n$.

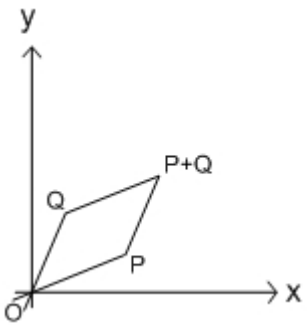
(b) Die Abbildung
$$\begin{array}{rcl} \cdot : \mathbb{R} \times \mathbb{R}^n & \to & \mathbb{R}^n \\ (\lambda(a_1, \ldots, a_n)) & \mapsto & (\lambda a_1, \ldots, \lambda a_n) \end{array}$$
heißt die skalare Multiplikation im $\mathbb{R}^n$.

4.5 Beispiel:

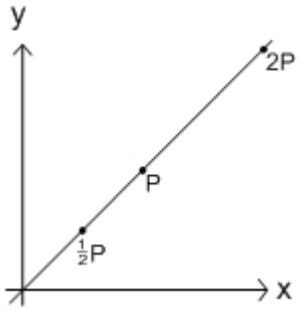
Man kann jeden Punkt $(a_1, \ldots, a_n) \in \mathbb{R}^n$ durch Addition und skalare Multiplikation aus den Punkten $P_1 = (1, 0, \ldots, 0), P_2 = (0, 1, 0, \ldots, 0), \ldots, P_n = (0, \ldots 0, 1)$ gewinnen:
$(a_1, \ldots, a_n) = (a_1, 0, \ldots, 0) + (0, a_2, 0, \ldots, 0) + \ldots + (0, \ldots, 0, a_n) = (a_1 P_1 + a_2 P_2 + \ldots + a_n P_n)$

4.6 Beispiel: (Geometrische Deutung der Addition und der skalaren Multiplikation im $\mathbb{R}^2$ und $\mathbb{R}^3$)

(a) (Vektor-)Addition im $\mathbb{R}^2$:



(b) Skalare Multiplikation im $\mathbb{R}^2$:



(c) Die Addition und skalare Multiplikation im $\mathbb{R}^3$: entsprechen ebenfalls der „Hintereinanderlegung“ der Strecken, bzw. ihrer „zentrischen Streckung“ .

(d) Man kann die Punkte des $\mathbb{R}^n$ mit Vektoren identifizieren. Ein Punkt $P \in \mathbb{R}^n$ entspricht dem Vektor („Pfeil“) $\overrightarrow{OP}$ vom Ursprung oder auch Nullpunkt O zum Punkt P.

4.7 Satz: (Rechenregeln für Addition und skalare Multiplikation im $\mathbb{R}^n$)

(a) $(\mathbb{R}^n, +)$ ist eine abelsche Gruppe.

(b) Es gelten die Distributivgesetze:

1.) $\lambda(v + w) = \lambda v + \lambda w$ für $\lambda \in \mathbb{R}$ und $v, w \in \mathbb{R}^n$

2.) $(\lambda + \mu)v = \lambda v + \mu v$ für $\lambda, \mu \in \mathbb{R}$ und $v \in \mathbb{R}^n$

(c) Es gilt $1 \cdot v = v$ für $v \in \mathbb{R}^n$ (Treue).

(d) Es gilt ein Assoziativgesetz: $(\lambda \cdot \mu)v = \lambda(\mu v)$ für $\lambda, \mu \in \mathbb{R}$ und $v \in \mathbb{R}^n$

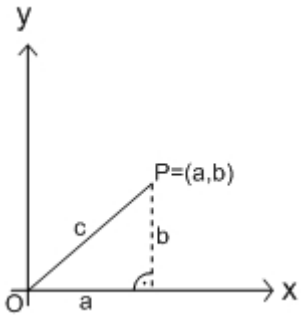
C. Was hat das alles mit Geometrie zu tun?

In der Geometrie will man Längen und Winkel messen.

4.8 Beispiel: (Längen- und Winkelmessung im $\mathbb{R}^2$)

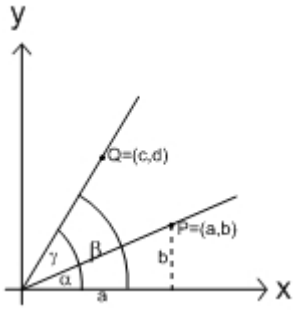
(a) Seien $P = (a, b)$ und $Q = (c, d)$ zwei Punkte im $\mathbb{R}^2$. Dann heißt $\|\overrightarrow{PQ}\| = \sqrt{(c-a)^2 + (d-b)^2}$ die Länge der Strecke $\overline{PQ}$ bzw. des Vektors $\overrightarrow{PQ}$.

(b) Die Abbildung $\|\cdot\| : \mathbb{R}^2 \to \mathbb{R}$, $P \mapsto \|\overrightarrow{PQ}\| = \sqrt{a^2+b^2}$ heißt die Norm von $\mathbb{R}^2$. Sie ordnet jedem Punkt P den Abstand vom Nulltpunkt O zu.
Skizze:



Der Satz von Pythagoras liefert $c^2 = a^2 + b^2$.
Also ist die obige Definition sinnvoll.

(c) Den Winkel zwischen zwei Gerade durch den Ursprung kann man über seinen Kosinus definieren.
Skizze:



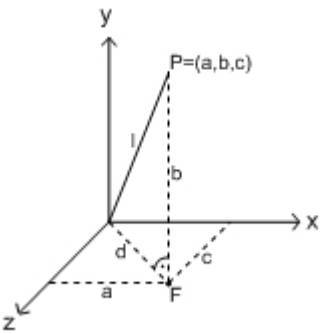
$$cos(\alpha) = \frac{a}{\sqrt{a^2+b^2}}$$
$$sin(\alpha) = \frac{b}{\sqrt{a^2+b^2}}$$
$$cos(\beta) = \frac{c}{\sqrt{c^2+d^2}}$$
$$sin(\beta) = \frac{d}{\sqrt{c^2+d^2}}$$

Für den Winkel $\gamma = \beta - \alpha$ folgt:
$cos(\gamma) = cos(\beta-\alpha) = cos(\alpha)cos(\beta) + sin(\alpha)sin(\beta) = \frac{ac+bd}{\sqrt{a^2+b^2}\cdot\sqrt{c^2+d^2}} = \frac{ac+bd}{\|P\|\cdot\|Q\|}$
Die Zahl $< P, Q >= ac + bd$ heißt dabei das Skalarprodukt der Vektoren $\overrightarrow{OP}$ und $\overrightarrow{OQ}$.

4.9 Beispiel: (Längen und Winkelmessung im $\mathbb{R}^3$)

(a) Für Punkte $P = (a, b, c)$ und $Q = (d, e, f)$ im $\mathbb{R}^3$ heißt $\|\overrightarrow{PQ}\| = \sqrt{(d-a)^2 + (e-b)^2 + (f-c)^2}$ die Länge der Strecke $\overline{PQ}$

(b) Die Abbildung $\|\cdot\| : \mathbb{R}^3 \to \mathbb{R}$, $(a, b, c) \mapsto \sqrt{a^2+b^2+c^2} = \|\overrightarrow{OP}\|$ heißt die Norm von $\mathbb{R}^3$.
Dass diese Definition sinnvoll ist, folgt wieder aus dem Satz des Pythagoras.
Skizze:



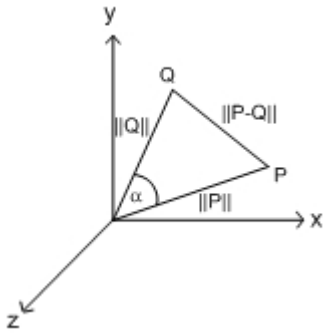
F sei der Fußpunkt des Lots von P auf die x-z-Ebene.

Dann gilt: $d = \sqrt{a^2+c^2}$ und
$l = \sqrt{d^2+b^2} = \sqrt{a^2+b^2+c^2}$

(c) Den Winkel zwischen zwei Geraden $\overrightarrow{OP}$ und $\overrightarrow{OQ}$ im $\mathbb{R}^3$ die sich in O schneiden, definieren wir für $P = (p_1, p_2, p_3)$ und $Q = (q_1, q_2, q_3)$ durch:
$cos(\alpha) = \dfrac{p_1q_1 + p_2q_2 + p_3q_3}{\|P\| \cdot \|Q\|}$

1.) Wieso ist dies wohldefiniert, d.h. wieso liegt die rechte Seite im Intervall [-1,1]?
Dies folgt aus der Cauchy-Schwarzschen Ungleichung (siehe unten).

2.) Wieso macht diese Definition Sinn?
In einem Dreieck $\bigtriangleup ABC$ mit Seitenlängen a, b, c gilt:
$c^2 = a^2 + b^2 - 2ab \cdot cos(\alpha)$
$\Rightarrow cos(\alpha) = \frac{a^2+b^2-c^2}{2ab}$ Wähle hier $a = \|P\|, b = \|Q\|, c = \|P - Q\|$
Dann folgt: $cos(\alpha) = \frac{p_1^2+p_2^2+p_3^2+q_1^2+q_2^2+q_3^2-\left[(p_1-q_1)^2+(p_2-q_2)^2+(p_3-q_3)^2\right]}{2\cdot\|P\|\cdot\|Q\|}$
$= \frac{2p_1q_1+2p_2q_2+2p_3q_3}{2\cdot\|P\|\cdot\|Q\|} = \frac{p_1q_1+p_2q_2+p_3q_3}{\|P\|\cdot\|Q\|}$
Skizze:



4.10 Definition: (Längenmessung im $\mathbb{R}^n$)

Die Abbildung $\begin{array}{rcl} \|\cdot\| : \mathbb{R}^n & \to & \mathbb{R} \\ (a_1, \ldots, a_n) & \mapsto & \sqrt{a_1^2 + \ldots + a_n^2} \end{array}$ heißt die (euklidische) Norm auf $\mathbb{R}^n$.

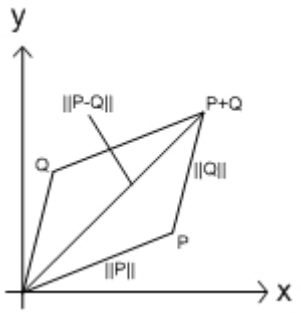
4.11 Satz: (Eigenschaften der Norm)

Sei $\|\cdot\| : \mathbb{R}^n \to \mathbb{R}$ die euklidische Norm. Dann gilt:

(a) $\|P\| \geq 0$ für alle $P \in \mathbb{R}^n$ und $\|P\| = 0$ genau dann, wenn $P = 0$ gilt.

(b) Für alle $\lambda \in \mathbb{R}$ und alle $P \in \mathbb{R}^n$ gilt: $\|\lambda P\| = \mid \lambda \mid \cdot \|P\|$

(c) Für $P, Q \in \mathbb{R}^n$ gilt die Dreiecksungleichung:
$\|P + Q\| \leq \|P\| + \|Q\|$
Skizze:



Beweis:

(a) Für $P = (a_1, \ldots, a_n)$ gilt $\|P\| = \sqrt{a_1^2 + \ldots + a_n^2} \geq 0$.
Hierbei ist $\|P\| = 0$ genau dann, wenn $a_1^2 + \ldots + a_n^2 = 0$ gilt, also genau für $(a_1, \ldots, a_n) = (0, \ldots, 0)$

(b) Es gilt $\|\lambda P\| = \sqrt{(\lambda a_1)^2 + \ldots + (\lambda a_n)^2}$ denn $\lambda P = (\lambda a_1, \ldots, \lambda a_n)$
$= \sqrt{\lambda^2(a_1^2 + \ldots + a_n^2)} = \mid \lambda \mid \sqrt{a_1^2 + \ldots + a_n^2} = \mid \lambda \mid \cdot \|P\|$

(c) Folgt aus der Cauchy-Schwarzschen Ungleichung (siehe unten). qed.

4.12 Definition: (Winkelmessung im $\mathbb{R}^n$)

(a) Seien $P = (a_1, \ldots, a_n)$ und $Q = (b_1, \ldots, b_n)$ zwei Punkte im $\mathbb{R}^n \backslash \{0\}$.
Dann ist der Winkel α zwischen $\overrightarrow{OP}$ und $\overrightarrow{OQ}$ definiert durch
$cos(\alpha) = \frac{a_1 b_1 + \ldots + a_n b_n}{\|P\| \cdot \|Q\|}$
Dies ist wohldefiniert, denn die rechte Seite liefert stets einen Wert im Intervall [-1,1], wie sich aus der Cauchy-Schwarzschen Ungleichung (siehe Unten) ergibt.

(b) Die Abbildung $< \cdot, \cdot >: \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$, $((a_1, \ldots, a_n), (b_1, \ldots, b_n)) \mapsto (a_1 b_1 + \ldots + a_n b_n)$ heißt das Skalarprodukt auf $\mathbb{R}^n$.

4.13 Satz: (Eigenschaften des Skalarprodukts)

Für $\lambda_1, \lambda_2 \in \mathbb{R}$ und $v, v_1, v_2, w, w_1, w_2 \in \mathbb{R}^n$ gilt:

(a) $< (\lambda_1 v_1 + \lambda_2 v_2), w >= \lambda_1 < v_1, w > + \lambda_2 < v_2, w >$

(b) $< v, (\lambda_1 w_1 + \lambda_2 w_2) >= \lambda_1 < v, w_1 > + \lambda_2 < v, w_2 >$

(c) $< v, w >=< w, v >$

(d) $< v, v >= \|v^2\| \geq 0$

(e) $< v, v >= 0$, genau dann, wenn $v = 0$ gilt

Beweis: Nachrechnen!

4.14 Theorem: (Die Cauchy-Schwarzsche Ungleichung)

Für $v, w \in \mathbb{R}^n$ gilt: $|< v, w >| \leq \|v\| \cdot \|w\|$.

Beweis: Für $w = 0$ ist die Behauptung wahr. Sei nun $w \neq 0$. Für $\lambda \in \mathbb{R}$ gilt:
$0 \underset{(a)}{=} < v - \lambda w, v - \lambda w > \underset{(a)}{=} < v, v - \lambda w > -\lambda < w, v - \lambda w >$
$\underset{(b)}{=} < v, v > -\lambda < v, w > -\lambda < w, v > + \lambda^2 < w, w > \underset{(c)}{=} < v, v > -2\lambda < v, w > + \lambda^2 < w, w >$
Wähle nun $\lambda = \frac{<v,w>}{<w,w>}$ (mit $< w, w >> 0$) und erhalte:
$0 \leq < v, v > - \frac{2<v,w>}{<w,w>} < v, w > + \frac{<v,w>^2}{<w,w>^2} < w, w >$
Multiplikation mit $< w, w >$ liefert:
$0 \leq < v, v >< w, w > -2 < v, w >^2 + < v, w >^2$ also $0 \leq \|v\|^2 \cdot \|w\|^2 - < v, w >^2$
Es folgt: $< v, w >^2 \leq \|v\|^2 \cdot \|w\|^2$ also $< v, w > \leq \|v\| \cdot \|w\|$ qed.

4.15 Bemerkung:

Aus der Cauchy-Schwarzschen Ungleichung folgt für $v, w \neq 0$ die Ungleichung $|\frac{<v,w>}{\|v\|\cdot\|w\|}| \leq 1$. Damit ist der Winkel zwischen v und w wohldefiniert.

4.16 Beweis der Dreiecksungleichung:

Es gilt: $\|v+w\|^2 + < v+w, v+w > = < v, v > + 2 < v, w > + < w, w >$
$\leq \|v\|^2 + 2\|v\| \cdot \|w\| + \|w\|^2 = (\|v\| + \|w\|)^2$
Wurzelziehen liefert:
$\|v+w\| \leq \|v\| + \|w\|$ qed.

4.17 Bemerkung:

Mit obigen Definitionen und Sätzen kann man viele geometrische Sätze wie folgt beweisen:

(a) Führe ein geeignetes rechtwinkliges Koordinatensystem ein.

(b) Stelle die Parameterdarstellungen bzw. die definierten Gleichungen aller beteiligten Geraden, Ebenen, etc. auf.

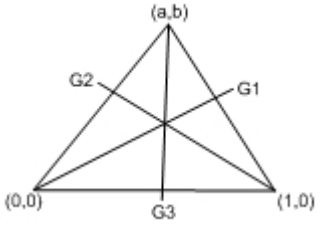
(c) Formuliere die Behauptung algebraisch und beweise sie mit algebraischen Mitteln (Lösen von LGS, Grübner-Basen, ...)

4.18 Beispiel:

Betrachte den folgenden Satz:
In einem Dreieck schneiden sich die drei Seitenhalbierenden in einem Punkt. Sie werden von diesem Punkt im Verhältnis 2:1 geteilt (Schwerpunkt).

Beweis:

(a) Skizze:



(b) Parameterdarstellung der beteiligte Geraden:
$G_1 = \{\lambda(\frac{a+1}{2}, \frac{b}{2}) \mid \lambda \in \mathbb{R}\}$
$G_2 = \{(1,0) + \mu(-1+\frac{a}{2}, \frac{b}{2}) \mid \mu \in \mathbb{R}\}$
$G_3 = \{(a,b) + \nu(\frac{1}{2} - a, -b) \mid \nu \in \mathbb{R}\}$

(c) Bestimmung der Schnittpunkte:

$$G_1 \cap G_2: \begin{cases} \lambda\frac{a+1}{2} = 1 + \mu(-1+\frac{a}{2}) \\ \lambda\frac{b}{2} = \mu\frac{b}{2} \end{cases} \text{ Es folgt: } \lambda = \mu = \tfrac{2}{3}$$

$$G_1 \cap G_3: \begin{cases} \lambda\frac{a+1}{2} = a + \nu(\frac{1}{2} - a) \\ \lambda\frac{b}{2} = b - \nu b \end{cases} \text{ Es folgt: } \lambda = \nu = \tfrac{2}{3}$$

also $G_1 \cap G_2 = G_1 \cap G_3 = G_3 \cap G_3$ qed.

Kapitel II: Die ersten Scharmützel

5 Räume voller Vektoren (Vektorräume und Untervektorräume)

A. Was ist ein Vektorraum?

Im Folgenden sei stets K ein Körper.
Die Beispiele in §3 und §4 legen die folgende Definition nahe:

5.1 Definition:

Eine Menge heißt ein K-Vektorraum, wenn die folgenden Bedingungen erfüllt sind:

(a) Es gibt eine Verknüpfung $+ : V \times V \to V$, $(v, w) \mapsto v + w$, so dass $(V, +)$ eine kommutative Gruppe ist.

(b) Es gibt eine Abbildung $\cdot : K \times V \to V$, $(\lambda, v) \mapsto \lambda v$, genannt skalare Multiplikation, so dass gilt:

1.) Assoziativgesetz: $\lambda(\mu v) = (\lambda\mu)v$ für $\lambda, \mu \in K$ und $v \in V$
2.) erstes Distributivgesetz: $\lambda(v + w) = \lambda v + \lambda w$ für $\lambda \in K$ und $v, w \in V$
3.) zweites Distributivgesetz: $(\lambda + \mu)v = \lambda v + \mu v$ für $\lambda, \mu \in K$ und $v \in V$
4.) Treue: $1 \cdot v = v$ für $v \in V$

Die Elemente von V werden auch als Vektoren bezeichnet.

5.2 Beispiele:

(a) In §4 haben wir gesehen, dass $\mathbb{R}^n$ ein Vektorraum über dem Körper $\mathbb{R}$ ist, wenn man komponentenweise Addition $+ : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n$, $((a_1, \ldots, a_n), (b_1, \ldots, b_n)) \mapsto (a_1 b_1 + \ldots + a_n b_n)$ und komponentenweise skalare Multiplikation $\cdot : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n$, $(\lambda, (a_1, \ldots, a_n)) \mapsto (\lambda a_1, \ldots, \lambda a_n)$ verwendet.

(b) Sei $L \subseteq K^n$ die Lösungsmenge eines homogenen LGS. Dann ist L auch ein K-Vektorraum bezüglich komponentenweiser Addition und skalarer Multiplikation.

(c) Ist M eine Menge, so ist die Menge $Abb(M, K)$ in natürlicher Weise ein K-Vektorraum.

5.3 Beispiel:

Sei $I \subseteq \mathbb{R}$ ein Intervall und $C^\circ(I)$ die Menge aller stetig differenzierbaren Funktionen $f : I \to \mathbb{R}$. Dann wird $C^\circ(I)$ durch

$$\begin{array}{rcl} + : C^\circ(I) \times C^\circ(I) & \to & C^\circ(I) \\ (f,g) & \mapsto & f+g \end{array} \text{ mit } \begin{array}{rcl} f+g : I & \to & \mathbb{R} \\ a & \mapsto & f(a)+g(a) \end{array} \text{ sowie}$$

$$\begin{array}{rcl} \cdot : \mathbb{R} \times C^\circ(I) & \to & C^\circ(I) \\ (\lambda, f) & \mapsto & \lambda f \end{array} \text{ mit } \begin{array}{rcl} \lambda f : I & \to & \mathbb{R} \\ a & \mapsto & \lambda f(a) \end{array}$$

zu einem $\mathbb{R}$-Vektorraum.
Ebenso ist z.B. $C^n(I)$ die Menge aller n-mal stetig differenzierbaren Funktionen auf I ein $\mathbb{R}$-Vektorraum.

5.4 Beispiel:

Sei $\mathbb{R}^{\mathbb{N}} = Abb(\mathbb{N}, \mathbb{R})$ die Menge aller Folgen $(a_i)_{i\geq 0}$.
Dann wird $\mathbb{R}^{\mathbb{N}}$ durch

$$\begin{array}{rcl} + : \mathbb{R}^{\mathbb{N}} \times \mathbb{R}^{\mathbb{N}} & \to & \mathbb{R}^{\mathbb{N}} \\ ((a_i)_{i\geq 0}, (b_i)_{i\geq 0}) & \mapsto & (a_i + b_i)_{i\geq 0} \end{array} \quad \text{und} \quad \begin{array}{rcl} \cdot : \mathbb{R}^{\mathbb{N}} \times \mathbb{R}^{\mathbb{N}} & \to & \mathbb{R}^{\mathbb{N}} \\ (\lambda, (a_i)_{i\geq 0}) & \mapsto & (\lambda a_i)_{i\geq 0} \end{array}$$

zu einem $\mathbb{R}$-Vektorraum.

5.5 Beispiel:

Sei $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$ der Körper der komplexen Zahlen.
Dann ist $\mathbb{C}$ ein $\mathbb{R}$-Vektorraum bezüglich

$$\begin{array}{rcl} + : \mathbb{C} \times \mathbb{C} & \to & \mathbb{C} \\ ((a_1 + b_1 i), (a_2 + b_2 i)) & \mapsto & (a_1 + a_2) + (b_1 + b_2)i \end{array}$$

und

$$\begin{array}{rcl} \cdot : \mathbb{C} \times \mathbb{C} & \to & \mathbb{C} \\ (a, (b + ci)) & \mapsto & ab + (ac)i \end{array}$$

5.6 Bemerkung:

Man kann folgende „allgemeine“ Beispiele aufstellen:

(a) Die Menge K^n ist ein K-Vektorraum bezüglich komponentenweiser Addition und skalarer Multiplikation.

(b) Sind K, L zwei Körper mit $K \subseteq L$, so ist L ein K-Vektorraum.

B. Kann ein Vektorraum in einem anderen enthalten sein?

5.7 Definition:

Sei V ein K-Vektorraum. Eine Teilmenge $U \subseteq V$ heißt K-Untervektorraum wenn U bezüglich $+$ und $\cdot$ von V selbst ein Vektorraum ist. Insbesondere muss U also bezüglich $+$ und $\cdot$ abgeschlossen sein, d.h. für $u_1, u_2 \in U$ und $\lambda \in K$ gilt $u_1 + u_2 \in U$ und $\lambda u_1 \in U$.

5.8 Satz: (Das Untervektorraumkriterium)

Sei V ein K-Vektorraum und $U \subseteq V$ eine Teilmenge. Genau dann ist U ein K-Untervektorraum von V, wenn folgende Bedingungen erfüllt sind:

(a) $U \neq \emptyset$ [Äquivalent zu $0 \in U$]

(b) Für $\lambda \in K$ und $u \in U$ gilt $\lambda u \in U$

(c) Für $u_1, u_2 \in U$ gilt $u_1 - u_2 \in U$

Beweis: „$\Rightarrow$“ siehe Definition.

„$\Leftarrow$“ Aus (a) und (b) folgt $0 \in U$.
Nach (a) gibt es ein $u \in U$. Nach dem Distributivgesetz gilt folgendes:
$0 \cdot u = (0+0)u = 0 \cdot u + 0 \cdot u$
Addiere $-0 \cdot u$ und erhalte $0 = 0 \cdot u$. Nach (b) folgt $0 \cdot u \in U$, also $0 \in U$.
Nach (c) gilt für jedes $u \in U$, dass auch $-u = 0 - u \in U$ gilt.
Somit ist U bezüglich $+$ abgeschlossen, denn für $u_1, u_2 \in U$ gilt $-u_2 \in U$ und somit
$u_1 + u_2 = u_1 - (-u_2) \in U$ nach (c). Insgesamt ist U also eine additive Untergruppe von V.
Nach (b) folgt, dass $\cdot : K \times U \to U$ wohldefiniert ist.
$(\lambda, u) \mapsto \lambda a$
Die Gültigkeit der Axiome eines Vektorraums in U folgt daraus, dass diese bereits in V gelten.
qed.

5.9 Beispiele:

(a) Eine Gerade durch den Ursprung O im $\mathbb{R}^2$ ist ein $\mathbb{R}$-Untervektorraum von $\mathbb{R}^2$.
Eine Gerade H, die nicht durch den Ursprung geht, ist kein $\mathbb{R}$-Untervektorraum, denn $0 \notin H$.

(b) Eine Ebene im $\mathbb{R}^3$ durch O ist ein $\mathbb{R}$-Untervektorraum von $\mathbb{R}^3$.
Eine Gerade im $\mathbb{R}^3$ durch O ebenfalls.

5.10 Beispiele:

(a) Die Menge $\{0\}$ ist ein K-Untervektorraum von V. Sie heißt der triviale Untervektorraum.

(b) Der ganze Vektorraum V ist auch ein K-Untervektorraum von V.

(c) Die Lösungsmenge L eines homogenen LGS in Unbestimmten ist ein K-Untervektorraum von K^n.

C. Wie kann man sich Untervektorräume selbst basteln?

Im Folgenden sei stets K ein Körper und V eine Vektorraum.

5.11 Definition:

(a) Ist eine Teilmenge $M \subseteq V$ gegeben, so ist $U = \{a_1v_1 + \ldots + a_kv_k \mid k \geq 0, a_i \in K, v_i \in M\}$ ein K-Untervektorraum von V. Er heißt der von M erzeugte K-Untervektorraum und wird mit $< M >$ bezeichnet.

(b) Sind $a_i, \ldots, a_k \in K$ und $v_1, \ldots, v_k \in V$, so heißt $a_1v_1 + \ldots + a_kv_k$ eine K-Linearkombination von $v_1, \ldots, v_k$. Mit anderen Worten, der von M erzeugte K-Untervektorraum $< M >$ besteht aus allen Linearkominationen von Elementen von M.
Man sagt $< M >$ wird von M erzeugt bzw. M ist ein Erzeugendensystem für $< M >$.
Ist $M = \{v_1, \ldots, v_k\}$ endlich, so schreiben wir auch $< M >=< v_1, \ldots, v_k >$.

5.12 Beispiel:

(a) Der K-Vektorraum K^n wird erzeigt von den sogenannten Einheitsvektoren $e_i = (0, \ldots, 0, i, 0, \ldots, 0)$ mit $1 \leq i \leq n$, denn für $(a_1, \ldots, a_n) \in K^n$ gilt:
$(a_1, \ldots, a_n) = (a_1, 0, \ldots, 0) + (0, a_2, 0, \ldots, 0) + \ldots + (0, \ldots, 0, a_n)$
$= a_1(1, 0, \ldots, 0) + a_2(0, 1, 0, \ldots, 0) + \ldots + a_n(0, \ldots, 0, 1)$
$= a_1e_1 + a_2e_2 + \ldots + a_ne_n$
Also gilt: $K^n =< e_1, \ldots, e_n >$

(b) Der triviale Untervektorraum $\{0\}$ wird von der leeren Menge $M = \emptyset$ erzeugt, denn die leere Summe ergibt definitionsgemäß 0.

(c) Der $\mathbb{R}$-Vektorraum $\mathbb{C}$ wird von $\{1, i\}$ erzeugt, denn $\mathbb{C} = \{a \cdot 1 + bi \mid a, b \in \mathbb{R}\}$. Sein $\mathbb{R}$-Untervektorraum $\mathbb{R}$ wird von $\{1\}$ erzeugt.

(d) Gegeben seien Vektoren $v_1 = (1, 2, 1), v_2 = (1, 0, 2), v_3 = (1, 1, 0)$ in $\mathbb{Q}^3$.
Gilt $(2, 1, 5) \in < v_1, v_2, v_3 >$?
Wir sichen also $a_1, a_2, a_3 \in \mathbb{Q}$ mit $a_1v_1 + a_2v_2 + a_3v_3 = (2, 1, 5)$, d.h. mit

$$\begin{cases} 1 \cdot a_1 + 1 \cdot a_2 + 1 \cdot a_3 = 2 \\ 2 \cdot a_1 + 0 \cdot a_2 + 1 \cdot a_3 = 1 \\ 1 \cdot a_1 + 1 \cdot a_2 + 0 \cdot a_3 = 5 \end{cases}$$

Lösen des LGS liefert $a_1 = 1, a_2 = 2, a_3 = 1$, also
$(2, 1, 5) = 1 \cdot v_1 + 2 \cdot v_2 + 1 \cdot v_3 \in < v_1, v_2, v_3 >$

D. Was kann man mit Untervektorräumen sonst noch anfangen?

Sei K ein Körper und V ein K-Vektorraum.

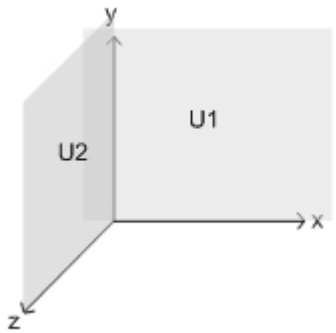
5.13 Bemerkung:

(a) Sind U_1, U_2 zwei K-Untervektorräume von V, so ist auch $U_1 \cap U_2$ ein K-Untervektorraum von V.

(b) Sind U_1, U_2 zwei K-Untervektorräume von V, so ist auch
$U_1 + U_2 = \{u_1 + u_2 \mid u_1 \in U_1, u_2 \in U_2\}$ ein K-Untervektorraum von V

5.14 Beispiel:

(a) Sei $K = \mathbb{R}$ und $V = \mathbb{R}^3$.
Betrachte die Untervektorräume $U_1 =< (1, 0, 0), (0, 1, 0) >$ und $U_2 =< (0, 1, 0), (0, 0, 1) >$
Skizze:



U_1 ist die x-y-Ebene
U_2 ist die y-z-Ebene.
$U_1 \cap U_2$ ist die y-Achse.

(b) Sei $G \subseteq \mathbb{R}^n$ eine Gerade in Parameterdarstellung, also durch den Ursprung O, also $G = \{\lambda(a_1, \ldots, a_n) \mid \lambda \in \mathbb{R}\}$ mit $(a_1, \ldots, a_n) \in \mathbb{R}^n \backslash \{0\}$.
Dann gilt: $G =< (a_1, \ldots, a_n) >$, d.h. G ist der von $\{(a_1, \ldots, a_n)\}$ erzeuge Untervektorraum.

(c) Sei $E \subseteq \mathbb{R}^n$ eine Ebene in Paramterdarstellung, also durch den Ursprung O, also $E = \{\lambda(a_1, \ldots, a_n) + \mu(b_1, \ldots, b_n) \mid \lambda, \mu \in \mathbb{R}\}$
Dann gilt: $E =< (a_1, \ldots, a_n), (b_1, \ldots, b_n) >$

5.15 Bemerkung:

Wie testet man, ob ein Untervektorraum in einem anderen enthalten ist?
Seien Vektoren $u_1, \ldots, u_k \in V$ gegeben mit $U =< u_1, \ldots u_k >$ Wir wollen wissen, ob U in einem Untervektorraum W enthalten ist.
Behauptung: Genau dann gilt $U \subseteq W$, wenn für $i = 1, \ldots, k$ gilt: $u_i \in W$.

Beweis: „$\Rightarrow$“ klar.

„$\Leftarrow$“ Sei $u \in U$. Schreibe $u = a_1u_1 + \ldots + a_ku_k$ mit $a_j \in K$. Wegen $a_i \in W$ für $i = 1, \ldots, k$ folgt auch $u = a_1u_1 + \ldots + a_ku_k \in W$ qed.

6 Basiswissen über Basen

Im Folgenden sei K ein Körper.

A. Was ist eine Basis?

6.1 Definition:

Eine Teilmenge B von V heißt eine K-Basis von V, wenn gilt:

(a) Die Menge B ist ein Erzeugendensystem von V, d.h. es gilt $V =< B >$.
Anders ausgedrückt: Jeder Vektor V ist Linearkombination endlich vieler Elemente von B.

(b) Die Menge B ist linear Unabhängig, d.h. es gilt $a_1v_1 + \ldots + a_kv_k = 0$ mit $a_1, \ldots a_k \in K$ und $v_1, \ldots, v_k \in B$, so folgt $a_1 = a_2 = \ldots = a_k = 0$.
Anders ausgedrückt: Die einzige Art, den Nullvektor aus den Vektoren in B durch eine Linearkombination zu erzeugen, ist die triviale Linearkombination $0 \cdot v_1 + \ldots + 0 \cdot v_k$.

6.2 Definition:

Eine Teilmenge $B \subseteq V$ mit Eigenschaft 6.1.b heißt eine linear unabhängige Menge von Vektoren. (Ist B nicht linear unabhängig, so heißt B linear abhängig.)

6.3 Beispiele:

(a) Sei $B = \{v\} \subseteq V$.
Ist der Vektor $v = 0$, so ist B linear abhängig, denn $1 \cdot v = 0$ ist eine nicht-triviale Linearkombination.
Sei nun $v \neq 0$. Ist $a \in K$ mit $a \cdot v = 0$ und ist $a \neq 0$, so folgt mit
$v = (a^{-1} \cdot a) \cdot v = a^{-1} \cdot 0 = 0$ ein Widerspruch zu $v \neq 0$.
Also muss $a = 0$ gelten, d.h. B ist linear unabhängig.

(b) Sei $B = \{v, w\} \subseteq V$.
Ist $v = 0$, so gilt $1 \cdot v + 0 \cdot w = 0$, d.h. die Menge B ist linear abhängig.
Sei nun $v \neq 0$.
1. Fall: w ist ein Vielfaches von v, d.h. es gibt ein $a \in K$ mit $w = a \cdot v$. Dann zeigt $1 \cdot w - a \cdot v = 0$ dass B linear abhängig ist.
2. Fall: $w \notin K \cdot v = \{\lambda v \mid \lambda \in K\}$. Wir behaupten, dass B in diesem Fall linear unabhängig ist. Sei $a, b \in K$ mit $a \cdot v + b \cdot w = 0$.
Gilt $b = 0$, so folgt $a \cdot v = 0$ und wegen $v \neq 0$ ist dann auch $a = 0$.
Gilt $b \neq 0$, so folgt mit $w = -\frac{a}{b} \cdot v \in K \cdot v$ ein Widerspruch zur Voraussetzung. Also ist $a = b = 0$ die einzige Möglichkeit.

6.4 Beispiel:

Sei $V = K^n$. Für $i = 1, \ldots, n$ sei $e_i = (0, \ldots, 0, 1, 0, \ldots, 0) \in K^n$ der i-te Einheitsvektor. Dann ist $B = \{e_1, \ldots, e_n\}$ eine K-Basis von K^n. Sie heißt die Standardbasis oder Einheitsbasis von K^n.
Begründung: Wir haben bereits gesehen, dass $K^n =< B >$ gilt.
Sei nun $a_1, \ldots, a_n \in K$ mit $a_1e_1 + \ldots + a_ne_n = 0$. Dann gilt:
$a_1e_1 + \ldots + a_ne_n = (a_1, \ldots, a_n) = (0, \ldots, 0)$, d.h. es folgt $a_1 = \ldots = a_n = 0$.

6.5 Beispiel:

Sei $M = \{m_1, \ldots, m_k\}$ eine endliche Menge und $V = Abb(M, K)$.
Für $i = 1, \ldots, k$ definiere $f_1 : M \to K$ (δ_{ij} = „Kroneckers Delta“)

$$m_j \mapsto \delta_{ij} = \begin{cases} 1, i=j \\ 0, i \neq j \end{cases}$$

Dann ist $\{f_1, \ldots, f_k\}$ eine K-Basis von $Abb(M, K)$.

B. Besitzt jeder Vektorraum eine Basis?

Im Prinzip ja, sprach Radio Eriwan.
Wir beweisen dies nur in einem Spezialfall, nämlich für endlich erzeugte Vektorräume, d.h. im Folgenden gelte:
Sei K eine Körper und V ein K-Vektorraum und es gebe Vektoren $v_1, \ldots, v_k \in V$ mit
$V = < v_1, \ldots, v_k >$.

6.6 Satz:

Ist $B = \{v_1, \ldots, v_k\}$ eine Basis von V, so besitzt jeder Vektor $w \in V$ eine eindeutige Darstellung $w = a_1v_1 + \ldots + a_kv_k$ mit $a_1, \ldots, a_k \in K$.

Beweis: Die *Existenz* einer solchen Darstellung folgt daraus, dass B ein Erzeugendensystem von V ist.

Eindeutigkeit: Sei $w = a_1v_1 + \ldots + a_kv_k = b_1v_1 + \ldots + b_kv_k$ mit $a_i, b_j \in K$. Dann gilt $(a_1 - b_1)v_1 + \ldots + (a_k - b_k)v_k = 0$ und aus der linearen Unabhängigkeit von B folgt $a_1 - b_1 = \ldots = a_k - b_k = 0$.
Also gilt $a_i = b_i$ für $i = 1, \ldots, k$. qed.

6.7 Satz: (Basisergänzungssatz)

Für eine Teilmenge $B \subseteq V$ sind die folgenden Bedingungen äquivalent:

(a) Die Menge B ist eine Basis von V.

(b) Die Menge B ist eine maximale linear unabhängige Teilmenge von V, d.h. es gibt keinen Vektor $w \in V \backslash B$, so dass $B \cup \{w\}$ immernoch linear unabhängig ist.

Insbesondere kann man jede linear unabhängige Teilmenge von V zu einer Basis von V ergänzen.

Beweis:

„(a) $\Rightarrow$ (b)“ Nach Definition ist B linear unabhängig. Zu zeigen ist noch, dass B maximal ist. Angenommen es gibt ein $w \in V \backslash B$, so dass $B \cup \{w\}$ linear unabhängig ist. Da B ein Erzeugendensystem von V ist, gibt es $a_1, \ldots, a_k \in K$ und $w_1, \ldots, w_k \in B$ mit $w = a_1w_1 + \ldots + a_kw_k$. Doch dann liefert $w - a_1w_1 - \ldots - a_kw_k = 0$ eine Widerspruch zur linearen Unabhängigkeit von $B \cup \{w\}$.

„(b) $\Rightarrow$ (a)“ Nach Voraussetzung ist B linear unabhängig. Zu zeigen ist also, dass B den Vektorraum V erzeugt.
Sei $v \in V$.
1. Fall: $v \in B$. Dann gilt offenbar $v \in < B >$.
2. Fall: $v \notin B$. Nach Voraussetzung ist $B \cup \{v\}$ linear unabhängig, d.h. es gibt $a_0, a_1, \ldots, a_l \in K$ und $w_1, \ldots, w_l \in B$ mit $a_0v + a_1w_1 + \ldots + a_lw_l = 0$ und $(a_0, \ldots, a_l) \neq (0, \ldots, 0)$.
Hierbei muss $a_0 \neq 0$ gelten, da B linear unabhängig ist.
Also folgt $v = -\frac{a_1}{a_0}w_1 - \ldots - \frac{a_l}{a_0}w_l \in < B >$. qed.

6.8 Satz: (Der Basisauswahlsatz)

Für eine Teilmenge B von V sind die folgenden Bedingungen äquivalent:

(a) Die Menge B ist eine Basis von V.

(b) Die Menge B ist ein minimales Erzeugendensystem von V, d.h. B erzeugt V, aber für alle $v \in B$ ist $B\backslash\{v\}$ kein Erzeugendensystem von V.

Insbesondere kann man von jedem Erzeugendensystem von V eine Basis auswählen.

Beweis:

„(a) $\Rightarrow$ (b)“ Nach Voraussetzung ist B ein Erzeugendensystem von V.
Angenommen, es gäbe ein $v \in B$, so dass $B\backslash\{v\}$ den Vektorraum erzeugt.
Schreibe dann $v = a_1w_1 + \ldots + a_lw_l$ mit $a_1, \ldots, a_l \in K$ und $w_1, \ldots, w_l \in B\backslash\{v\}$. Nun widerspricht $1 \cdot v - a_1w_1 - \ldots - a_lw_l = 0$ der vorrausgesetzten linearen Unabhängigkeit von B.

„(b) $\Rightarrow$ (a)“ Nach Voraussetzung ist B ein Erzeugendensystem von V.
Zu zeigen ist also, dass B linear unabhängig ist. Wäre B linear abhängig, so gäbe es $a_1, \ldots, a_l \in K$ und $w_1, \ldots, w_l \in B$ mit $a_1w_1 + \ldots + a_lw_l = 0$ und $(a_1, \ldots, a_l) \neq (0, \ldots, 0)$.
OBdA sei $a_i \neq 0$. Dann gilt:
$w_i = -\frac{a_1}{a_i}w_1 - \ldots - \frac{a_{i-1}}{a_i}w_{i-1} - \frac{a_{i+1}}{a_i}w_{i+1} - \ldots - \frac{a_l}{a_i}w_l$
also $w_i \in < w_1, \ldots, w_{i-1}, w_{i+1}, \ldots, w_l >$. Somit würde auch $B\backslash\{w_i\}$ den Vektorraum V erzeugen, was der Voraussetzung widerspricht. qed.

6.9 Korollar:

Jeder endlich erzeugte Vektorraum besitzt eine Basis.

Beweis: Nach Satz 6.8 kann man aus dem endlichen Erzeugendensystem eine Basis auswählen. qed.

C. Wie findet man eine Basis eines endlich erzeugten (Unter-)vektorraums?

Im Folgenden sei K ein Körper und V ein K-Vektorraum mit Basis $B = \{v_1, \ldots, v_k\}$.

6.10 Satz: (Basisberechnung)

Seien $w_1, \ldots, w_l \in V$ Vektoren, die einen Untervektorraum $U =< w_1, \ldots, w_l >$ erzeugen. Für $i = 1, \ldots, l$ schreibe $w_i = a_{i1}v_1 + \ldots + a_{ij}v_k$ mit $a_{ij} \in K$. Betrache folgende Instruktionen:

1.) Bilde eine Matrix

$$\begin{pmatrix} a_{11} & \cdots & a_{1k} \\ \vdots & & \vdots \\ a_{l1} & \cdots & a_{lk} \end{pmatrix}$$

2.) Bringe diese Matrix mit dem Gauß-Verfahren in Zeilenstufenform und erhalte:

$$\begin{pmatrix} b_{11} & \cdots & b_{1k} \\ \vdots & & \vdots \\ b_{m1} & \cdots & b_{mk} \\ 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix} \text{ mit } b_{ij} \in K.$$

(a) Dann bilden die Vektoren $u_i = b_{i1}v_1 + \ldots + b_{ik}v_k$ mit $1 \leq i \leq m$ eine K-Basis von U.

(b) Wurden keine Zeilen vertauscht, so bilden die Vektoren $\{w_1, \ldots, w_m\}$ ebenfalls eine Basis von U.

Beweisskizze:

(a) Bei elementaren Zeilenumformungen ändert sich der von den Vektoren erzeugte Untervektorraum nicht. ($< v + \lambda\tilde{v}, v >=< v, \tilde{v} >$)
Also gilt: $U =< u_1, \ldots, u_m >$. Seien $1 \leq i_1 < \ldots < i_m \leq k$ die Positionen (Spaltennummern) der Pirotelemente.
Sei nun $a_1u_1 + \ldots + a_mu_m = 0$ mit $a_i \in K$. Dann gilt:
$a_1(v_{i_1} + b_{1i_1+1}v_{i_1+1} + \ldots + b_{1k}v_k) + a_2(v_{i_2} + b_{2i_2+1}v_{i_2+1} + \ldots + b_{2k}v_k) + \ldots$
$+a_m(v_{i_m} + b_{mi_m+1}v_{i_m+1} + \ldots + b_{mk}v_k) = 0$
Hieraus folgt $a_1 = 0$ wie man am Koeffizienten von v_i erkennt. Nun ergibt sich $a_2 = 0$ aus dem Koeffizienten von v_2 usw.
Insgesamt ergibt sich also $a_1 = a_2 = \ldots = a_m = 0$, d.h. die lineare Unabhängigkeit von $\{u_1, \ldots, u_m\}$.

(b) Es gilt $< w_1, \ldots, w_l >=< u_1, \ldots, u_m >= U$. Im Fall $l = m$ folgt die Behauptung aus dem Basisauswahlsatz.
Betrache den Fall $l > m$. Nach Voraussetzung gilt $w_l - c_1w_1 - \ldots - c_{l-1}w_{l-1} = 0$ für gewisse $c_i \in K$. Also folgt $w_l \in< w_1, w_2, \ldots, w_{l-i-1} >$ für $i = 1, \ldots, l - m + 1$.
Aus $w_{m+1} \in< w_1, \ldots, w_m >$ und $w_{m+2} \in< w_1, \ldots, w_m, w_{m+1} >$ folgt
$w_{m+2} \in< w_1, \ldots, w_m >$. Induktiv folgt wieder $w_{m+i} \in< w_1, \ldots, w_m >$ für $i = 1, \ldots, l - m$.
Dies zeigt $U =< w_1, \ldots, w_m >$.
Da $\{u_1, \ldots, u_m\}$ ein minimales Erzeugendensystem von U ist, ist auch $\{w_1, \ldots, w_m\}$ eines und der Basisauswahlsatz liefert die Behauptung (vgl. später). qed.

6.11 Beispiel:

Gegeben seien die Vektoren $v_1 = (1, 0, 2, 1), v_2 = (-1, 2, 2, 0)$ und $v_3 = (3, -4, -2, 1)$ im $\mathbb{Q}$-Vektorraum $\mathbb{Q}^4$. Wir suchen eine $\mathbb{Q}$-Basis von $U =< v_1, v_2, v_3 >$.

1.) Bilde die Matrix

$$\begin{pmatrix} 1 & 0 & 2 & 1 \\ -1 & 2 & 2 & 0 \\ 3 & -4 & -2 & 1 \end{pmatrix}$$

2.) Berechne die Zeilenstufenform

$$\begin{pmatrix} 1 & 0 & 2 & 1 \\ 0 & 2 & 4 & 1 \\ 3 & -4 & -2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 2 & 1 \\ 0 & 2 & 4 & 1 \\ 0 & -4 & -8 & -2 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 2 & 1 \\ 0 & 2 & 4 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 2 & 1 \\ 0 & 1 & 2 & \frac{1}{2} \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Also sind $B = \{(1, 0, 2, 1), (0, 1, 2, \frac{1}{2})\}$ sowie $\tilde{B} = \{v_1, v_2\}$ Basen von U.

D. Sind alle Basen gleich lang?

Im Folgenden sei K eine Körper und V ein endlich erzeugter K-Vektorraum.

6.12 Lemma: (Das Austauschlemma)

Sei B eine Basis von V und $w \in V \setminus \{0\}$. Dann gibt es einen Vektor $v \in B$, so dass $(B \setminus \{v\}) \cup \{w\}$ wieder eine Basis von V ist.

Beweis: Sei $B = \{v_1, \ldots, v_k\}$. Schreibe $w = a_1v_1 + \ldots + a_kv_k$ mit $a_i \in K$.
Wegen $w \neq 0$ gibt es ein $i \in \{1, \ldots, k\}$ mit $a_i \neq 0$. Wir behaupten, dass $\tilde{B} = (B \setminus \{v_i\}) \cup \{w\}$ eine K-Basis von V ist.
Erzeugendensystem: Es gilt: $v_i = \frac{1}{a_i}w - \frac{a_1}{a_i}v_1 - \ldots - \frac{a_{i-1}}{a_i}v_{i-1} - \frac{a_{i+1}}{a_i}v_{i+1} - \ldots - \frac{a_k}{a_i}v_k \in < \tilde{B} >$
Also liegen alle Vektoren von B in $< \tilde{B} >$, d.h. es gilt $< \tilde{B} > = < B > = V$
Lineare Unabhängigkeit: Angenommen, es gibt $b_0, b_1, \ldots, b_{i-1}, b_{i+1}, \ldots, b_k \in K$ mit $b_0w + b_1v_1 + \ldots + b_{i-1}v_{i-1} + b_{i+1}v_{i+1} + \ldots + b_kv_k = 0$ und nicht alle b_j sind Null. Da B linear unabhängig ist, muss dann $b_0 \neq 0$ gelten. Es folgt:
$(a_1v_1 + \ldots + a_kv_k) + \frac{b_1}{b_0}v_1 + \ldots + \frac{b_{i-1}}{b_0}v_{i-1} + \frac{b_{i+1}}{b_0}v_{i+1} + \ldots + \frac{b_k}{b_0}v_k = 0$
Der Koeffizient von v_i liefert $a_i = 0$ ↯ qed.

6.13 Theorem: (Der Steinizsche Austauschsatz)

Sei $B = \{v_1, \ldots, v_k\}$ eine Basis von V und $C = \{w_1, \ldots, w_l\}$ eine Menge linear unabhängiger Vektoren von V.
Dann gibt es Indizes $1 \leq i_1 < \ldots < i_l \leq k$, so dass $(B \setminus \{v_{i_1}, \ldots, v_{i_l}\}) \cup \{w_1, \ldots, w_l\}$ eine Basis von V ist.
Mit anderen Worten, man kann l Vektoren einer Basis B gegen die Vektoren in C austauschen.

Beweis: Wir schließen mit vollständiger Induktion nach l
$l = 1$: Dies ist genau der im Austauschlemma behandelte Fall.
$l > 1$: Sei $\tilde{C} = \{w_1, \ldots, w_l\}$. Nach Induktionsvoraussetzung gibt es Indizes $1 \leq i_1 < \ldots < i_{l-1} \leq k$, so dass $\tilde{B} = (B \setminus \{v_{i_1} \ldots, v_{i_{l-1}}\}) \cup \tilde{C}$ eine Basis von V ist.
Wir müssen noch den Vektor w_l in die Basis $\tilde{B}$ hineintauschen und zwar gegen einen der Vektoren aus B.
OBdA seien $\{v_l, \ldots, v_k\}$ die Vektoren in $B \setminus \{v_{i_1}, \ldots, v_{i_{l-1}}\}$ (d.h. es gelte $i_1 = 1$ etc.)
Schreibe $w_l = a_1w_1 + \ldots + a_{l-1}w_{l-1} + a_lv_l + \ldots + a_kv_k$ mit $a_i \in K$.
Wäre $a_l = \ldots = a_k = 0$ so wäre die Gleichung ein Widerspruch zur vorrausgesetzten linearen Unabhängigkeit von C.
Also gibt es $j \in \{l, \ldots, k\}$ mit $a_j \neq 0$ und aus dem Beweis des Austauschlemmas folgt, dass man w_l gegen v_j in die Basis $\tilde{B}$ hineintauschen kann. Die neue Basis enthält dann C. qed.

6.14 Korollar:

Je zwei Basen von V haben gleich viele Elemente. Dieses Elementezahl heißt die Dimension von V und wird mit $dim_k(V)$ bezeichnet.

Beweis: Seien B und C zwei Basen von V. Tauscht man C mit Hilfe des Theorems in B hinein, so folgt $\#C \subseteq \#B$.
Tauscht man B mit dem Theorem in C hinein, so folgt $\#B \subseteq \#C$.
Also folgt $\#B = \#C$ qed.

Aufgrund dieses Korollars heißen endlich erzeugte Vektorräume endlich dimensional. Ist ein Vektorraum nicht endlich dimensional, so schreiben wir $dim_k(V) = \infty$.

6.15 Beispiel:

Es gilt $dim_K(K^n) = n$, denn die Standardbasis $\{e_1, \ldots, e_n\}$ hat n Elemente.

6.16 Korollar:

Sei U ein Untervektorraum von V.

(a) Es gilt $dim_K(U) \leq dim_K(V)$

(b) Jede Basis von U kann zu einer Basis von V ergänzt werden.

(c) Ist W ein weiterer Untervektorraum von V und gilt $U \subseteq W$ sowie $dim_K(U) = dim_K(W)$, so folgt $U = W$.

Beweis: (a)/(b) Wählt man eine Basis von U, so kann man sie in eine Basis von V hineintauschen. Dies beweist (a) und (b).
(c) Wähle Basen von U und W und tausche eine Basis von U in die Basis von W hinein. Aus $dim_K(U) = dim_K(W)$ folgt dann, dass die Basis von U bereits eine Basis von W ist. Somit gilt $U = W$. qed.

6.17 Definition:

Seien U, W Untervektorräume von V.
Gilt $U + W = V$ und $U \cap W = \{0\}$ so heißt V die direkte Summe von U und W. Man sagt auch, W sei ein Komplement von U in V oder U und W sind komplementär.
Schreibweise: $V = U \oplus W$

6.18 Satz:

Sei U eine Untervektorraum von V.

(a) Es gibt einen zu U komplementären Untervektorraum von V.

(b) Gilt $V = U \oplus W$, so besitzt jeder Vektor $v \in V$ eine eindeutige Darstellung $v = u + w$ mit $u \in U$ und $w \in W$.

Beweis:

(a) Wähle eine Basis $\{u_1, \ldots, u_k\}$ von U und ergänze sie zu einer Basis $\{u_1, \ldots, u_k, w_1, \ldots, w_l\}$ von V. Setze $W =< w_1, \ldots, w_l >$. Wir behaupten, dass dann $V = U \oplus W$ gilt.

$V = U + W$: Da $\{u_1, \ldots, u_k, w_1, \ldots, w_l\}$ eine Basis von V ist, besitzt jeder Vektor $v \in V$ eine Darstellung $v = a_1u_1 + \ldots + a_ku_k + b_1w_1 + \ldots + b_lw_l$ mit $a_i, b_j \in K$.
Wegen $a_1u_1 + \ldots + a_ku_k \in U$ und $b_1w_1 + \ldots + b_lw_l \in W$ folgt $v \in U + W$.

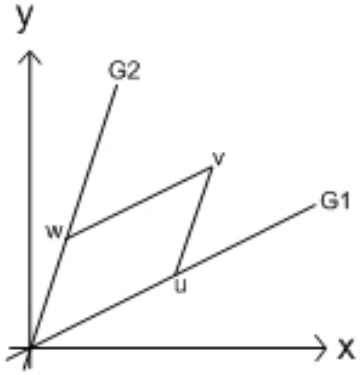
$U \cap W = \{0\}$: Sei $v \in U \cap W$. Schreibe $v = a_1u_1 + \ldots + a_ku_k$ mit $a_i \in K$ und $v = b_1w_1 + \ldots + b_lw_l$ mit $b_j \in K$. Dann folgt:
$a_1u_1 + \ldots + a_ku_k - b_1w_1 - \ldots - b_lw_l = 0$. Da $\{u_1, \ldots, u_k, w_1, \ldots, w_l\}$ eine Basis von V ist, folgt $a_1 = \ldots = a_k = b_1 = \ldots = b_l = 0$.
Insbesondere folgt $v = 0$.

(b) *Existenz:* Wegen $V = U + W$ ist die Existenz klar.

Eindeutigkeit: Sei $v \in V$ mit $v = u_1 + w_1 = u_2 + w_2$, $u_1, u_2 \in U$, $w_1, w_2 \in W$.
Dann folgt: $u_1 - u_2 = w_2 - w_1 \in U \cap W = \{0\}$, also $u_1 - u_2 = 0$ und $w_2 - w_1 = 0$.
Dies liefert $u_1 = u_2$ und $w_1 = w_2$, also die Behauptung. qed.

6.19 Beispiel:

Betrache zwei verschiedene Geraden G_1, G_2 durch O im $\mathbb{R}^2$:



Es gilt: $\mathbb{R}^2 = G_1 \oplus G_2$.
Für jeden Vektor $v \in \mathbb{R}^2$ gibt es genau eine Zerlegung $v = u + w$ mit $u \in G_1$ und $w \in G_2$.

E. Ist das alles was man über die Dimension wissen muss?

6.20 Satz: (Der Dimensionssatz)

Seien U_1, U_2 Untervektorräume von V. Dann gilt:
$dim_K(U_1 + U_2) = dim_K(U_1) + dim_K(U_2) - dim_K(U_1 \cap U_2)$

Beweis: Wähle eine Basis $\{u_1, \ldots, u_k\}$ von $U_0 = U_1 + U_2$.
Ergänze sie zu einer Basis $\{u_1, \ldots, u_k, v_1, \ldots, v_l\}$ von U_1. Ergänze sie auch zu einer Basis $\{u_1, \ldots, u_k, w_1, \ldots, w_m\}$ von U_2.
Wir zeigen nun, dass $\{u_1, \ldots, u_k, v_1, \ldots, v_l, w_1 \ldots, w_m\}$ eine Basis von $U_1 + U_2$ ist. Dann folgt die Behauptung.

Erzeugendensystem: Es gilt: $U_1 + U_2 =< u_1 \ldots, u_k, v_1, \ldots, v_l > + < u_1, \ldots, u_k, w_1, \ldots, w_m >$
$=< u_1, \ldots, u_k, v_1, \ldots, v_l, w_1 \ldots, w_m >$

Lineare Unabhängigkeit: Seien $a_i, b_j, c_\kappa \in K$ mit
$a_1u_1 + \ldots + a_ku_k + b_1v_1 + \ldots + b_lv_l + c_1w_1 + \ldots + c_mw_m = 0$
Dann folgt: $a_1u_1 + \ldots + a_ku_k + b_1v_1 + \ldots + b_lv_l = \underbrace{-c_1w_1 - \ldots - c_mw_m}_{\in U_2}$
Verwende nun, dass $< w_1, \ldots, w_m >$ ein Komplement von $U_1 \cap U_2$ ist (vgl. 6.18.a).
Aus $< w_1, \ldots, w_m > \cap (U_1 \cap U_2) = \{0\}$ folgt somit $c_1 = \ldots = c_m = 0$.
Nun ergibt sich auch $a_1 = \ldots = a_k = b_1 = \ldots = b_l = 0$. qed.

6.21 Korollar:

Sind U_1 und U_2 komplementäre Untervektorräume von V, so gilt:
$dim_K(U_1 \oplus U_2) = dim_K(U_1) + dim_K(U_2)$

Beweis: Dies folgt aus Satz 6.20 und $dim_K(U_1 \cap U_2) = dim_K(\{0\}) = 0$. qed.

6.22 Beispiel:

Seien E_1 und E_2 zwei Ursprungsebenen im $\mathbb{R}^4$.

(a) Gilt $E_1 \subseteq E_2$ oder $E_2 \subseteq E_1$, so folgt $E_1 = E_2$ und $dim_{\mathbb{R}}(E_1 \cap E_2) = 2$

(b) Ist $E_1 \neq E_2$, so gibt es zwei Möglichkeiten:

1.) $E_1 \cap E_2$ ist eine Gerade,
z.B. wenn $E_1 =< e_2, e_2 >$ und $E_2 =< e_2, e_3 >$ gilt, so ist $E_1 \cap E_2 =< e_2 >$ eine Gerade (y-Achse).

2.) $E_1 \cap E_2$ ist ein Punkt, nämlich O,
z.B. wenn $E_1 =< e_1, e_2 >$ und $E_3 =< e_3, e_4 >$ gilt, so folgt $E_1 \cap E_3 = \{0\}$.

Es folgt $dim_{\mathbb{R}}(E_1 + E_2) = 3$ und $dim_{\mathbb{R}}(E_1 + E_3) = 4$, also $\mathbb{R}^4 = E_1 \oplus E_3$.

7 Wilde Reise durch die Dimensionen (Lineare Abbildungen, ihre Kerne und Bilder)

A. Wie bitte? Homomorphismus?

Im Folgenden sei K ein Körper und V, W K-Vektorräume.

7.1 Definition:

Eine Abbildung $f : V \to W$ heißt K-linear (oder ein Homomorphismus von Vektorräumen), wenn für alle $v_1, v_2 \in V$ und alle $a_1, a_2 \in K$ gilt: $f(a_1v_1 + a_2v_2) = a_1f(v_1) + a_2f(v_2)$.
Äquivalent dazu ist, dass 1.) $f(v_1 + v_2) = f(v_1) + f(v_2)$ „Additivität“
und 2.) $f(a_1v_1) = a_1f(v_1)$ „Homogenität“
gilt.

7.2 Beispiel:

Betrachte die $\mathbb{Q}$-lineare Abbildung $f : \mathbb{Q} \to \mathbb{Q}$.
Sei $a = f(1)$. Für alle $x \in \mathbb{Q}$ gilt dann $f(x) = f(x \cdot 1) = x \cdot f(1) = ax$
Also ist f eine direkte Proportionalität.

7.3 Beispiel:

(a) Die Nullabbildung $\begin{array}{rccc} f : V & \to & V & \text{ist stets K-linear.} \\ v & \mapsto & 0 & \end{array}$

(b) Die Identität $\begin{array}{rccc} id_V : V & \to & V & \text{ist ebenfalls K-linear.} \\ v & \mapsto & v & \end{array}$

Lineare Abbildungen $f : V \to V$ heißen auch Endomorphismen von V.

7.4 Beispiel:

Sei $a \in K$. Dann ist die Homothetie (Streckung) um den Faktor a $\begin{array}{rccc} h_a : V & \to & V & \text{eine} \\ v & \mapsto & av & \end{array}$
K-lineare Abbildung, denn für $c_1, c_2 \in K$ und $v_1, v_2 \in V$ gilt:
$h_a(c_1v_1 + c_2v_2) = a(c_1v_1 + c_2v_2) = ac_1v_1 + ac_2v_2 = c_1(av_1) + c_2(av_2) = c_1h_a(v_1) + c_2h_a(v_2)$.

7.5 Beispiel:

(a) Sei $C^{(k)}(\mathbb{R})$ der $\mathbb{R}$-Vektorraum aller k-mal stetig differenzierbaren Funktionen $f : \mathbb{R} \to \mathbb{R}$ mit $k \geq 0$.
Dann ist $\begin{array}{rccc} \frac{d}{dx} : C^{(k)}(\mathbb{R}) & \to & C^{(k-1)}(\mathbb{R}) & \text{eine } \mathbb{R}\text{-lineare Abbildung.} \\ f & \mapsto & \frac{df}{dx} & \end{array}$

(b) Ebenso seien $a, b \in \mathbb{R}$ mit $a < b$. Dann ist auch $\begin{array}{rccc} \int_a^b : C^0(\mathbb{R}) & \to & \mathbb{R} & \text{eine } \mathbb{R}\text{-lineare} \\ f & \mapsto & \int_a^b f(x)dx & \end{array}$
Abbildung.

7.6 Satz:

Seien U, W Untervektorräume von V mit $V = U \oplus W$.

(a) Die Abbildung $pr_U : V \to U$ sei wie folgt definiert: Zu $v \in V$ wähle die eindeutig bestimmte Darstellung $v = u + w$ mit $u \in U$ und $w \in W$.
Dann setze $pr_U(v) = u$. Die Abbildung $pr_U : V \to U$ ist K-linear. Sie heißt die Projektion von V auf U.

(b) Ebenso definiert man die Projektion $pr_W : V \to W$. Sie ist ebenfalls K-linear.

Beweis: (a) Die Wohldefiniertheit von pr_U folgt aus Satz 6.18.b.

K-Linearität: Seien $v_1, v_2 \in V$. Schreibe $v_1 = u_1 + w_1$ und $v_2 = u_2 + w_2$ mit $u_1, u_2 \in U$ und $w_1, w_2 \in W$.
Dann ist $v_1 + v_2 = \underbrace{(u_1 + u_2)}_{\in U} + \underbrace{(w_1 + w_2)}_{\in W}$ die eindeutige Zerlegung von $v_1 + v_2$.
Es folgt: $pr_U(v_1 + v_2) = u_1 + u_2 = pr_U(v_1) + pr_U(v_2)$.
Für $a \in K$ gilt $av_1 = (au_1) + (au_2)$ und dies ist die eindeutige Zerlegung von av_1.
Somit gilt $pr_U(av_1) = au_1 = a \cdot pr_U(v_1)$ qed.

Fragen: 1.) Wie kann man einen Überblick über alle möglichen linearen Abbildungen $f : V \to W$ erhalten?
2.) Wie kann man herausfinden, ob eine lineare Abbildung injektiv/surjektiv/bijektiv ist?
3.) Wie werden Untervektorräume bei linearen Abbildungen abgebildet?

Beispiel: Ein Student will eine Party organisieren. Er kauft a_1 Artikel A_1 zum Preis von je x_1 Euro, a_2 Artikel A_2 zu je x_2 Euro, ...
Was kostet der Spaß?
Die Gesamtkosten berechnen sich mit der linearen Abbildung

$$\begin{array}{rcl} f : \mathbb{Q}^n & \to & \mathbb{Q} \\ (a_1, \ldots, a_n) & \mapsto & a_1x_1 + \ldots + a_nx_n \end{array}$$

wobei n die Anzahl der A_i bezeichne.

B. Kleine Bastelanleitung für lineare Abbildungen.

7.7 Satz:

Sei $\{v_1, \ldots, v_n\}$ eine K-Basis von V. Seien $w_1, \ldots, w_n \in W$ beliebig vorgegebene Vektoren. Dann gibt es eine K-lineare Abbildung $f : V \to W$ mit $f(v_i) = w_i$, für $i = 1, \ldots, n$.
Man kann also die Bilder der Basisvektoren von V beliebig festlegen. Dann gibt es genau eine lineare Abbildung, die die Basis wie gewünscht abbildet.

Beweis:

Existenz: Definiere f wie folgt: Ist $v \in V$ gegeben, so schreibe $v = a_1w_1 + \ldots + a_nw_n$. Offenbar erfüllt f die Behauptung $f(v_i) = w_i$ für $i = 1, \ldots, n$.
Zum Beweis der K-Linearität seien $v = a_1v_1 + \ldots + a_nv_n$ und $\tilde{v} = b_1v_1 + \ldots + b_nv_n$ mit $a_i, b_j \in K$ vorgegeben und $c, d \in K$.
Dann gilt:
$f(cv + d\tilde{v}) = f(c(a_1v_1 + \ldots + a_nv_n) + d(b_1v_1 + \ldots + b_nv_n)) = f((ca_1 + db_1)v_1 + \ldots + (ca_n + db_n)v_n)$
$= (ca_1 + db_1)w_1 + \ldots + (ca_n + db_n)w_n) = c(a_1w_1 + \ldots + a_nw_n) + d(b_1w_1 + \ldots + b_nw_n) = cf(v) + df(\tilde{v})$

Eindeutigkeit: Sei $g : V \to W$ eine K-lineare Abbildung mit $g(v_1) = w_i$ für $i = 1, \ldots, n$
Für $v = a_1v_1 + \ldots + a_nv_n$ mit $a_i \in K$ gilt dann $g(v) = a_1g(v_1) + \ldots + a_ng(v_n)$
$= a_1w_1 + \ldots + a_nw_n = f(v)$.
Da $v \in V$ beliebig war, folgt $g = f$. qed.

7.8 Beispiel:

Sei $K = \mathbb{F}_2$, $V = (\mathbb{F}_2)^3$ und $W = (\mathbb{F}_2)^4$).

(a) Jeder Vektor in V besitzt eine eindeutige Darstellung $v = a_1e_1 + a_2e_2 + a_3e_3$ mit $a_1, a_2, a_3 \in \mathbb{F}_2$. Also folgt $\#V = 8$ und $\#W = 16$.

(b) Wie viele $\mathbb{F}_2$-lineare Abbildungen $f : (\mathbb{F}_2)^3 \to (\mathbb{F}_2)^4$ gibt es?
Für $f(e_1), f(e_2)$ und $f(e_3)$ hat man jeweils 16 Wahlmöglichkeiten. Es gibt also $16^3 = 2^12 = 4096$ $\mathbb{F}_2$-lineare Abbildungen $f : (\mathbb{F}_2)^3 \to (\mathbb{F}_2)^4$.

C. Monomorphismen, Epimorphismen, Isomorphismen, Endomorphismen und Automorphismem: Es wird immer wilder!

7.9 Definition:

Sei $f : V \to W$ eine K-lineare Abbildung.

(a) Die Abbildung f heißt ein Monomorphismus, wenn f injektiv ist.

(b) Die Abbildung f heißt ein Epimorphismus, wenn f surjektiv ist.

(c) Die Abbildung f heißt ein Isomorphismus, wenn f bijektiv ist.

(d) Die Menge $Kern(f) = \{v \in V \mid f(v) = 0\}$ heißt der Kern von f.

(e) Die Menge $Bild(f) = \{w \in W \mid w = f(v) \text{ für ein } v \in V\} = f(V) = \{f(v) \mid v \in V\}$ heißt das Bild von f.

(f) Gilt $W = V$, d.h. ist f eine K-lineare Abbildung $f : V \to V$, so heißt f ein Endomorphismus von V.

(g) Ist $f : V \to V$ ein bijektiver Endomorphismus, so heißt f ein Automorphismus von V.

7.10 Satz:

(a) Die Menge $Kern(f)$ ist ein K-Untervektorraum von V.

(b) Genau dann ist f injektiv, wenn $Kern(f) = \{0\}$ gilt.

(c) Die Menge $Bild(f)$ ist ein K-Untervektorraum von W.

(d) Genau dann ist f surjetkiv, wenn $Bild(f) = W$ gilt. Ist W endlich-dimensional, so ist f also genau dann surjektiv, wenn $dim_K(Bild(f)) = dim_K(W)$ gilt.

Beweis:

(a) Verwende das Untervektorraum-Kriterium:

1.) $f(0_V) = f(0_k \cdot v) = 0_k f(v) = 0_V$, d.h. der Vektor 0_V liegt in $Kern(f)$ $(v \in V)$.

2.) Seien $v_1, v_2 \in Kern(f)$ und $a_1, a_2 \in K$.
Dann gilt $f(a_1v_1 + a_2v_2) = a_1f(v_1) + a_2f(v_2) = a_1 \cdot 0 + a_2 \cdot 0 = 0$
Also gilt $a_1v_1 + a_2v_2 \in Kern(f)$.

(b) „⇒“ Sei f injektiv. Es gilt stets $f(0_V) = 0_W$. Nach Voraussetzung ist 0_V der einzige Vektor von V, der auf 0_W abgebildet wird, d.h. es gilt $Kern(f) = \{0_W\}$.

„⇐“ Sei $v_1, v_2 \in V$ mit $f(v_1) = f(v_2)$. Dann gilt $f(v_1 - v_2) = f(v_1) - f(v_2) = 0$, also $v_1 - v_2 \in Kern(f) = \{0\}$.
Dies liefert $v_1 - v_2 = 0$ und somit ist $v_1 = v_2$.

(c) Es gilt $0_W = f(0_V) \in Bild(f)$.
Seien nun $w_1 = f(v_1) \in Bild(f)$ und $w_2 = f(v_2) \in Bild(f)$ und $a_1, a_2 \in K$.
Dann folgt: $a_1w_1 + a_2w_2 = a_1f(v_1) + a_2f(v_2) = f(a_1v_1 + a_2v_2) \in Bild(f)$.

(d) Klar nach Definition. qed.

7.11 Beispiel:

Gegeben sei eine $\mathbb{Q}$-lineare Abbildung $\begin{array}{rcl} f : \mathbb{Q}^2 & \to & \mathbb{Q}^2 \\ (a,b) & \mapsto & (3a-2b, a+b) \end{array}$.

Sie ist die eindeutig bestimmte lineare Abbildung mit $f(e_1) = (3,1)$ und $f(e_2) = (-2,1)$.

(1) Wir berechnen $Kern(f)$: Ist $(a,b) \in \mathbb{Q}^2$ mit $f(a,b) = 0$, so gilt:

$$\left\{ \begin{array}{rcrcl} 3a & - & 2b & = & 0 \\ a & + & b & = & 0 \end{array} \right. \text{ und daher } a = b = 0$$

Somit ist f injektiv.

(2) Andererseits gilt $Bild(f) =< f(e_1), f(e_2) >=< (3,1), (-2,1) >= \mathbb{Q}^2$.
Damit ist f auch surjektiv.

Folglich ist f ein $\mathbb{Q}$-Automorphismus des $\mathbb{Q}$-Vektorraums $\mathbb{Q}^2$.

7.12 Satz: (Charakterisierungen von Monomorphismen und Epimorphismen)

Sei $\{v_1, \ldots, v_n\}$ eine Basis von V, seien $w_1, \ldots, w_n \in W$ und sei $f : V \to W$ die K-lineare Abbildung mit $f(v_i) = w_i$ für $i = 1, \ldots, n$.

(a) Genau dann ist f ein Monomorphismus, wenn $w_1, \ldots, w_n$ linear unabhängig sind.

(b) Genau dann ist f ein Epimorphismus, wenn $\{w_1, \ldots, w_n\}$ ein Erzeugendensystem von W bilden.

(c) Genau dann ist f ein Isomorphismus, wenn $\{w_1, \ldots, w_n\}$ eine Basis von W ist.

Beweis:

(a) „⇒“ Sei f injektiv. Nach Satz 7.10.b gilt $Kern(f) = \{0\}$.
Seien $a_1, \ldots, a_n \in K$ mit $a_1w_1 + \ldots + a_nw_n = 0$. Aus der Rechnung
$f(a_1v_1 + \ldots + a_nv_n) = a_1f(v_1) + \ldots + a_nf(v_n) = a_1w_1 + \ldots + a_nw_n = 0$ folgt
$a_1v_1 + \ldots + a_nv_n = 0$. Die lineare Unabhängigkeit von $\{v_1, \ldots, v_n\}$ impliziert dann
$a_1 = \ldots = a_n = 0$.

„⇐“ Nach Satz 7.10.b genügt es zu zeigen, dass $Kern(f) = \{0\}$ gilt.
Sei $v \in Kern(f)$. Schreibe $v = a_1v_1 + \ldots + a_nv_n$ mit $a_i \in K$. Betrachte
$a_1w_1 + \ldots + a_nw_n = a_1f(v_1) + \ldots + a_nf(v_n) = f(a_1v_1 + \ldots + a_nv_n) = f(v) = 0$.
Die vorrausgesetzte lineare Unabhängigkeit von $w_1, \ldots, w_n$ zeigt nun $a_1 = \ldots = a_n = 0$,
also $v = 0$.

(b) „⇒“ Sei f surjektiv. Sei $w \in W$ vorgegeben. Nach Voraussetzung gibt es einen Vektor
$v \in V$ mit $f(v) = w$.
Schreibe $v = a_1v_1 + \ldots + a_nv_n$ mit $a_i \in K$. Es gilt $w = f(v) = f(a_1v_1 + \ldots + a_nv_n)$
$= a_1f(v_1) + \ldots + a_nf(v_n) = a_1w_1 + \ldots + a_nw_n \in < w_1, \ldots, w_n >$.
Da $w \in W$ beliebig war, erhalten wir $< w_1, \ldots, w_n >= W$.

„⇐“ Sei $w \in W$. Nach Voraussetzung gibt es $a_1, \ldots, a_n \in K$ mit $w = a_1w_1 + \ldots + a_nw_n$.
Setze $v = a_1v_1 + \ldots + a_nv_n$. Dann gilt
$w = a_1w_1 + \ldots + a_nw_n = a_1f(v_1) + \ldots + a_nf(v_n) = f(a_1v_1 + \ldots + a_nv_n) = f(v) \in Bild(f)$.
Da $w \in W$ beliebig war, ist f surjektiv.

(c) Folgt sofort aus (a) und (b). qed.

7.13 Korollar:

Seien V und W endlich-dimensionale K-Vektorräume. Genau dann sind V und W isomorph (d.h. es gibt einen Isomorphismus $f : V \to W$, Schreibweise: $V \cong W$), wenn $dim_K(V) = dim_K(W)$ gilt.

Beweis: „⇒“ Sei $f : V \to W$ ein Isomorphismus und $\{v_1, \ldots, v_n\}$ eine Basis von V. Nach Satz 7.12 ist dann $\{f(v_1), \ldots, f(v_n)\}$ eine Basis von W, d.h. es gilt $dim_K(V) = dim_K(W)$.

„⇐“ Wähle eine Basis $\{v_1, \ldots, v_n\}$ von V und $\{w_1, \ldots, w_n\}$ von W.
Nach Satz 7.12 ist die K-lineare Abbildung $f : V \to W$ mit $f(v_i) = w_i$ für $i = 1, \ldots, n$ ein Isomorphismus. qed.

D. Was geschieht denn mit den Dimensionen bei lineare Abbildungen?

7.14 Satz: (Der Dimensionssatz für lineare Abbildungen)

Seien V, W endlich-dimensionale K-Vektorräume und sei $f : V \to W$ eine K-lineare Abbildung.
Dann gilt: $dim_K(Bild(f)) + dim_K(Kern(f)) = dim_K(V)$

Beweis: Wir wählen eine K-Basis $\{u_1, \ldots, u_k\}$ von $Kern(f)$ und ergänzen sie zu einer Basis $\{u_1, \ldots, u_k, v_1, \ldots, v_l\}$ von V.
Es genügt zu zeigen, dass $\{f(v_1), \ldots, f(v_l)\}$ eine Basis von $Bild(f)$ darstellt.

Erzeugendensystem: Es gilt $Bild(f) =< f(u_1), \ldots, f(u_k), f(v_1), \ldots, f(v_l) >$
$=< 0, \ldots, 0, f(v_1), \ldots, f(v_l) >=< f(v_1), \ldots, f(v_l) >$.

Lineare Unabhängigkeit: Seien $b_1, \ldots, b_l \in K$ mit $b_1 f(v_1) + \ldots + b_l f(v_l) = 0$
Dann gilt: $0 = b_1 f(v_1) + \ldots + b_l f(v_l) = f(b_1 v_1) + \ldots + f(b_l v_l)$, also $b_1 v_1 + \ldots + b_l v_l \in Kern(f)$.
Somit gibt es $a_1, \ldots, a_k$ mit $b_1 v_1 + \ldots + b_l v_l = a_1 u_1 + \ldots + a_k u_k$.
Nun folgt aus $a_1 u_1 + \ldots + a_k u_k - b_1 v_1 - \ldots - b_l v_l = 0$, dass $a_1 = \ldots = a_k = b_1 = \ldots = b_l = 0$ gelten muss. qed.

7.15 Korollar:

Sei $f : V \to W$ eine K-lineare Abbildung und es gelte $dim_K(V) = dim_K(W)$. Dann sind die folgenden Bedingungen äquivalent:

(a) f ist injektiv.

(b) f ist surjektiv.

(c) f ist bijektiv.

Beweis: „(a)⇒(b)“ Ist f injektiv, dann gilt $Kern(f) = 0$ und daher $dim_K(Kern(f)) = 0$
Nach der Dimensionsformel folgt $dim_K(Bild(f)) = dim_K(V) = dim_K(W)$.
Wegen $Bild(f) \subseteq W$ zeigt dies, dass $Bild(f) = W$ gilt, d.h. dass f surjektiv ist.

„(b)⇒(c)“ Es ist nur zu zeigen, dass f injektiv ist. Aus $Bild(f) = W$ folgt
$dim_K(Bild(f)) = dim_K(W) = dim_K(V)$ und der Dimensionssatz liefert $dim_K(Kern(f)) = 0$.
Also gilt $Kern(f) = 0$, d.h. f ist injektiv.

„(c)⇒(a)“ Klar. qed.

7.16 Beispiel:

Sei $E \subseteq \mathbb{R}^3$ eine Ebene durch O und $G \subseteq \mathbb{R}^3$ eine Gerade durch O mit $G \nsubseteq E$.
Dann gilt $\mathbb{R}^3 = E \oplus G$.

(a) Für die Projektion $\begin{array}{rcl} pr_E : \mathbb{R}^3 & \to & E \\ (v_1 + v_2) & \mapsto & v_1 \end{array}$ (für $v_1 \in E, v_2 \in G$) gilt:
$Kern(pr_E) = G$ und $Bild(pr_E) = E$.
Dabei gilt $dim_{\mathbb{R}}(Kern(pr_E)) = 1$ und $dim_{\mathbb{R}}(Bild(pr_E)) = 2$.

(b) Ebenso gilt für die Projektion $pr_G : \mathbb{R}^3 \to G$ dass
$dim_{\mathbb{R}}(Kern(pr_G)) = dim_{\mathbb{R}}(E) = 2$ und
$dim_{\mathbb{R}}(Bild(pr_G)) = dim_{\mathbb{R}}(G) = 1$ ist.

E. Hat dies etwas mit LGS zu tun?

7.17 Definition:

Sei $A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$ eine $m \times n$-Matrix von Elementen von K.

(a) Betrachte die Spalten von A als Tupel $(a_{1j}, a_{2j}, \ldots, a_{mj}) \in K^m$ (mit $1 \leq j \leq n$). Sei B der von diesen Tupeln erzeugte K-Untervektorraum von K^m. Er heißt der Spaltenraum von A. Die Zahl $dim_K(B)$ heißt der Spaltenrang von A und wird mit $rang(A)$ bezeichnet.

(b) Betrachte die Zeilen von A als Tupel $(a_{i1}, \ldots, a_{in}) \in K^n$ (mit $1 \leq i \leq m$). Der von diesen Tupeln erzeugte Untervektorraum C von K^n heißt der Zeilenraum von A.
Seine Dimension $dim_K(C)$ heißt der Zeilenrang von A.

Ziel: Zeige Zeilenrang = Spaltenrang und stelle eine Verbindung zur Dimension des Lösungsraums eines LGS her!

7.18 Satz: (Dimension des Lösungsraums eines homogenen LGS)

Sei $L \subseteq K^n$ der Lösungsraum eines homogenen LGS $A \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0$

mit einer $m \times n$-Matrix $A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$.
Sei $f : K^n \to K^m$ die K-lineare Abbildung die definiert ist, durch $f(e_j) = (a_{1j}, \ldots, a_{mj}) \in K^M$ für $j = 1, \ldots, n$.

(a) Es gilt $rang(A) = dim_K(Bild(f))$.

(b) Es gilt $\mathbb{L} = Kern(f)$ und $dim_K(\mathbb{L}) = n - rang(A)$.

(c) Der Zeilenrang und der Spaltenrang von A sind gleich.

Beweis:

(a) Es gilt $Bild(f) =< f(e_1), \ldots, f(e_n) >=< (a_{11}, \ldots, a_{m1}) >$,
d.h. $Bild(f)$ ist genau der Spaltenraum von A.

(b) Für $(x_1, \ldots, x_n) \in K^n$ gilt $(x_1, \ldots, x_n) \in Kern(f)$, genau dann, wenn
$f((x_1, \ldots, x_n)) = f((x_1e_1 + \ldots + x_ne_n)) = x_1f(e_1) + \ldots + x_nf(e_n)$
$= x_1(a_{11}, \ldots, a_{m1}) + \ldots + x_n(a_{1n}, \ldots, a_{mn})$
$= (a_{11}x_1 + \ldots + a_{1n}x_n, \ldots, a_{m1}x_1 + \ldots + a_{mn}x_n) = (0, \ldots, 0)$
erfüllt ist, also genau dann, wenn $A \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0$ gilt.

Dies zeigt $Kern(f) = \mathbb{L}$.
Die zweite Behauptung folgt nun aus der Dimensionsformel:
$dim_K(Kern(f)) + dim_K(Bild(f)) = dim_K(K) \Rightarrow dim_K(\mathbb{L}) + rang(A) = n$.

(c) Wir bringen das LGS mit dem Gaußschen Verfahren in Zeilenstufenform und erhalten eine Koeffizientenmatrix der Form

$$B = \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & & \vdots \\ b_{l1} & \cdots & b_{ln} \\ 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix}$$ Mit den Zeilen $1, \ldots, l \neq 0$.

Aus der Parameterdarstellung des Lösungsraums $\tilde{\mathbb{L}}$ der neuen Matrix erhalten wir $dim_K(\tilde{\mathbb{L}}) = \underbrace{n - l}$

Zahl der Spalten ohne Pirotelement.

Bei elementaren Zeilenumformungen bleibt der Lösungsraum unverändert, d.h. es gilt $\tilde{\mathbb{L}} = \mathbb{L}$.

Da die Zeilenvektoren der Matrix in Zeilenstufenform linear unabhängig sind (vgl. 6.10.a), folgt, dass l die Dimension des Zeilenraums von B ist.

Bei den Zeilenumformungen ändert sich der Zeilenraum nicht. Daher ist l die Dimension des Zeilenraums von A und wir erhalten:

$Zeilenrang(A) = l = n - dim_K(\mathbb{L}) = rang(A)$. qed.

8 Lustiges Rechnen mit Zahlenvierecken (Matrizenrechnung)

8.1 Definition:

Sei R ein Ring (d.h. ein kommutativer Ring mit Einselement).

(a) Seien $m, n \in \mathbb{N}_+$. Eine $m \times n$-Matrix über R ist ein Zahlenviereck der Form

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \text{ mit } a_{ij} \in R.$$

Schreibweise: $A = (a_{ij})_{i,j}$ oder einfach $A = (a_{ij})$

(b) Für $i = 1, \ldots, m$ heißt $(a_{i1}, \ldots, a_{in})$ die i-te Zeile von A.

(c) Für $j = 1, \ldots, n$ heißt $\begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix}$ die j-te Spalte von A.

(d) Die Menge aller $m \times n$-Matrizen über R wird mit $Mat_{m,n}(R)$ bezeichnet.
Im Fall $m = n$ („quadratische Matrizen“) schreiben wir auch $Mat_n(R)$.

8.2 Beispiele:

Matrizen sind bequeme Mittel, um Statistiken vieler Arten darzustellen, z.B.:

(a) Temperaturen an verschiedenen Orten zu verschiedenen Zeiten.

(b) Absatzzahlen einer Firma für verschiedene Produkte in verschiedenen Märkten.

(c) Preise für verschiedene Rohstoffe bei verschiedenen Lieferanten.

Frage: Welche Matrizenoperationen sind sinnvoll?

8.3 Beispiel: (Jahresbilanz)

Eine Firma verkauft ihre Produkte P_1, P_2, P_3, P_4 in 4 Absatzmärkten M_1, M_2, M_3 wie folgt:

1. Halbjahr:

	P_1	P_2	P_3	P_4
M_1	a_{11}	a_{12}	a_{13}	a_{14}
M_2	a_{21}	a_{22}	a_{23}	a_{24}
M_3	a_{31}	a_{32}	a_{33}	a_{34}

2. Halbjahr:

	P_1	P_2	P_3	P_4
M_1	b_{11}	b_{12}	b_{13}	b_{14}
M_2	b_{21}	b_{22}	b_{23}	b_{24}
M_3	b_{31}	b_{32}	b_{33}	b_{34}

Sei $A = (a_{ij})$ und $B = (b_{ij})$. Dann ist die Jahresbilanz gegeben durch:

$$A + B = \begin{pmatrix} a_{11} + b_{11} & \cdots & a_{14} + b_{14} \\ a_{21} + b_{21} & \cdots & a_{24} + b_{24} \\ a_{31} + b_{31} & \cdots & a_{34} + b_{34} \end{pmatrix}$$

8.4 Beispiel: (Preissteigerung)

Am Ende eines Jahres erhöhe sich die Mehrwertsteuer um 2%. Die Rohstoffpreise ändern sich wie folgt (Rohstoffe R_1, R_2, R_3, Lieferanten L_1, L_2):

vorher:

	R_1	R_2	R_2
L_1	2	11	7,5
L_2	1,9	10	8

nachher:

	R_1	R_2	R_3
L_1	2,04	11,22	7,65
L_2	1,938	10,2	8,16

Die Preismatrix wird elementeweise mit 1,02 multipliziert.

8.5 Definition:

Sei R ein Ring und seien $A = (a_{ij})$ sowie $B = (b_{ij})$ zwei $m \times n$-Matrizen über R.

(a) Die Summe $A + B$ ist definiert als:

$$A + B = \begin{pmatrix} a_{11} + b_{11} & \cdots & a_{1n} + b_{1n} \\ \vdots & \ldots & \vdots \\ a_{m1} + b_{m1} & \cdots & a_{mn} + b_{mn} \end{pmatrix} = (a_{ij} + b_{ij}) \in Mat_{m,n}(R).$$

(b) Sei $\lambda \in R$. Das skalare Produkt $\lambda \cdot A$ ist definiert als:

$$\lambda \cdot A = \begin{pmatrix} \lambda a_{11} & \cdots & \lambda a_{1n} \\ \vdots & \ldots & \vdots \\ \lambda a_{m1} & \cdots & \lambda a_{mn} \end{pmatrix} = (\lambda \cdot a_{ij}) \in Mat_{m,n}(R).$$

8.6 Satz:

Ist K ein Körper, so ist die $Mat_{m,n}(K)$ mit den in 8.5 definierten Operationen ein K-Vektorraum.
Es gilt: $dim_K(Mat_{m,n}(K)) = m \cdot n$.

Beweis: Nachrechnen der Axiome, bzw. Konstruktion der Basis (vgl. Übungen). qed.

8.7 Beispiel: (Produtionsplanung: Zweistufiger Produktionsprozess)

Eine Firma stellt aus 3 Rohstoffen R_1, R_2, R_3 vier Zwischenprodukte Z_1, Z_2, Z_3, Z_4 her. Der Rohstoffverbrauch sei gegeben durch die Matrix:

$$A = \begin{array}{c} \begin{matrix} Z_1 & Z_2 & Z_3 & Z_4 \end{matrix} \\ \begin{pmatrix} 11 & 8 & 0 & 0 \\ 0 & 3 & 12 & 0 \\ 7 & 5 & 8 & 10 \end{pmatrix} \end{array} \begin{matrix} R_1 \\ R_2 \\ R_3 \end{matrix}$$ „Rohstoffproduktions-Matrix“

Aus den Zwischenprodukten werden die Endprodukte E_1, E_2 hergestellt. Die benötigte Zahl von Zwischenprodukten sei gegeben duch die Matrix:

$$B = \begin{array}{c} \begin{matrix} E_1 & E_2 \end{matrix} \\ \begin{pmatrix} 5 & 3 \\ 3 & 0 \\ 6 & 2 \\ 0 & 10 \end{pmatrix} \end{array} \begin{matrix} Z_1 \\ Z_2 \\ Z_3 \\ Z_4 \end{matrix}$$ „Zwischenprodukt-Endprodukt-Matrix“

Frage: Wieviele Rohstoffe benötigt man, um 20 Endprodukte E_1 und 25 Endprodukte E_2 herzustellen?

Sei $r = (r_1, r_2, r_3)$ der sogenannte Rohstoffvektor (Zahlen der verbrauchten Mengeneinheiten von R_i).
Und sei $z = (z_1, z_2, z_3, z_4)$ der sogenannte Zwischenproduktvektor (Zahlen der erzeugten Zwischenprodukte). Dann gilt:

$$\left\{\begin{array}{rcrcrcrcl} r_1 & = & 11z_1 & + & 8z_2 & & & & \\ r_2 & = & & & 3z_2 & + & 12z_3 & & \\ r_2 & = & 7z_1 & + & 5z_2 & + & 8z_3 & + & 10z_4 \end{array}\right. \quad \text{und somit } r = A \cdot z.$$

Gilt also $A = (a_{ij})$, so folgt $r_1 = a_{i1}z_1 + a_{i2}z_2 + a_{i3}z_3 + a_{i4}z_4$

Sei $e = (e_1, e_2)$ der Endproduktvektor (Zahlen der produzierten Endprodukte). Dann gilt:

$$\left\{\begin{array}{rcrcrcl} z_1 & = & 5e_1 & + & 3e_2 & & \\ z_2 & = & 3e_1 & & & & \\ z_3 & = & 6e_1 & + & 2e_2 & & \\ z_4 & = & & & 10e_2 & & \end{array}\right. \quad \text{also } z = B \cdot e \text{ mit } B = (b_{ij}) \in Mat_{4,2}(\mathbb{Q}).$$

Einsetzen dieser Gleichungen liefert:
$r_i = a_{i1}(b_{11}e_1 + b_{12}e_2) + a_{i2}(b_{21}e_1 + b_{22}e_2) + a_{i3}(b_{31}e_1 + b_{32}e_2) + a_{i4}(b_{41}e_1 + b_{42}e_2)$
$= \underbrace{(a_{i1}b_{11} + a_{i2}b_{21} + a_{i3}b_{31} + a_{i4}b_{41})}_{c_{i1}} e_1 + \underbrace{(a_{i1}b_{12} + a_{i2}b_{22} + a_{i3}b_{32} + a_{i4}b_{42})}_{c_{i2}} e_2$
Also folgt: $r = C \cdot e$ mit einer Matrix $C = (c_{ij}) \in Mat_{3,2}(\mathbb{Q})$ wobei gilt:
$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + a_{i3}b_{3j} + a_{i4}b_{4j}$
Wir nennen $C = A \cdot B$ das Matrizenprodukt von A und B. Es gilt:

$$AB = \begin{pmatrix} 79 & 33 \\ 82 & 24 \\ 98 & 137 \end{pmatrix} \text{ und für } e = (20, 25) \text{ folgt:}$$

$$r = (AB)e = \begin{pmatrix} 79 & 33 \\ 82 & 24 \\ 98 & 137 \end{pmatrix} \cdot \begin{pmatrix} 20 \\ 25 \end{pmatrix} = \left.\begin{pmatrix} 2405 \\ 2220 \\ 5385 \end{pmatrix}\right\} \text{benötigte Rohstoffe.}$$

8.8 Definition:

Sei R ein Ring und seien $A = (a_{ij}) \in Mat_{m,l}(R)$ sowie $B = (b_{ij}) \in Mat_{l,n}(R)$ zwei Matrizen über R. [Die Spaltenzahl von A muss also gleich der Zeilenzahl von B sein!]
Dann ist das Matrizenprodukt $A \cdot B$ die Matrix $A \cdot B = (c_{ij}) \in Mat_{m,n}(R)$ mit den Einträgen $c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \ldots + a_{il}b_{lj}$ für $i = 1, \ldots, m$ und $j = 1, \ldots, n$.

Regel: Um c_{ij} zu errechnen, bilde das Produkt der i-ten Zeile von A mit der j-ten Zeile von B:

$$A = \begin{pmatrix} \vdots & & \\ a_{i1} & \cdots & a_{il} \\ \vdots & & \end{pmatrix}, \; B = \begin{pmatrix} & b_{1j} & \\ \ldots & \vdots & \ldots \\ & b_{lj} & \end{pmatrix} \Rightarrow A \cdot B = \begin{pmatrix} & \vdots & \\ \cdots & a_{i1}b_{1j} + \ldots + a_{il}b_{lj} & \cdots \\ & \vdots & \end{pmatrix}$$

8.9 Satz: (Eigenschaften des Matrizenprodukts)

Seien A, B, C Matrizen „passender Größe“ , Also $A \in Mat_{k,l}(R), B \in Mat_{l,m}(R)$, und $C \in Mat_{m,n}(R)$.

(a) Es gilt $(A \cdot B) \cdot C = A \cdot (B \cdot C)$ (Assoziativgesetz)

(b) Ist $\tilde{A} \in Mat_{k,l}(R)$ eine weitere Matrix, so gilt:
$(A + \tilde{A}) \cdot B = A \cdot B + \tilde{A} \cdot B$ (erstes Distributivgesetz)

(c) Ist $\tilde{B} \in Mat_{l,m}(R)$ eine weitere Matrix, so gilt:
$A \cdot (B + \tilde{B}) = A \cdot B + A \cdot \tilde{B}$ (zweites Distributivgesetz)

(d) Die $l \times l$-Einheitsmatrix $I_l = \begin{pmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 1 & 0 \\ 0 & \cdots & \cdots & 0 & 1 \end{pmatrix} = (\delta_{ij})$
↖„Hauptdiagonale“

erfüllt $A \cdot I_l = A$ und $B \cdot I_l = B$ $(I_l \in Mat_{l,l}(R))$.

Beweis: Wir rechnen nur (c) nach.

Sei $A = (a_{ij})$ und $B = (b_{ij})$ und $\tilde{B} = (\tilde{b}_{ij})$. Dann gilt:
$A \cdot (B + \tilde{B}) = (a_{ij})_{i,j} \cdot (b_{j\kappa} + \tilde{b}_{j\kappa})_{j,\kappa}$
$= (a_{i1}(b_{1\kappa} + \tilde{b}_{1\kappa}) + \ldots + a_{il}(b_{l\kappa} + \tilde{b}_{l\kappa}))_{i,\kappa}$
$= (a_{i1}b_{1\kappa} + \ldots + a_{il}b_{l\kappa} + a_{i1}\tilde{b}_{1\kappa} + \ldots + a_{il}\tilde{b}_{l\kappa})_{i,\kappa}$
$= ((a_{i1}b_{1\kappa} + \ldots + a_{il}b_{l\kappa})_{i,\kappa} + (a_{i1}\tilde{b}_{1\kappa} + \ldots + a_{il}\tilde{b}_{l\kappa})_{i,\kappa} = A \cdot B + A \cdot \tilde{B}$ qed.

8.10 Korollar:

Die Menge $Mat_n(R)$ ist ein Ring (der Matrizenring).
Für $n \geq 2$ ist dieser Ring nicht kommutativ.

Beweis: Die Ringaxiome folgen aus Satz 8.9.

$n = 2$: Betrachte $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ und $B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. Dann gilt:

$A \cdot B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ und $B \cdot A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$

$n < 2$: Betrachte $A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$ und $B = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & & & \vdots \\ \vdots & & & \vdots \\ 0 & \cdots & \cdots & 0 \end{pmatrix}$. qed.

Im Folgenden sei stets K ein Körper. Der Ring $Mat_n(K)$ ist für $n \geq 2$ kein Körper.

8.11 Definition:

Eine Matrix $A \in Mat_n(K)$ heißt invertierbar wenn es eine Matrix $B \in Mat_n(K)$ gibt mit $A \cdot B = B \cdot A = I_n$.

Schreibweise: $A^{-1} = B$ heißt die inverse Matrix (die Inverse) von A (Hierbei ist $I_n = (\delta_{ij}) \in Mat_n(K)$ die n-te Einheitsmatrix).

8.12 Beispiele:

(a) Die Matrix $A = \begin{pmatrix} -2 & 4 \\ 0 & 1 \end{pmatrix} \in Mat_2(\mathbb{Q})$ ist invertierbar, denn:

$$\begin{pmatrix} -2 & 4 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -\frac{1}{2} & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ und } \begin{pmatrix} -\frac{1}{2} & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -2 & 4 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Also folgt: $A^{-1} = \begin{pmatrix} -\frac{1}{2} & 2 \\ 0 & 1 \end{pmatrix}$

(b) Die Matrix $B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ ist nicht invertierbar, denn:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \text{ liefert } 0 = 1 \lightning$$

8.13 Satz:

Sei $n \geq 1$ und $A \in Mat_n(K)$.

(a) Ist A invertierbar, so ist A^{-1} eindeutig bestimmt.

(b) Gibt es eine Linksinverse zu A, d.h. gibt es eine Matrix $B \in Mat_n(K)$ mit $B \cdot A = I_n$, so ist A invertierbar und B ist die Inverse ($B = A^{-1}$).

(c) Gibt es eine Rechtsinverse zu A, d.h. gibt es eine Matrix $B \in Mat_n(K)$ mit $A \cdot B = I_n$, so ist A invertierbar und B ist die Inverse ($B = A^{-1}$).

(d) Ist A invertierbar, so ist auch A^{-1} invertierbar und $(A^{-1})^{-1} = A$.

(e) Sind $A, B \in Mat_n(K)$ invertierbar, so ist auch $A \cdot B$ invertierbar und es gilt $(A \cdot B)^{-1} = B^{-1} \cdot A^{-1}$

Beweis:

(a) Seien $B_1, B_2 \in Mat_n(K)$ mit $AB_1 = B_1A = I_n$ und $AB_2 = B_2A = I_n$.
Dann gilt: $B_1 = B_1 \cdot I_n = B_1(AB_2) = (B_1A)B_2 = I_n \cdot B_2 = B_2 \lightning$

(b) vgl. Übungen

(c) vgl. Übungen

(d) Es gilt $A(A^{-1}) = (A^{-1})A = I_n$. Daher gilt: $B(A^{-1}) = (A^{-1})B = I_n$ für $B = A$, d.h. A^{-1} ist invertierbar und $(A^{-1})^{-1} = A$.

(e) Es gilt $(AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AI_nA^{-1} = AA^{-1} = I_n$
und $(B^{-1}A^{-1})(AB) = B^{-1}(A^{-1}A)B = B^{-1}I_nB = B^{-1}B = I_n$.
Somit ist $B^{-1}A^{-1}$ invers zu AB. qed.

B. Wie berechnet man die inverse Matrix?

Im Folgenden sei K ein Körper.

8.14 Definition:

Sei $n \geq 1$.

(a) Für $1 \leq i < j \leq n$ definieren wir die Matrix

$$P_{i,j} = \begin{pmatrix}
 & & & \mathrm{i} & & & & \mathrm{j} & & & & \\
1 & & & \vdots & & & & \vdots & & & & \\
 & \ddots & & \vdots & & & & \vdots & & & & \\
 & & 1 & \vdots & & & & \vdots & & & & \\
\cdots & \cdots & \cdots & 0 & \cdots & \cdots & \cdots & 1 & \cdots & \cdots & \cdots & \mathrm{i} \\
 & & & \vdots & 1 & & & \vdots & & & & \\
 & & & \vdots & & \ddots & & \vdots & & & & \\
 & & & \vdots & & & 1 & \vdots & & & & \\
\cdots & \cdots & \cdots & 1 & \cdots & \cdots & \cdots & 0 & \cdots & \cdots & \cdots & \mathrm{j} \\
 & & & \vdots & & & & \vdots & 1 & & & \\
 & & & \vdots & & & & \vdots & & \ddots & & \\
 & & & \vdots & & & & \vdots & & & 1 &
\end{pmatrix}$$

als „Permutationsmatrix“ oder Elementarmatrix vom Typ P.

(b) Sei $\lambda \in K \setminus \{0\}$ und $1 \leq i \leq n$. Dann heißt

$$D_{i,\lambda} = \begin{pmatrix}
 & & & \mathrm{i} & & & & \\
1 & & & \vdots & & & & \\
 & \ddots & & \vdots & & & & \\
 & & 1 & \vdots & & & & \\
\cdots & \cdots & \cdots & \lambda & \cdots & \cdots & \cdots & \mathrm{i} \\
 & & & \vdots & 1 & & & \\
 & & & \vdots & & \ddots & & \\
 & & & \vdots & & & 1 &
\end{pmatrix}$$

eine „Diagonalmatrix“ oder Elementarmatrix vom Typ D.

(c) Sei $\lambda \in K \setminus \{0\}$ und $i, j \in \{1, \ldots, n\}$ mit $i \neq j$. Dann heißt

$$E_{i,j,\lambda} = \begin{array}{c} \\ \\ \\ \\ \\ \\ \\ \end{array} \begin{array}{c} \text{j} \\ \\ \\ \\ \\ \\ \text{i} \end{array} \begin{pmatrix} 1 & & & & \vdots & & \\ & \ddots & & & \vdots & & \\ \cdots & \cdots & 1 & \cdots & \lambda & \cdots & \\ & & & \ddots & \vdots & & \\ & & & & \vdots & 1 & \end{pmatrix}$$

eine Elementarmatrix vom Typ E.

8.15 Satz:

Sei $A \in Mat_{n,l}(K)$ und sei $B \in Mat_n(K)$ eine Elementarmatrix. Dann entsteht die Matrix BA aus A, indem man die entsprechende elementare Zeilenoperation ausführt.

Beweis: *Typ P:* Multipliziert man die erste Zeile $(1, 0, \ldots, 0)$ von $P_{i,j}$ mit A, so ist das Ergebnis $(a_{11}, \ldots, a_{1l})$, d.h. die erste Zeile wird reproduziert.
Ganz allgemein gilt $e_k \cdot A = (a_{k1}, \ldots, a_{kl})$ für $k = a, \ldots, n$.
Die i-te Zeile von $P_{i,j} \cdot A$ ist die j-te Zeile von A und die j-te Zeile von $P_{i,j} \cdot A$ ist die i-te Zeile von A.
Für $k \neq i$ ist die k-te Zeile von $P_{i,j} \cdot A$ gerade die k-te Zeile von A.
Also sind bei der Berechnung von $P_{i,j} \cdot A$ gerade die i-te und j-te Zeile von A vertauscht worden.

Typ D: Für $\lambda \in K$ gilt $\lambda e_k \cdot A = (\lambda a_{k1}, \ldots, \lambda a_{kl})$. Das bedeutet also, dass bei der Berechnung von $D_{i,\lambda} \cdot A$ alle Zeilen von A außer der i-ten unverändert bleiben und die i-te Zeile von A mit λ multipliziert wird.

Typ E: Bei der Berechnung von $E_{i,j,\lambda} \cdot A$ werden alle Zeilen von A außer der i-ten unverändert gelassen.
Die i-te Zeile von $E_{i,j,\lambda} \cdot A$ ist $(e_i + \lambda e_{ij}) \cdot A = (a_{i1}, \ldots, a_{il}) + (\lambda a_{j1}, \ldots, \lambda a_{jl})$
$= (a_{i1} + \lambda a_{j1}, \ldots, a_{il} + \lambda ajl)$.
Somit wurde zur i-ten Zeile von A das λ-fache der j-ten Zeile addiert. qed.

8.16 Korollar:

Multipliziert man eine Matrix $A \in Mat_{l,n}(K)$ von rechts mit einer Elementarmatrix $B \in Mat_n(K)$, so entsteht die Matrix $AB \in Mat_{l,n}(K)$ aus A, indem man die entsprechende elementare Spaltenoperation durchführt.

8.17 Satz:

(a) Für $1 \leq i < j \leq n$ gilt $(P_{i,j})^{-1} = P_{i,j}$.

(b) Für $\lambda \in K \setminus \{0\}$ und $1 \leq i \leq n$ gilt $(D_{i,\lambda})^{-1} = D_{i,\frac{1}{\lambda}}$.

(c) Für $\lambda \in K \setminus \{0\}$ und $i, j \in \{1, \ldots, n\}$ mit $i \neq j$ gilt $(E_{i,j,\lambda})^{-1} = E_{i,j,-\lambda}$.

8.18 Satz:

Jede invertierbare Matrix ist darstellbar als das Produkt von Elementarmatrizen.

Beweis: Sei A eine invertierbare $n \times n$-Matrix. Wir bringen A mit Hilfe des Gauß-Verfahrens in reduzierte Zeilenstufenform.
Dabei gilt $B = M_1 \cdots M_r \cdot A$ mit Elementarmatrizen $M_1, \ldots, M_r$. Da A und $M_1, \ldots, M_r$ invertierbar sind, ist nach Satz 8.13.e auch B invertierbar.
Wir behaupten nun $b_{ij} \neq 0$ für $i = 1, \ldots, n$.

Wir schließen durch vollständige Induktion nach i. Sei $B^{-1} = (c_{ij})$.

$\underline{i = 1}$ Es gilt $B^{-1} \cdot B = \begin{pmatrix} b_{11}c_{11} & \cdots & b_{1n}c_{1n} \\ & & \\ & * & \end{pmatrix} = I_n$

Also folgt $b_{11} = c_{11} = 1$ und $c_{12} = \ldots = c_{1n} = 0$.

$\underline{i > 1}$ Angenommen es gilt $b_{ij} = 0$. Dann ist der i-te Spaltenvektor $(b_{1i}, \ldots, b_{i-1,i}, 0, \ldots, 0)$ einer der Einheitsvektoren in $\{e_1, \ldots, e_{i-1}\}$ oder der Nullvektor. Also könnte man den Spaltenraum von B mit $n-1$ Vektoren erzeugen, d.h. es gilt $rang(B) \leq n-1$.
Betrachte nun $B \cdot B^{-1} = I_n$. Seien $v_1, \ldots, v_n$ die Spaltenvektoren von B. Die j-te Spalte von $B \cdot B^{-1}$ ist $c_{1j}v_1 + \ldots + c_{nj}v_n$.
Daher liegen die Spaltenvektoren von $B \cdot B^{-1}$ im Spaltenraum von B. Die Spaltenvektoren von $B \cdot B^{-1} = I_n$ sind die Einheitsvektoren, die den K^n erzeugen. Also ist der Spaltenraum von $B \cdot B^{-1}$ der K^n. $\lightning$ (zu $rang(B) \leq n-1$)

Insgesamt folgt $B = I_n = M_1 \cdots M_r \cdot A$.
Somit ist $A = M_r^{-1} \cdots M_1^{-1}$ ein Produkt von Elementarmatrizen. qed.

8.19 Korollar: (Berechnung der inversen Matrix)

Gegeben sei eine invertierbare Matrix $A = (a_{ij}) \in Mat_n(K)$.

(a) Bilde die zusammengesetzte Matrix

$$(A \mid I_n) = \left(\begin{array}{ccc|ccc} a_{11} & \cdots & a_{1n} & 1 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} & 0 & \cdots & 1 \end{array}\right) \in Mat_{n,2n}(K).$$

(b) Führe elementare Zeilenoperationen durch, bis auf der linken Seite die Einheitsmatrix steht. Es entsteht eine Matrix der Form

$$(I_n \mid B) = \left(\begin{array}{ccc|ccc} 1 & \cdots & 0 & b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 1 & b_{n1} & \cdots & b_{nn} \end{array}\right)$$

(c) Dann gilt $A^{-1} = (b_{ij})$.

Beweis: Nach Satz 8.18 gilt $A = M_r^{-1} \cdots M_1^{-1}$ wobei die Matrizen M_i den durchzuführenden elementaren Zeilenoperationen entsprechen. Dann gilt: $A^{-1} = M_1 \cdots M_r \cdot I_n$.
Somit kann man A^{-1} berechnen, indem man an I_n genau dieselben Zeilenoperationen durchführt wie an A. qed.

8.20 Beispiel:

Sei $a \in \mathbb{Q} \setminus \{1, -1\}$. Wir berechnen die Inverse der Matrix $A = \begin{pmatrix} 1 & a \\ a & 1 \end{pmatrix}$

1.) Bilde $\left(\begin{array}{cc|cc} 1 & a & 1 & 0 \\ a & 1 & 0 & 1 \end{array}\right) \in Mat_{2,4}(\mathbb{Q})$

2.) Berechne

$$\left(\begin{array}{cc|cc} 1 & a & 1 & 0 \\ 0 & 1-a^2 & -a & 1 \end{array}\right) \rightsquigarrow \left(\begin{array}{cc|cc} 1 & a & 1 & 0 \\ 0 & 1 & -\frac{a}{1-a^2} & \frac{1}{1-a^2} \end{array}\right) \rightsquigarrow \left(\begin{array}{cc|cc} 1 & 0 & \frac{1}{1-a^2} & -\frac{a}{1-a^2} \\ 0 & 1 & -\frac{a}{1-a^2} & \frac{1}{1-a^2} \end{array}\right)$$

3.) Die Inverse von A ist $A^{-1} = \frac{1}{1-a^2} \begin{pmatrix} 1 & -a \\ -a & 1 \end{pmatrix}$

8.21 Korollar:

Die Menge der invertierbaren $n \times n$-Matrizen über K bildet eine Gruppe bezüglich der Matrizenmultiplikation. Sie heißt die allgemeine lineare Gruppe über K und wird mit $GL_n(K)$ bezeichnet.
Die Gruppe $GL_n(K)$ wird von den Elementarmatrizen erzeugt.

C. Was kann man mit Matrizen sonst noch anfangen?

Man kann sie transponieren.

8.22 Definition:

Sei R ein Ring und $A = (a_{ij}) \in Mat_{m,n}(R)$. Dann heißt die Matrix

$$A^{tr} = \begin{pmatrix} a_{11} & a_{21} & \cdots & a_{m1} \\ a_{12} & a_{22} & \cdots & a_{m2} \\ \vdots & \vdots & & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{mn} \end{pmatrix} \in Mat_{n,m}(R)$$

die Transponierte von A. Die Zeilen von A sind also die Spalten von A^{tr} und die Spalten von A sind die Zeilen von A^{tr}.

8.23 Satz: (Eigenschaften der transponierten Matrix)

Seien $A, B \in Mat_{m,n}(R)$ und $C \in Mat_{n,l}(R)$.

(a) $(A^{tr})^{tr} = A$

(b) $(A + B)^{tr} = A^{tr} + B^{tr}$

(c) Für $\lambda \in R$ gilt $(\lambda A)^{tr} = \lambda \cdot A^{tr}$

(d) $(A \cdot C)^{tr} = C^{tr} \cdot A^{tr}$

(e) $rang(A^{tr}) = rang(A)$

(f) Genau dann ist A invertierbar, wenn auch A^{tr} invertierbar ist (im Fall $m = n$).
In diesem Fall gilt $(A^{tr})^{-1} = (A^{-1})^{tr}$

Beweis:

(a) klar

(b) klar

(c) klar

(d) Der (ij)-Eintrag von AC ist $a_{i1}c_{1j} + \ldots + a_{in}c_{nj}$. Der (ij)-Eintrag von $(AC)^{tr}$ ist also $a_{j1}c_{1i} + \ldots + a_{jn}c_{ni}$ und dies ist dann genau der (ij)-Eintrag von $(C^{tr})(A^{tr}) = (c_{ji})(a_{ji}) = (c_{1i}a_{j1} + \ldots + c_{ni}a_{jn})$.

(e) Folgt aus $Zeilenrang(A) = Spaltenrang(A)$.

(f) Folgt aus (d), denn $A^{tr} \cdot (A^{-1})^{tr} = (A^{-1} \cdot A)^{tr} = I_n^{tr} = I_n$ und $(A^{-1})^{tr} \cdot A^{tr} = (AA^{-1})^{tr} = I_n^{tr} = I_n$. qed.

9 Basis, wechsle dich!

A. Was haben Matrizen mit linearer Algebra zu tun?

Sei K einer Körper, sei V ein endlich-dimensionaler K-Vektorraum mit Basis $B = \{v_1, \ldots, v_n\}$, sei W ein endlich-dimensionaler K-Vektorraum mit Basis $C = \{w_1, \ldots, w_m\}$ und sei $f : V \to W$ eine K-lineare Abbildung.

9.1 Definition:

(a) Für $i = 1, \ldots, n$ schreibe $f(v_i) = a_{1i}w_1 + \ldots + a_{mi}w_m$ mit $a_{1i}, \ldots, a_{mi} \in K$. Dann bilden wir die Matrix $A = (a_{ij}) \in Mat_{m,n}(K)$. Mit anderen Worten, die Matrix A hat die Koordinatentupel der Bilder der Basisvektoren von V in ihren Spalten.
Dann heißt A die Darstellungsmatrix von f bezüglich der Basen B und C und wird mit $M_C^B(f)$ bezeichnet.

(b) Sei nun umgekehrt eine Matrix $A = (a_{ij}) \in Mat_{m,n}(K)$ gegeben.
Dann gibt es eine eindeutig bestimmte K-lineare Abbildung $f_A : V \to W$ mit $f_A(v_j) = a_{1j}w_1 + \ldots + a_{mj}w_m$. Sie heißt die bezüglich der Basen B und C zu f assoziierte K-lineare Abbildung.

9.2 Satz:

(a) Die beiden Zuordnungen $f \mapsto M_C^B(f)$ und $A \mapsto f_A$ sind invers zueinander.

(b) Ist $g : V \to W$ eine weitere K-lineare Abbildung dann gilt $M_C^B(f + g) = M_C^B(f) + M_C^B(g)$.

(c) Für $\lambda \in K$ gilt $M_C^B(\lambda f) = \lambda M_C^B(f)$.

(d) Sei $\tilde{A} \in Mat_{m,n}(K)$ eine weitere Matrix. Dann gilt $f_{A+\tilde{A}} = f_A + f_{\tilde{A}}$.

(e) Für $\lambda \in K$ gilt $f_{\lambda A} = \lambda f_A$.

(f) Die Abbildungen $M_C^B : Hom_K(V, W) \to Mat_{m,n}(K)$, $f \mapsto M_C^B(f)$ und
$(-)_A : Mat_{m,n}(K) \to Hom_K(V, W)$, $A \mapsto f_A$ sind invers zueinander und definieren einen Isomorphismus von K-Vektorräumen.
(Beachte: Dieser Isomorphismus hängt von der Wahl der Basen B und C ab!)

Beweis:

(a) klar

(b) Es gilt $(f + g)(v_j) = f(v_j) + g(v_j)$. Schreibe $M_C^B(f) = (a_{ij})$ und $M_C^B(g) = (b_{ij})$.
Dann folgt $(f + g)(v_j) = (a_{1j}w_1 + \ldots + a_{mj}w_m) + (b_{1j}w_1 + \ldots + b_{mj}w_m)$
$= (a_{1j} + b_{1j})w_1 + \ldots + (a_{mj} + b_{mj})w_m$.
Dies zeigt $M_C^B(f + g) = (a_{ij} + b_{ij})_{i,j} = (a_{ij}) + (b_{ij}) = M_C^B(f) + M_C^B(g)$.

(c) Es gilt $(\lambda f)(v_j) = \lambda f(v_j) = \lambda(a_{1j}w_1 + \ldots + a_{mj}w_m) = (\lambda a_{1j})w_1 + \ldots + (\lambda a_{mj})w_m$.
Dies zeigt $M_C^B(\lambda f) = (\lambda a_{ij}) = \lambda(a_{ij}) = \lambda M_C^B(f)$.

(d) Für $i = 1, \ldots, n$ gilt $f_{A+\tilde{A}}(v_j) = (a_{1j} + \tilde{a}_{1j})w_1 + \ldots + (a_{mj} + \tilde{a}_{mj})w_m$
denn $A + \tilde{A} = (a_{ij} + \tilde{a}_{ij})$ für $A = (a_{ij})$ und $\tilde{A} = (\tilde{a}_{ij})$.
Nun folgt $f_{A+\tilde{A}}(v_j) = (a_{1j}w_1 + \ldots + a_{mj}w_m) + (\tilde{a}_{1j}w_1 + \ldots + \tilde{a}_{mj}w_m) = f_A(v_j) + f_{\tilde{A}}(v_j)$.
Für einen beliebigen Vektor $v = c_1v_1 + \ldots + c_nv_n \in V$ mit $c_i \in K$ folgt wegen der Linearität von $f_A, f_{\tilde{A}}$ und $f_{A+\tilde{A}}$ dann $f_{A+\tilde{A}}(v) = f_{A+\tilde{A}}(c_1v_1 + \ldots + c_nv_n)$
$= c_1f_{A+\tilde{A}}(v_1) + \ldots + c_nf_{A+\tilde{A}}(v_n)$
$= c_1(f_A(v_1) + f_{\tilde{A}}(v_1)) + \ldots + c_n(f_A(v_n) + f_{\tilde{A}}(v_n))$
$= c_1f_A(v_1) + \ldots + c_nf_A(v_n) + c_1f_{\tilde{A}}(v_1) + \ldots + c_nf_{\tilde{A}}(v_n)$
$= f_A(c_1v_1 + \ldots + c_nv_n) + f_{\tilde{A}}(c_1v_1 + \ldots + c_nv_n) = f_A(v) + f_{\tilde{A}}(v)$.

(e) Für $i = 1, \ldots, n$ gilt $f_{\lambda A}(v_j) = (\lambda a_{1j})w_1 + \ldots + (\lambda a_{mj})w_m$
$= \lambda(a_{1j}w_1 + \ldots + a_{mj}w_m) = \lambda f_A(v_j)$.
Wegen der Linearität von f_A und $f_{\lambda A}$ folgt dann $f_{\lambda A}(v) = \lambda f_A(v)$ für alle $v \in V$.

(f) Folgt aus (a) - (e) qed.

9.3 Beispiele:

(a) Für die Nullabbildung $\begin{array}{rcl} 0 : V & \to & W \\ v & \mapsto & 0 \end{array}$ gilt $M_C^B(0) = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix}$

(b) Für die Abbildung $\begin{array}{rcl} id_V : V & \to & V \\ v_j & \mapsto & v_j \end{array}$ gilt $M_B^B(id_V) = \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix} = I_n$

denn $v_j = 0 \cdot v_1 + \ldots + 0 \cdot v_{j-1} + 1 \cdot v_j + 0 \cdot v_{j+1} + \ldots + 0 \cdot v_n$

(c) Sei $K = \mathbb{Q}$ und $V = [x]_{\leq 5}$ der Vektorraum der Polynome vom Grad ≤ 5 in der Variablen x, d.h. der Vektorraum aller Elemente $a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + a_5x^5$ mit $a_i \in \mathbb{Q}$.
Dieser Vektorraum hat die $\mathbb{Q}$-Basis $\{1, x, x^2, \ldots, x^5\}$ und erhält somit $dim_{\mathbb{Q}}(V) = 6$.
Die Darstellungsmatrix der $\mathbb{Q}$-linearen Abbildung

$$\begin{array}{rcl} \frac{d}{dx} : V & \to & V \\ f & \mapsto & f' \end{array} \text{ bezüglich der Basis } B \text{ ist } M_B^B(\tfrac{d}{dx}) = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 5 \end{pmatrix}$$

9.4 Beispiel:

Sei $f : K^n \to K^m$ eine K-lineare Abbildung und seien $E = \{e_1, \ldots, e_n\}$ bzw. $\tilde{E} = \{\tilde{e}_1, \ldots, \tilde{e}_m\}$ die Standardbasen von K^n bzw. K^m. Schreibe $f(e_j) = a_{1j}\tilde{e}_1 + \ldots + a_{mj}\tilde{e}_m = (a_{1j}, \ldots, a_{mj})$.
Wenn man also die Darstellungsmatrix $M_{\tilde{E}}^E(f)$ bildet, braucht man nur die Bilder der Standardbasisvektoren in die Spalten von $M_{\tilde{E}}^E(f)$ zu setzen.

Ziel: Untersuche wie sich die Eigenschaften von linearen Abbildungen in ihren Darstellungsmatrizen wiederspiegeln!

9.5 Satz:

Sei $f : V \to W$ eine K-lineare Abbildung mit Darstellungsmatrix $M_C^B(f)$. Dann gilt:

(a) $rang(M_C^B(f)) = dim_K(Bild(f))$
Diese Zahl hängt somit nicht von der Wahl der Basen B von V und C von W ab. Sie heißt auch der Rang von f und wird mit $rang(f)$ bezeichnet.

(b) Genau dann ist $f : V \to V$ ein Isomorphismus, wenn $A = M_B^B(f)$ invertierbar ist. Dies ist auch äquivalent mit $rang(f) = n$.

Beweis:

(a) Der Rang von $M_C^B(f) = (a_{ij})$ ist der Spaltenrang, d.h. die Dimension des von den Spaltenvektoren $(a_{11}, \ldots, a_{m1}), \ldots, (a_{1n}, \ldots, a_{mn})$ erzeugten Untervektorraums von K^n.
Nun verwenden wir den Isomorphismus von K-Vektorräumen $\Phi : K^m \to W$ und $e_i \mapsto w_i$
bestimmen das Bild des Spaltenrangs und Φ. Es gilt:

$\Phi((a_{1j}, \ldots, a_{mj})) = a_{1j}e_1 + \ldots + a_{mj}e_m = a_{1j}\Phi(e_1) + \ldots + a_{mj}\Phi(e_m)$
$= a_{1j}w_1 + \ldots + a_{mj}w_m = f(v_j)$.
Somit ist das Bild des Spaltenrangs von $M_C^B(f)$ unter Φ genau $Bild(f)$ und die Behauptung folgt.

(b) 1.) Sei g ein Isomorphismus. Dann gibt es eine K-lineare Abbildung $g^{-1} : V \to V$ mit $g \circ g^{-1} = id_V$. Aufgrund des nachfolgenden Satzes gilt
$M_B^B(g \circ g^{-1}) = M_B^B(g) \cdot M_B^B(g^{-1}) = M_B^B(id_V) = I_n$.
Entsprechend gilt $I_n = M_B^B(id_V) = M_B^B(g^{-1} \circ g) = M_B^B(g^{-1}) \cdot M_B^B(g)$.
Daher ist $A = M_B^B(g)$ invertierbar und $A^{-1} = M_B^B(g^{-1})$.

2.) Sei $A = M_B^B(g)$ invertierbar. Aus $A \cdot A^{-1} = I_n$ und der Tatsache, dass die Spaltenvektoren von $A \cdot A^{-1}$ Linearkombinationen der Spaltenvektoren von A sind, folgt $n = rang(I_n) = rang(A \cdot A^{-1}) \leq rang(A)$.
Dies zeigt $rang(A) = n \underset{\text{(a)}}{=} rang(g)$.

3.) Gilt $rang(g) = n$, so ist g ein Epimorphismus. Nach Korollar 7.15 ist g somit ein Isomorphismus. qed.

9.6 Satz:

Seien $f : V \to W$ und $g : W \to U$ zwei K-lineare Abbildungen, sei $B = \{v_1, \ldots, v_n\}$ eine Basis von V, $C = \{w_1, \ldots, w_m\}$ eine Basis von W und $D = \{u_1, \ldots, u_l\}$ eine Basis von U.
Dann gilt: $M_D^B(g \circ f) = M_D^C(g) \cdot M_C^B(f)$

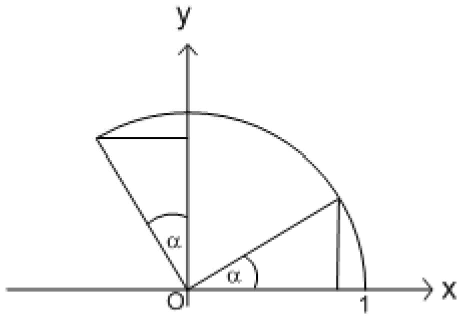
Beweis: Sei $A = M_C^B(f) = (a_{ij})$ und $\tilde{A} = M_D^C(g) = (b_{ij})$.
Betrachte $(g \circ f)(v_j) = g(a_{1j}w_1 + \ldots + a_{mj}w_m) = a_{1j}g(w_1) + \ldots + a_{mj}g(w_m)$
$= a_{1j}(b_{11}u_1 + \ldots + b_{l1}u_l) + \ldots + a_{mj}(b_{1m}u_1 + \ldots + b_{lm}u_l)$
$= (a_{1j}b_{11} + \ldots + a_{mj}b_{1m})u_1 + \ldots + (a_{1j}b_{l1} + \ldots + a_{mj}b_{lm})u_l$

Somit ist das Koordinatentupel von $(g \circ f)(v_j)$ in der Basis D gerade die j-te Spalte der Matrix $\tilde{A} \cdot A = (b_{i1}a_{1j} + \ldots + b_{im}a_{mj})_{i,j}$ qed.

9.7 Beispiel:

Sei $K = \mathbb{R}$, $V = \mathbb{R}^2$ und $B = C = \{e_1, e_2\}$
Seien $\alpha, \beta \in [0, 2\pi[$. Die lineare Abbildung $f_\alpha : \mathbb{R}^2 \to \mathbb{R}^2$ mit der Darstellungsmatrix
$M_C^B(f_\alpha) = \begin{pmatrix} cos(\alpha) & -sin(\alpha) \\ sin(\alpha) & cos(\alpha) \end{pmatrix}$ ist die Drehung um O um den Winkel α.
$\qquad\qquad f_\alpha(e_1) \quad f_\alpha(e_2)$

Skizze:



Es gilt: $M_B^B(f_\beta \circ f_\alpha) = \begin{pmatrix} cos(\alpha) & -sin(\alpha) \\ sin(\alpha) & cos(\alpha) \end{pmatrix} \cdot \begin{pmatrix} cos(\beta) & -sin(\beta) \\ sin(\beta) & cos(\beta) \end{pmatrix}$

$$= \begin{pmatrix} cos(\alpha)cos(\beta) - sin(\alpha)sin(\beta) & -cos(\alpha)sin(\beta) - sin(\alpha)cos(\beta) \\ sin(\alpha)cos(\beta) + cos(\alpha)sin(\beta) & -sin(\alpha)sin(\beta) + cos(\alpha)cos(\beta) \end{pmatrix}$$

$$= \begin{pmatrix} cos(\alpha+\beta) & -sin(\alpha+\beta) \\ sin(\alpha+\beta) & cos(\alpha+\beta) \end{pmatrix} = M_B^B(f_{\alpha+\beta})$$

Also ist $f_\beta \circ f_\alpha$ die Drehung um O um den Winkel $\alpha + \beta$.

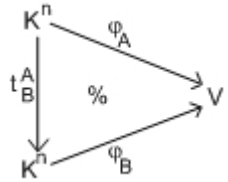
B. Was passiert mit der Darstellungsmatrix einer linearen Abbildung, wenn man sie bezüglich anderer Basen bestimmt?

Sei K einer Körper, sei V ein endlich-dimensionaler K-Vektorraum mit Basis $B = \{v_1, \ldots, v_n\}$, sei W ein endlich-dimensionaler K-Vektorraum mit Basis $C = \{w_1, \ldots, w_m\}$ und sei $f : V \to W$ eine K-lineare Abbildung.

9.8 Bemerkung:

(a) Die K-lineare Abbildung $\varphi_B : K^n \to V$ mit $\varphi_B(e_i) = v_i$ für $i = 1, \ldots, n$ ist ein Isomorphismus von Vektorräumen.
Für ein Tupel $(a_1, \ldots, a_n) \in K^n$ gilt $\varphi_B((a_1, \ldots, a_n)) = a_1v_1 + \ldots + a_nv_n$. Die Abbildung φ_B heißt das durch B bestimmte Koordinatensystem in V.
(Es gilt $M_B^E(\varphi_B) = I_n$ mit $E = \{e_1, \ldots, e_n\}$.)

(b) Sei $A = \{u_1, \ldots, u_n\}$ eine weitere Basis von V. Dann hat man ein Diagramm von Isomorphismen:



mit $t_B^A = \varphi_B^{-1} \circ \varphi_A$.

Die Abbildung t_B^A heißt der Basiswechsel von A nach B.

Sei $T_B^A = M_E^E(t_B^A)$ die Darstellungsmatrix des Basiswechsels bezüglich der Standardbasis. Sie heißt die Transformationsmatrix des Basiswechsels.

9.9 Satz: (Berechnung der Transformationsmatrix)

(a) In der Situation von Bemerkung 9.8.b schreibe $v_j = c_{1j}u_1 + \ldots + c_{nj}u_n$ mit $c_{ij} \in K$ für $i = 1, \ldots, n$.
Bilde die Matrix $C = (c_{ij}) \in Mat_n(K)$. Dann ist C invertierbar und es gilt $T_B^A = C^{-1}$.

(b) Es gilt $(T_B^A)^{-1} = T_A^B$. Insbesondere kann man T_B^A berechnen, indem man $u_j = d_{1j}v_1 + \ldots + d_{nj}v_n$ schreibt mit $d_{ij} \in K$ für $j = 1, \ldots, n$ und $T_B^A = (d_{ij})$ setzt.

(c) Ist $v \in V$ und $v = a_1u_1 + \ldots + a_nu_n$ die Darstellung von v in der Basis A, sowie $v = b_1v_1 + \ldots + b_nv_n$ die Darstellung von v in der Basis B, so gilt also:

$$\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = T_B^A \cdot \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$$

Beweis:

(a) Sei $\gamma : K^n \to K^n$ die lineare Abbildung mit $M_E^E(\gamma) = C$. Für $j = 1, \ldots, n$ gilt dann:
$(\varphi_A \circ \gamma)(e_j) = \varphi_A((c_{1j}, \ldots, c_{nj})) = c_{1j}u_1 + \ldots + c_{nj}u_n = v_j = \varphi_B(e_j)$
Also folgt $(\varphi_A \circ \gamma) = \varphi_B$ und $\gamma = \varphi_A^{-1} \circ \varphi_B = (\varphi_B^{-1} \circ \varphi_A)^{-1} = (t_B^A)^{-1}$.

(b) Folgt aus $t_A^B = \varphi_A^{-1} \circ \varphi_B = (\varphi_B^{-1} \circ \varphi_A)^{-1} = (t_B^A)^{-1}$.

(c) klar qed.

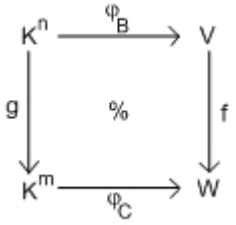
9.10 Beispiel:

Sei $K = \mathbb{Q}$ und $V = \mathbb{Q}^2$ mit den Basen $E = \{e_1, e_2\}$ und $B = \{v_1, v_2\}$ gegeben mit $v_1 = (2, 1)$ und $v_2 = (1, 3)$. Dann gilt: $v_1 = 2e_1 + e_2$ und $v_2 = e_1 + 3e_2$, also

$T_E^B = \begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix}$ Nun folgt: $T_B^E = (T_E^B)^{-1} = \begin{pmatrix} \frac{3}{5} & -\frac{1}{5} \\ -\frac{1}{5} & \frac{2}{5} \end{pmatrix}$

9.11 Bemerkung:

(a) Betrachte das Diagramm K-linearer Abbildungen:



Dieses Diagramm ist kommutativ,
d.h. es gelte $\varphi_C \circ g = f \circ \varphi_B$,
also $g = (\varphi_C)^{-1} \circ f \circ \varphi_B$.

Für die Darstellungsmatrix $M_E^E(g)$ gilt:
$M_E^E(g) = (\underbrace{M_E^C(\varphi_C)}_{I_m})^{-1} \cdot M_C^B(f) \cdot \underbrace{M_B^E(\varphi_B)}_{I_n}$ und somit $M_E^E(g) = M_C^B(f)$.

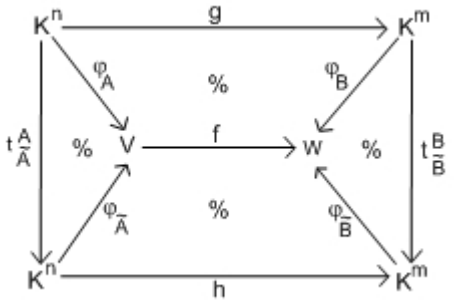
(b) Im Fall $V = W$ und $f = id_V$ folgt $g = \varphi_C^{-1} \circ \varphi_B = t_C^B$ und $M_E^E(g) = T_C^B = M_C^B(id_V)$.
Darstellungsmatrizen linearer Abbildungen verallgemeinern also Transformationsmatrizen.

9.12 Satz: (Die Basis-Transformationsformel)

Sei $f : V \to W$ eine K-lineare Abbildung, seien $A, \tilde{A}$ Basen von V und $B, \tilde{B}$ Basen von W.

Dann gilt: $M_{\tilde{B}}^{\tilde{A}}(f) = T_{\tilde{B}}^B \cdot M_B^A(f) \cdot (T_{\tilde{A}}^A)^{-1} = T_{\tilde{B}}^B \cdot M_B^A(f) \cdot T_A^{\tilde{A}}$

Beweis: Betrachte das folgende Diagramm:



Dabei gilt $M_E^E(g) = M_B^A(f)$ und $M_E^E(h) = M_{\tilde{B}}^{\tilde{A}}(f)$ nach Bemerkung 9.11.

Nach Bemerkung 9.8.b sind die beiden Dreiecke kommutativ. Nach 9.11 sind die beiden Trapeze kommutativ. Dann ist auch das große Quadrat kommutativ.
Für die Darstellungsmatrizen bedeutet dies:
$T_{\tilde{B}}^B \cdot M_B^A(f) = M_{\tilde{B}}^{\tilde{A}} \cdot T_{\tilde{A}}^A$ qed.

9.13 Korollar:

Sei $f : V \to V$ ein Endomorphismus und seien $A, \tilde{A}$ Basen von V. Dann gilt:
$M_{\tilde{A}}^{\tilde{A}} = T_{\tilde{A}}^A \cdot M_A^A(f) \cdot T_A^{\tilde{A}}$

9.14 Korollar:

(a) Zu jeder K-linearen Abbildung $f : K^n \to K^M$ gibt es Basen A von K^n und B von K^m, so dass gilt:

$$M_B^A(f) = \left(\begin{array}{ccc|c} 1 & \cdots & 0 & \\ \vdots & \ddots & \vdots & 0 \\ 0 & \cdots & 1 & \\ \hline & & & \\ & 0 & & 0 \\ & & & \end{array}\right) \left.\begin{array}{c}\\\\\\\\\\\end{array}\right\} r$$

wobei $r = rang(f)$ gilt.

(b) Zu jeder $m \times n$-Matrix $M \in Mat_{m,n}(K)$ gibt es invertierbare Matrizen $A \in Mat_n(K)$ und $B \in Mat_m(K)$, so dass $\tilde{M} = B \cdot M \cdot A^{-1}$ die in (a) angegebene Gestalt besitzt.

Beweis:

(a) Es gilt $n - r = dim_K(Kern(f))$.
Wähle eine Basis $\{v_{r+1}, \ldots, v_n\}$ von $Kern(f)$ und ergänze sie zu einer Basis $A = \{v_1, \ldots, v_r, v_{r+1}, \ldots, v_n\}$ von V. Dann ist $\{f(v_1), \ldots, f(v_r)\}$ eine Basis von $Bild(f)$.
Setze $w_i = f(v_i)$ für $i = 1, \ldots, r$ und ergänze $\{w_1, \ldots, w_r\}$ zu einer Basis $B = \{w_1, \ldots, w_r, w_{r+1}, \ldots, w_m\}$ von W.
Dann besitzt $M_B^A(f)$ die angegebene Gestalt.

(b) Folgt aus (a) und Satz 9.12. qed.

9.15 Beispiele:

Für eine Abbildung $f : \mathbb{Q}^2 \to \mathbb{Q}^2$ gelte $M_E^E(f) = \begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix}$

Wir bringen $M_E^E(f)$ mit Zeilen- und Spaltenumformungen in die gewünschte Gestalt:

1.) Addiere das (-2)-fache der ersten Zeile zur zweiten:

$$\begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$

2.) Addiere das (-2)-fache der ersten Spalte zu zweiten:

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Insgesamt folgt: $\underbrace{\begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}}_{\in GL_2(\mathbb{Q})} \cdot \begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix} \cdot \underbrace{\begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}}_{\in GL_2(\mathbb{Q})} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

9.16 Definition:

Seien $A, B \in Mat_{m,n}(K)$

(a) Die beiden Matrizen A und B heißen äquivalent, wenn es invertierbare Matrizen $S \in GL_m(K)$ und $T \in GL_n(K)$ gibt mit $B = SAT^{-1}$.

(b) Sei nun $m = n$ und seien $A, B \in Mat_n(K)$.
Die beiden Matrizen heißen ähnlich, wenn es eine invertierbare Matrix $T \in GL_n(K)$ gibt mit $B = TAT^{-1}$.

9.17 Korollar:

(a) Zwei Matrizen sind genau dann äquivalent, wenn sie bezüglich verschiedener Paare von Basen dieselbe lineare Abbildung beschreiben.

(b) Zwei Matrizen aus $Mat_{m,n}(K)$ sind genau dann äquivalent, wenn sie den gleichen Rang haben.

(c) Jede Matrix von Rang r ist äquivalent zu

$$\left(\begin{array}{ccc|c} 1 & \cdots & 0 & \\ \vdots & \ddots & \vdots & 0 \\ 0 & \cdots & 1 & \\ \hline & & & \\ & 0 & & 0 \\ & & & \end{array}\right) \Bigg\} r$$

(d) Zwei quadratische Matrizen aus $Mat_n(K)$ sind genau dann ähnlich, wenn sie Darstellungsmatrizen $M_A^A(f)$ bzw. $M_B^B(f)$ des gleichen Endomorphismus bezüglich zwei Basen A und B sind.

Bemerkung: Nicht jede quadratische Matrix ist ähnlich zu I_n

Äquivalenzen und Ähnlichkeiten von Matrizen sind Äquivalenzrelationen.

Kapitel III: In der Bredouille

10 Alle sind gleich, aber einer ist gleicher (Äquivalenzrelationen)

10.1 Definition:

Sei M eine Menge.

(a) Eine Relation auf M ist eine Teilmenge R von $M \times M$.
Gilt $(a, b) \in R$, so schreiben wir auch $a \sim_R b$ (oder einfach $\sim$) und sagen „a steht bezüglich R in Relation zu b“.

(b) Eine Relation R heißt reflexiv, wenn für alle $a \in M$ gilt: $a \sim a$.

(c) Eine Relation R heißt symmetrisch, wenn für $a, b \in M$ aus $a \sim b$ folgt, dass auch $b \sim a$ gilt.

(d) Eine Relation R heißt transitiv, wenn für $a, b, c \in M$ aus $a \sim b$ und $b \sim c$ folgt, dass auch $a \sim c$ gilt.

(e) Eine Relation R, die reflexiv, symmetrisch und transitiv ist, ist eine Äquivalenzrelation auf M.

10.2 Beispiele:

(a) Die Gleichheitsrelation auf M ist eine Äquivalenzrelation. Sie ist gegeben durch die Teilmenge $\{(a, a) \in M \times M \mid a \in M\}$ von $M \times M$.

(b) Die Relation $\leq$ auf $\mathbb{Q}$ ist reflexiv und transitiv, aber nicht symmetrisch.

(c) Die Relation $>$ auf $\mathbb{Z}$ ist transitiv, aber weder reflexiv noch symmetrisch.

(d) Sei $n \geq 1$. Die Relation $R = \{\{(a, b)\} \in \mathbb{Z}^2 \mid a \equiv b(mod\ n)\}$ ist eine Äquivalenzrelation:

1.) $a \equiv a(modn)$, denn $0 = a - a \in n\mathbb{Z}$
2.) Gilt $a \equiv b(mod\ n)$, so folgt auch $b \equiv a(mod\ n)$
3.) Gilt $a \equiv b(mod\ n)$ und $b \equiv c(mod\ n)$, so folgt aus $a - b \in n\mathbb{Z}$ und $b - c \in n\mathbb{Z}$, dass auch $a - c = (a - b) + (b - c) \in n\mathbb{Z}$ gilt, also $a \equiv c(mod\ n)$

10.3 Beispiele:

Sei K ein Körper und $m, n \geq 1$.

(a) Für $A, B \in Mat_{m,n}(K)$ sei $A \sim B$ („A ist äquivalent zu B“), genau dann, wenn es invertierbare Matrizen S und T gibt, mit $B = SAT^{-1}$. Dann ist $\sim$ eine Äquivalenzrelation:

1.) $A \sim A$, denn $A = I_m \cdot A \cdot (I_n)^{-1}$
2.) Gilt $A \sim B$, also $B = SAT^{-1}$, so folgt $A = S^{-1}BT$, also $A = \tilde{S}B\tilde{T}^{-1}$ mit $\tilde{S} = S^{-1}$ und $\tilde{T} = T^{-1}$.
Somit erhalten wir $B \sim A$.
3.) Gilt $A \sim B$ und $B \sim C$, also $B = SAT^{-1}$ und $C = \tilde{S}B\tilde{T}^{-1}$, so folgt $C = (\tilde{S}S)A(T^{-1}\tilde{T}^{-1}) = (\tilde{S}S)A(\tilde{T}T)^{-1}$.
Dies zeigt $A \sim C$.

(b) Für $A, B \in Mat_n(K)$ sei $A \sim_S B$ genau dann, wenn es ein $T \in GL_n(K)$ gibt, mit $B = TAT^{-1}$ („A ist ähnlich zu B“). Dann ist auch $\sim_S$ eine Äquivalenzrelation.

Im Folgenden sei stets R eine Äquivalenzrelation auf einer Menge M.

10.4 Definition:

Für ein Element $a \in M$ heißt $[a]_R = \{b \in M \mid a \sim b\}$ die Äquivalenzklasse von a bezüglich R.

10.5 Satz:

(a) Für $a, b \in M$ gilt $[a]_R = [b]_R$ genau dann, wenn $a \sim b$ erfüllt ist.

(b) Jedes Element von M ist in genau einer Äquivalenzklasse enthalten.

(c) Die Menge M ist die disjunkte Vereinigung der Äquivalenzklassen.

Beweis:

(a) „$\Rightarrow$“ Aus $[a]_R = [b]_R$ folgt wegen $b \in [b]_R$, dass $b \in [a]_R$ ist und somit $a \sim b$.

„$\Leftarrow$“ „$\subseteq$“ Aus $a \sim b$ folgt $b \sim a$ und somit $a \in [b]_R$.
Ist $c \in [a]_R$, also $a \sim c$, so gilt $b \sim c$ nach der Transitivität und somit $c \in [b]_R$.
Da c beliebig war, folgt $[a]_R \subseteq [b]_R$.

„$\supseteq$“ Analog.

(b) *Existenz:* $a \in [a]_R$, denn $a \sim a$.

Eindeutigkeit: Sei $a \in [b]_R$ und $a \in [c]_R$. Dann gilt $a \sim b$ und $a \sim c$. Wegen der Symmetrie folgt $b \sim a$ und die Transitivität liefert $b \sim c$. Nach (a) ergibt sich $[b]_R = [c]_R$.

(c) *Vereinigung:* Folgt aus $a \in [a]_R$.

Disjunktheit: Folgt aus (b) qed.

10.6 Beispiel:

Sei $n \geq 1$ und $R \subseteq \mathbb{Z} \times \mathbb{Z}$ die Relation $\{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a \equiv b (mod\ n)\}$.
Für ein festes $a \in \mathbb{Z}$ gilt $a \sim b$ genau dann, wenn $b - a \in n\mathbb{Z}$ erfüllt ist, also genau für alle $b \in a + n\mathbb{Z}$. Somit folgt $[a]_R = a + n\mathbb{Z}$.
Es gilt $\mathbb{Z} = (0 + n\mathbb{Z}) \cup (1 + n\mathbb{Z}) \cup \ldots \cup (n - 1 + n\mathbb{Z})$.
Es gibt genau die n Äquivalenzklassen $[0]_R, [1]_R, \ldots, [n-1]_R$. Die Menge der Äquivalenzklassen ist also $\mathbb{Z}/n\mathbb{Z}$.

10.7 Definition:

(a) Die Menge aller Äquivalenzklassen von M bezüglich R wird mit $M/\sim_R$ bezeichnet (sprich „M modulo R“).

(b) Ist $[a]_R \in M/\sim_R$, so heißt jedes Element $b \in [a]_R$ ein Repräsentant der Äquivalenzklasse $[a]_R$.

(c) Die Abbildung $\begin{array}{ccc} M & \to & M/\sim \\ a & \mapsto & [a]_R \end{array}$ ist surjektiv. Sie heißt die kanonische surjektive Abbildung von M in die Menge der Äquivalenzklassen.

10.8 Beispiele:

(a) Sei $n \geq 1$ und $R = \{(a,b) \in \mathbb{Z}^2 \mid a \equiv b(mod\ n)\}$.
Dann gilt $\mathbb{Z}/\sim_R = \mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$. Die Zahlen $0, 1, \ldots, n-1$ sind die kleinsten, nicht negativen Repräsentanten dieser Restklassen.

(b) Sei K ein Körper und $\sim$ die Äquivalenzrelation von Matrizen in $Mat_n(K)$. Dann gilt:

$Mat_n(K)/\sim =$

$$\left\{ \left[\begin{pmatrix} 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix} \right], \left[\begin{pmatrix} 1 & \cdots & \cdots & 0 \\ \vdots & 0 & & \vdots \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & \cdots & 0 \end{pmatrix} \right], \left[\begin{pmatrix} 1 & \cdots & \cdots & \cdots & 0 \\ \vdots & 1 & & & \vdots \\ \vdots & & 0 & & \vdots \\ \vdots & & & \ddots & \vdots \\ 0 & \cdots & \cdots & \cdots & 0 \end{pmatrix} \right], \ldots, \left[\begin{pmatrix} 1 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 1 \end{pmatrix} \right] \right\}$$

{Nullmatrix} {Matrizen vom Rang 1} {Matrizen vom Rang 2} {Invertierbare Matrizen}

Somit gibt es genau $n+1$ Äquivalenzklassen.

10.9 Bemerkung:

(a) Interessant ist besonders der Fall, dass $M/\sim_R$ eine algebraische Struktur besitzt.
Z.b. ist $\mathbb{Z}/n\mathbb{Z}$ ein Ring.

(b) Wir suchen in Äquivalenzklassen häufig nach einem kanonischen Repräsentanten.
Z.b. sind $0, 1, \ldots, n-1$ kanonische Repräsentanten in der Äquivalenzklasse von $\mathbb{Z}/n\mathbb{Z}$.

11 Buntes Treiben in Gruppen

A. Was war gleich noch 'mal ne Gruppe?

11.1 Definition:

Eine Menge G zusammen mit einer Verknüpfung $\circ : G \times G \to G$ heißt eine Gruppe, wenn gilt:

(a) Für alle $a, b, c \in G$ gilt $(a \circ b) \circ c = a \circ (b \circ c)$. (Assoziativgesetz)

(b) Es gibt ein $e \in G$ mit $e \circ a = a \circ e = a$ für alle $a \in G$. (neutrales Element)

(c) Für jedes $a \in G$ gibt es ein $a^{-1} \in G$ mit $a^{-1} \circ a = a \circ a^{-1} = e$. (inverse Elemente)

Eine Gruppe heißt kommutativ (oder abelsch), wenn für alle $a, b \in G$ gilt $a \circ b = b \circ a$.

B. Ja gibt's denn so 'was?

11.2 Beispiele:

(a) $(\mathbb{Z}, +)$ ist eine kommutative Gruppe.

(b) $(\mathbb{Q} \setminus \{0\}, \cdot)$ ist eine kommutative Gruppe.

(c) $(Mat_{m,n}(K), +)$ ist eine kommutative Gruppe.

(d) $(GL_n(K), \cdot)$ ist eine Gruppe, die aber für $n \geq 2$ nicht kommutativ ist.

11.3 Beispiel: (Die symmetrische Gruppe S_n)

(a) Eine lineare Abbildung $\varphi : \{1, \ldots, n\} \to \{1, \ldots, n\}$ heißt eine Permutation der Menge $\{1, \ldots, n\}$. Wir schreiben φ auch in der Form

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \varphi(1) & \varphi(2) & \cdots & \varphi(n) \end{pmatrix}$$

(b) Die Menge S_n aller Permutationen von $\{1, \ldots, n\}$ ist eine Gruppe bezüglich der Komposition (Hintereinanderausführung) von Abbildungen

$$\begin{array}{rccl} \circ : & S_n \times S_n & \to & S_n \qquad (\text{„}\varphi \text{ nach } \psi\text{“}) \\ & (\varphi, \psi) & \mapsto & (\varphi \circ \psi) \end{array}$$

(c) Die Gruppe S_n ist für $n \geq 3$ nicht kommutativ:

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

(d) Die Gruppe S_n besitzt $n!$ Elemente (Für $\varphi(1)$ gibt es n Möglichkeiten, für $\varphi(2)$ gibt es danach noch $n - 1$ Möglichkeiten, ...)

11.4 Bemerkung: (Gruppentafeln)

Man kann eine endliche Gruppe $G = \{g_1, \ldots, g_n\}$ auch durch ihre Gruppentafel beschreiben. Dies ist eine $m \times n$-Matrix über G, an deren (ij)-Eintrag das Ergebnis von $g_i \circ g_j$ steht.

(a) Gruppentafel von $S_1 = \{e\}$:

$\circ$	e
e	e

(b) Gruppentafel von $S_2 = \{e, \tau\}$ mit $\tau = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ („Transposition“):

$\circ$	e	τ
e	e	τ
τ	τ	e

In einer Gruppentafel kommt jedes Element in jeder Zeile und in jeder Spalte genau einmal vor.

(c) Gruppentafel von $S_3 = \{e, \tau_1, \tau_2, \tau_3, \sigma_1, \sigma_2\}$ mit:

$$\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$\circ$	e	τ_1	τ_2	τ_3	σ_1	σ_2
e	e	τ_1	τ_2	τ_3	σ_1	σ_2
τ_1	τ_1	e	σ_1	σ_2	τ_2	τ_3
τ_2	τ_2	σ_2	e	σ_1	τ_3	τ_1
τ_3	τ_3	σ_1	σ_2	e	τ_1	τ_2
σ_1	σ_1	τ_3	τ_1	τ_2	σ_2	e
σ_2	σ_2	τ_2	τ_3	τ_1	e	σ_1

$$\tau_1 \circ \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

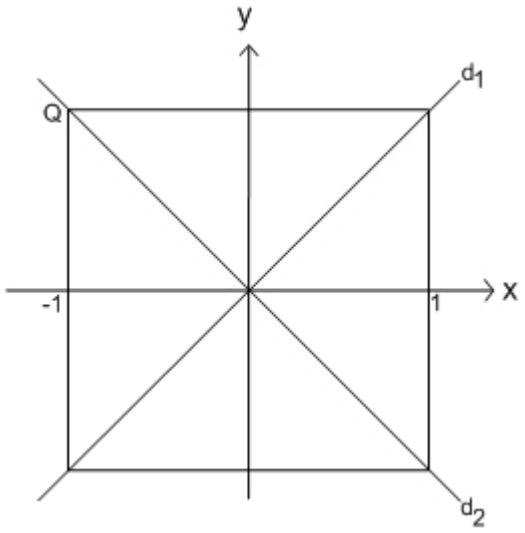
$$\tau_2 \circ \tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

11.5 Beispiel: (Symmetriegruppen)

(a) Die Menge der Kongruenzabbildungen der Ebene $\mathbb{R}^2$ ist bezüglich der Komposition eine Gruppe. Kongruenzabbildungen sind Kompositionen von Drehungen, Spiegelungen und Translationen.

(b) Sei $M \subseteq \mathbb{R}^2$ eine Teilmenge. Die Symmetriegruppe $Sym(M)$ ist die Menge aller Kongruenzabbildungen $\varphi : \mathbb{R}^2 \to \mathbb{R}^2$ mit $\varphi(M) = M$.

(c) Als Beispiel betrachten wir das Quadrat
$Q = \{(x, y) \in \mathbb{R}^2 \mid (|x| = 1 \text{ und } |y| \leq 1) \text{ oder } (|x| \leq 1 \text{ und } |y| = 1)\}$
Skizze:



Wir untersuchen die Quadratgruppe $Sym(Q)$: Sie Enthält:

1.) Die Identität e
2.) τ_1, die Spiegelung an d_1
3.) τ_2, die Spiegelung an d_2
4.) τ_3, die Spiegelung an der x-Achse
5.) τ_4, die Spiegelung an der y-Achse
6.) σ_1, die Drehung um 90° um O
7.) σ_2, die Drehung um 180° um O (Punktspiegelung an O)
8.) σ_3, die Drehung um $-90°$ um O

Gruppentafel:

$\circ$	e	τ_1	τ_2	τ_3	τ_4	σ_1	σ_2	σ_3
e	e	τ_1	τ_2	τ_3	τ_4	σ_1	σ_2	σ_3
τ_1	τ_1	e	σ_2	σ_1	$\cdots$			
τ_2	τ_2	$\vdots$						
$\vdots$	$\vdots$	$\vdots$						

Diese Gruppe heißt auch die vierte Diedergruppe D_4.

(d) Man kann entsprechend auch Symmetriegruppen von Teilmengen von $\mathbb{R}^3$ definieren. Z.b. besitzt die Symmetriegruppe des Würfels 48 Elemente.

C. Kann eine Teilmenge einer Gruppe wieder eine Gruppe sein?

Im Folgenden sei G eine Gruppe mit Verknüpfung $\circ$ und neutralem Element e.

11.6 Definition:

Eine Teilmenge $U \subseteq G$ heißt Untergruppe, wenn U bezüglich der Verknüpfung $\circ$ selbst eine Gruppe ist.

11.7 Satz: (Das Untergruppenkriterium)

Eine Teilmenge $U \subseteq G$ ist genau dann eine Untergruppe, wenn die folgenden Bedingungen erfüllt sind:

(a) $U \neq \emptyset$

(b) Aus $a \in U$ folgt $a^{-1} \in U$

(c) Aus $a, b \in U$ folgt $a \circ b \in U$

Beweis: Wenn U eine Untergruppe ist, sind (a)-(c) offensichtlich erfüllt.

Sie nun (a)-(c) erfüllt. Wegen (c) ist $\circ : U \times U \to U$ eine wohldefinierte Abbildung.
Die Assoziativität der Verknüpfung auf U folgt aus der aus G. Nach (a) gibt es ein Element $a \in U$. Nach (b) gibt es dann auch $a^{-1} \in U$. Nach (c) folgt $e = a \circ a^{-1} \in U$. Also besitzt U das neutrale Element e. Nach (b) gibt es in U inverse Elemente. qed.

11.8 Beispiele:

(a) Für $n \geq 1$ ist $n\mathbb{Z}$ eine Untergruppe von $\mathbb{Z}$ bezüglich $+$.

(b) $\{1, -1\} \subseteq \mathbb{R} \setminus \{0\}$ ist eine Untergruppe von $(\mathbb{R} \setminus \{0\}, \cdot)$.

(c) Sei $\tau = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 2 & 1 & 3 & \cdots & n \end{pmatrix} \in S_n$. Dann ist $T = \{e, \tau\}$ eine Untergruppe von S_n.

(d) Ist $M \subseteq \mathbb{R}^2$, so ist $Sym(M)$ eine Untergruppe der Gruppe der Kongruenzabbildungen von $\mathbb{R}^2$.

11.9 Definition:

Sei $U \subseteq G$ eine Untergruppe.
Für jedes $a \in G$ heißt $aU = \{au \mid u \in U\}$ die (Links-)Nebenklasse von a bezüglich U.

11.10 Satz:

Sei $U \subseteq G$ eine Untergruppe.

(a) Für $a, b \in G$ gilt $aU = bU$ genau dann, wenn $b^{-1} \circ a \in U$ gilt.

(b) Die Relation $\{(a, b) \in G \times G \mid aU = bU\}$ ist eine Äquivalenzrelation auf G. Insbesondere ist G die disjunkte Vereinigung der Nebenklassen bezüglich U.

(c) Für jedes $a \in G$ ist die Abbildung $\begin{array}{ccc} U & \to & aU \\ u & \mapsto & au \end{array}$ bijektiv.
Wenn G endlich ist, haben also alle Nebenklassen bezüglich U dieselbe Elementezahl.

Beweis:

(a) „$\Rightarrow$“ Aus $aU = bU$ folgt $a = a \circ e \in bU$, d.h. es gibt ein $u \in U$ mit $a = b \circ u$. Multiplikation mit b^{-1} liefert $b^{-1} \circ a = b^{-1} \circ b \circ u = e \circ u = u \in U$.

„$\Leftarrow$“ „$\subseteq$“ Aus $b^{-1} \circ a \in U$ folgt $a \in bU$ und somit $aU \subseteq bU$

„$\supseteq$“ Schreibe $b^{-1} \circ a = u$ mit $u \in U$. Dann folgt $a = b \circ u$ und somit $b = a \circ u^{-1} \in aU$. Dies zeigt $bU \subseteq aU$.

(b) *Reflexivität:* Für alle $a \in G$ gilt $aU = aU$.

Symmetrie: Für $a, b \in G$ folgt aus $aU = bU$, dass auch $bU = aU$ gilt.

Transitivität: Für $a, b, c \in G$ folgt aus $aU = bU$ und $bU = cU$, das auch $aU = cU$ gilt.

(c) *Injektivität:* Sei $u, \tilde{u} \in U$ mit $a \circ u = a \circ \tilde{u}$. Multipliziere von links mit a^{-1} und erhalte $u = a^{-1} \circ (a \circ u) = a^{-1} \circ (a \circ \tilde{u}) = \tilde{u}$.

Surjektivität: Klar nach Definition von aU. qed.

11.11 Definition:

Sei $U \subseteq G$ eine Untergruppe.

(a) Die Menge der Nebenklassen bezüglich U wird mit G/U bezeichnet (sprich „G modulo U“ oder „G nach U“).

(b) Ist $\#(G/U)$ endlich, so heißt $[G : U] = \#(G/U)$ der Index von U in G.
Ist $\#(G/U)$ unendlich, so setzen wir $[G : U] = \infty$.

11.12 Korollar: (Satz von Lagrange)

Ist G eine endliche Gruppe und $U \subseteq G$ eine Untergruppe, so gilt:
$\#G = \#U \cdot [G : U]$.

Beweis: Jede Nebenklasse besitzt nach Satz 11.10 gleich viele Elemente. Es gibt $[G : U]$ Nebenklassen und G ist die disjunkte Vereinigung dieser Nebenklassen. qed.

11.13 Beispiel:

Betrachte die Untergruppe $T = \{e, \tau\}$ von S_3 mit $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ Dann gilt: $\#T = 2, \#S_3 = 6$ und $[S_3 : T] = 3$.

11.14 Definition:

Sei G eine Gruppe und $M \subseteq G$ eine Teilmenge.

(a) Die Menge aller Produkte $a_1 \cdot a_2 \cdots a_n$ mit $a_i \in M$ oder $a_i^{-1} \in M$ bildet eine Untergruppe von G. Sie heißt die von M erzeugte Untergruppe von G und wird mit $< M >$ bezeichnet.

(b) Besitzt G ein Erzeugendensystem, bestehend aus nur einem Element a, so heißt G eine zyklische Gruppe. Wir schreiben auch $G =< a >$ statt $G =< \{a\} >$.

(c) Ist $a \in G$, so dass $< a >$ endlich ist, so heißt $ord_G(a) = \# < a >$ die Ordnung von a in G.
Ist $< a >$ nicht endlich, so setzen wir $ord_G(a) = \infty$.

11.15 Beispiele:

(a) Die Gruppe $(\mathbb{Z}, +)$ ist zyklisch und es gilt $\mathbb{Z} =< 1 >$.

(b) Die Gruppe $(\mathbb{Z}/n\mathbb{Z}, +)$ ist zyklisch und es gilt $\mathbb{Z}/n\mathbb{Z} =< \overline{1} >= \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$.

(c) Die Untergruppe $T = \{e, \tau\}$ von S_3 ist zyklisch und es gilt $T =< \tau >$.

11.16 Satz:

Sei G eine Gruppe und $a \in G$.

(a) Ist $< a >$ unendlich, so gilt $< a >= \{a^i \mid i \in \mathbb{Z}\}$
Ist $< a >$ endlich und $m = ord_G(a) = \# < a >$, so gilt:
$< a >= \{a^i \mid i = 0, \ldots, m-1\}$.

(b) Eine zyklische Gruppe ist stets kommutativ.

(c) Ist eine Gruppe G endlich, so ist $ord_G(a)$ ein Teiler von $\#G$.

(d) („Kleiner Satz von Fermat in Gruppen“)
Ist G endlich, so gilt $a^{(\#G)} = e$ für alle $a \in G$.

Beweis:

(a) „$\supseteq$“ klar

„$\subseteq$“ Die Elemente von $< a >$ sind Produkte $b_1, \ldots, b_n$ mit $b_i \in \{a, a^{-1}\}$. Nach Vereinfachung mittels $a \cdot a^{-1} = e$ bleibt entweder a^i mit $i > 0$ oder $(a^{-1})^i$ mit $i > 0$ oder e übrig. Dies zeigt $< a > \subseteq \{a^i \mid i \in \mathbb{Z}\}$.

Im Fall $\# < a >< \infty$ gilt zusätzlich $\#\{a^i \mid i \in \mathbb{Z}\} = ord_G(a)$.
Sei $m \geq 0$ die kleinste nicht-negative Zahl mit $a^m = e$ (eine solche Zahl exisitiert, denn es gibt $0 < i < j$ mit $a^i = a^j$ und dann folgt $a^{j-i} = e$).
Wir behaupten nun $< a >= \{e, a, a^2, \ldots, a^{m-1}\}$ (und somit $m = ord_G(a)$).

„$\subseteq$“ Sei $a^i \in < a >$ mit $i \in \mathbb{Z}$. Schreibe $i = q \cdot m + r$ mit $q \in \mathbb{Z}$ und $r \in \{0, \ldots, m-1\}$.
Dann gilt $a^i = a^{qm} \cdot a^r = (a^m)^q \cdot a^r = e^q \cdot a^r = a^r \in \{e, a, \ldots, a^{m-1}\}$.

„$\supseteq$“ klar

Die Elemente von $\{e, a, \ldots, a^{m-1}\}$ sind paarweise verschieden. Gilt $a^i = a^j$ mit $0 \leq i \leq j \leq m-1$, so folgt $a^{j-i} = e$ und $j - i < m$ im Widerspruch zur Definition von m.
Insgesamt erhalten wir $\# < a >= m$ und $< a >= \{e, a, \ldots, a^{m-1}\}$.

(b) Folgt aus (a).

(c) Folgt aus (a) und dem Satz von Lagrange.

(d) Schreibe $\#G = ord_G(a) \cdot r$ mit $r \in \mathbb{N}$ gemäß (c).
Dies liefert $a^{(\#G)} = (a^{ord_G(a)})^r = e^r = e$. qed.

11.17 Beispiel:

(a) (Kleiner Satz von Fermat)
Sei p eine Primzahl. Betrachte die Gruppe $G = (\mathbb{F}_p)^x = (\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}$ bezüglich $\cdot$
Für jedes $\overline{a} \in (\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}$ gilt dann $\overline{a}^{(p-1)} = \overline{1}$.
Anders ausgedrückt: Für jedes $a \in (\mathbb{Z}/p\mathbb{Z})$ gilt $a^{(p-1)} \equiv 1 (mod\ p)$.

(b) Sind p, q zwei Primzahlen und ist $n = pq$, so gilt: Ist $a \in \mathbb{Z}$ weder durch p, noch durch q teilbar, so gilt $a^{(p-1)(q-1)} \equiv 1 (mod\ n)$, denn $a^{(p-1)(q-1)} \equiv 1^{(q-1)} \equiv 1 (mod\ p)$ und $a^{(p-1)(q-1)} \equiv 1^{(p-1)} \equiv 1 (mod\ q)$ (vgl. Übungen).

11.18 Bemerkung: (RSA Verfahren)

„Public Key Kryptosystem“
Ziel: *Bob* will *Alice* eine Nachricht senden.
Alice besitzt einen öffentlichen Schlüssel, den alle kennen.
Alice besitzt auch einen geheimen Schlüssel, den nur sie kennt.
Die Gegenerin *Eve*, die die verschlüsselte Nachricht mithört und den öffentlichen Schlüssel von *Alice* kennt, soll die Nachricht nicht entschlüsseln können.

Verfahren:

(a) A wählt zwei große Primzahlen p, q und eine Zahl $e \in \{10, \dots, pq\}$ mit $ggT(e, (p-1)(q-1)) = 1$.

(b) A berechnet $n = pq$ und ein $0 < d < pq$ mit $de \equiv 1 (mod\ (p-1)(q-1))$.

(c) Der öffentliche Schlüssel von A ist (n, e).

(d) Der geheime Schlüssel von A ist (p, q, d).

(e) Will B eine Zahl $0 < m < n$ mit $ggT(m, n) = 1$ verschlüsseln, so berechnet er $c = m^e (mod\ n)$. Die Zahl c ist die verschlüsselte Nachricht.

(f) Will A die Nachricht c entschlüsseln, so berechnet sie $m' \equiv c^d (mod\ n)$.

Korrektheit: Es gilt $m' \equiv c^d \equiv (m^e)^d \equiv m^{(p-1)(q-1)k+1} \equiv (m^k)^{(p-1)(q-1)} \cdot m \equiv 1 \cdot m \equiv m (mod\ n)$, denn $ed = k(p-1)(q-1) + 1$.

Sicherheit: Will E die Nachricht c entschlüsseln, so muss sie n in die Primfaktoren p, q zerlegen.

D. Welche Gruppen braucht man in der linearen Algebra?

Die symmetrische Gruppe $S_n = \{\varphi : \{1, \dots, n\} \to \{1, \dots, n\} \text{ (bijektiv)}\}$ spielt eine große Rolle.

11.19 Definition:

Sei $\varphi \in S_n$ eine Permutation.

(a) Eine Zahl $i \in \{1, \dots, n\}$ heißt Fixpunkt von φ, wenn $\varphi(i) = i$ gilt.

(b) Die Menge $\{i \in \{1, \dots, n\} \mid \varphi(i) \neq i\}$ heißt der Wirkungsbereich von φ.

(c) Besteht der Wirkungsbereich von φ aus genau zwei Zahlen, so heißt φ eine Transposition. Ist er von der Form $\{i, i+1\}$, so heißt φ eine Nachbartransposition.

(d) Die Permutation φ heißt Zykel (oder Zyklus oder zyklische Vertauschung), wenn man den Wirkungsbereich $\{i_1, \dots, i_k\}$ von φ so nummerieren kann, dass $\varphi(i_1) = i_2, \varphi(i_2) = i_3, \dots, \varphi(i_k) = i_1$ gilt.
Schreibweise: $\varphi = (\ i_1 \quad i_2 \quad \cdots \quad i_k)\ )$

11.20 Beispiel:

Es gibt 6 Elemente in der S_3:

- die Identität ( )
- drei Transpositionen (1 2), (1 3), (2 3)
- zwei Dreierzyklen (1 2 3), (3 2 1)

11.21 Satz:

Jede Permutation kann man darstellen als Produkt von Zyklen mit disjunkten Wirkungsbereichen. Diese Zyklen sind dabei eindeutig bestimmt und sie kommutieren miteinander.

Beweis: *Existenz:* Sei $\varphi \in S_n$. Wir konstruieren die gewünschte Zerlegung induktiv. Sei i_1 eine noch nicht abgearbeitete Zahl im Wirkungsbereich von φ. Bilde $i_2 = \varphi(i_1), i_3 = \varphi(i_2)$ usw. bis $i_1 = \varphi(i_k)$ auftritt. Wegen der Injektivität von φ kann dabei nie $\varphi(i_k) = i_l$ mit $1 < l \leq k$ gelten. Dann ist $\sigma_1 = (\ i_1 \quad i_2 \quad \cdots \quad i_k\ )$ ein Zykel in der Darstellung von φ und $\{i_1, \ldots, i_k\}$ sind abgearbeitet. Fahre mit dem nächsten i_1 fort, solange bis der Wirkungsbereich von φ ganz abgearbeitet ist.
Jedes $i \in \{1, \ldots, n\}$ ist dann entweder ein Fixpunkt oder liegt im Wirkungsbereich genau eines der Zykel σ_j, d.h. es gilt $\varphi = \sigma_1 \cdot \sigma_2 \cdots \sigma_l$.

Eindeutigkeit: Sei $\varphi = \sigma'_1 \cdots \sigma'_m$ eine weitere solche Darstellung. Dann gilt:

(a) Der Wirkungsbereich von φ ist die disjunkte Vereinigung der Wirkungsbereiche der σ'_j.

(b) Die σ'_j kommutieren miteinander.

(c) Liegt i im Wirkungsbereich eine σ'_j, so gilt $\sigma'_j = (\ i \quad \varphi(i) \quad \varphi^2(i) \quad \cdots \quad \varphi^k(i)\ )$.
Der Index i kommt auch als i_λ im Wirkungsbereich eines σ_p vor.
Es folgt $\sigma_p = (\ i_1 \quad i_2 \quad \cdots \quad i_\lambda \quad \cdots \quad i_\kappa\ ) = (\ i_\lambda \quad i_{\lambda+1} \quad \cdots \quad i_\kappa \quad i_1 \quad \cdots \quad i_{\lambda-1}\ )$
$= (\ i_\lambda \quad \varphi(i_\lambda) \quad \varphi^2(i_\lambda) \quad \cdots \quad \varphi^\kappa(i_\lambda)\ ) = \sigma'_j$

Kommutativität: klar qed.

11.22 Beispiel:

In S_4 gilt $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (\ 1 \quad 3\ )(\ 2 \quad 4\ )$

11.23 Satz:

(a) Jede Permutation in S_n kann man als Produkt von Transpositionen schreiben.

(b) Jede Permutation in S_n kann man als Produkt von Nachbartranspositionen schreiben.

(c) Diese Darstellungen sind im Allgemeinen nicht eindeutig.

Beweis:

(a) Wegen Satz 11.21 brauchen wir nur Zyklen als Produkte von Transpositionen zu schreiben.
Es gilt $(\ i_1 \quad i_2 \quad \cdots \quad i_k\ ) = (\ i_1 \quad i_2\ )(\ i_2 \quad i_3\ ) \cdots (\ i_{k-1} \quad i_k\ )$.

(b) Wegen (a) brauchen wir nur beliebige Transpositionen als Produkt von Nachbartranspositionen darzustellen.
Sei $1 \leq i < j \leq n$. Dann gilt:$(\ i \quad j\ ) =$
$(\ j-1 \quad j\ )(\ j-2 \quad j-1\ ) \cdots (\ i+1 \quad i+2\ )(\ i \quad i+1\ )(\ i+1 \quad i+2\ ) \cdots (\ j-1 \quad j\ )$
(Beachte: Dies sind $2(j-i-1)+1$ Nachbartranspositionen!)

(c) Folgt aus $(\ 1 \quad 2 \quad 3\ ) = (\ 1 \quad 2\ )(\ 2 \quad 3\ ) = (\ 1 \quad 3\ )(\ 2 \quad 3\ )(\ 1 \quad 2\ )(\ 1 \quad 3\ )$ qed.

11.24 Definition:

Sei $\varphi \in S_n$.

(a) Gilt $1 \leq i < j \leq$ und $\varphi(j) > \varphi(i)$, so heißt das Paar (i, j) ein Fehlstand von φ.

(b) Die Permutation φ heißt gerade, wenn sie eine gerade Anzahl von Fehlständen besitzt. Ansonsten heißt φ eine ungerade Permutation.

(c) Die Menge aller gerade Permutationen wird mit A_n bezeichnet.

11.25 Satz:

(a) Eine Nachbartransposition besitzt genau einen Fehlstand.

(b) Jede Transposition besitzt eine ungerade Anzahl von Fehlständen.

(c) Hat $\varphi \in S_n$ genau k Fehlstände und ist τ eine Nachbartransposition, so hat $\tau \circ \varphi$ entweder $k-1$ oder $k+1$ Fehlstände.

Beweis:

(a) Es gibt für $\begin{pmatrix} i & i+1 \end{pmatrix}$ genau den Fehlstand $(i, i+1)$.

(b) Sei $1 \leq i < j \leq n$. Für die Transposition $\tau = \begin{pmatrix} i & j \end{pmatrix}$ gibt es genau die Fehlstände (i, k) mit $i+1 \leq k \leq j-1$ und (l, j) mit $i+1 \leq l \leq j-1$ und den Fehlstand (i, j).
Insgesamt sind dies $2(j = i-1)+1$ Fehlstände.

(c) Sei $\tau = \begin{pmatrix} i & i+1 \end{pmatrix}$. Ist $(i, i+1)$ ein Fehlstand von φ, so ist $(i, i+1)$ kein Fehlstand von $\tau \circ \varphi$.
Ist $(i, i+1)$ kein Fehlstand von φ, so ist $(i, i+1)$ ein Fehlstand von $\tau \circ \varphi$. qed.

11.26 Satz: (Charakterisierung der geraden Permutationen)

Für eine Permutation $\varphi \in S_n$ sind die folgenden Bedingungen äquivalent:

(a) φ ist eine gerade Permutation.

(b) Jede Darstellung von φ als Produkt von Nachbartranspositionen hat eine gerade Anzahl von Faktoren.

(c) Es gibt eine Darstellung von φ als Produkt von Nachbartranspositionen mit einer geraden Anzahl von Faktoren.

(d) Es gibt eine Darstellung von φ als Produkt einer geraden Anzahl von Transpositionen.

Beweis: „(a)⇒(b)“ Schreibe φ als Produkt von Nachbartranspositionen $\varphi = \tau_1 \cdot \tau_2 \cdots \tau_l$.
Multipliziere φ nacheinander von links mit τ_1, τ_2 usw. Wegen $\tau_i \cdot \tau_i = e$ wird das Produkt jeweils um einen Faktor kürzer.
Nach 11.25.c ändert sich bei jeder Multiplikation die Partität (gerade/ungerade) der Anzahl der Fehlstände.
Da es am Anfang eine gerade Anzahl von Fehlständen gibt und am Ende 0 Fehlstände, muss also l gerade sein.

„(b)⇒(c)“ klar

„(c)⇒(d)“ klar

„(d)⇒(c)“ Nach dem Beweis von 11.23.b ist jede Transposition Produkt einer ungeraden Anzahl von Nachbartranspositionen.

„(c)⇒(a)“ Schreibe $\varphi = \tau_1 \cdot \tau_2 \cdots \tau_{2l} \cdot e$. Da e keine Fehlstände hat und sich bei der Multiplikation mit τ_i die Partität der Fehlstände ändert, besitzt φ insgesamt eine gerade Anzahl von Fehlständen. qed.

11.27 Beispiel:

Sei $\varphi \in S_n$ ein K-Zykel, also $\varphi = \begin{pmatrix} i_1 & i_2 & \cdots & i_k \end{pmatrix}$.
Wegen $\varphi = \begin{pmatrix} i_1 & i_2 \end{pmatrix}\begin{pmatrix} i_2 & i_3 \end{pmatrix}\cdots\begin{pmatrix} i_{k-1} & i_k \end{pmatrix}$ ist φ genau dann gerade, wenn k ungerade ist.

11.28 Korollar:

(a) Die Menge A_n aller geraden Permutationen ist eine Untergruppe von S_n. Sie heißt die alternierende Gruppe.

(b) Für eine feste ungerade Permutation φ gilt: $S_n = A_n \dot\cup \varphi A_n$.

(c) Für jedes $n \geq 1$ gilt: $\#A_n = \frac{1}{2}n!$

Beweis:

(a) Nach Satz 11.26 ist das Produkt zweier gerader Permutationen wieder gerade. Sei φ gerade. Wegen $r = \varphi \circ \varphi^{-1}$ ist auch φ^{-1} gerade.

(b) Nach Satz 11.26 sind die Elemente von φA_n alle ungerade.
Sei nun ψ ungerade. Dann ist $\varphi^{-1}\psi$ gerade, also $\varphi^{-1}\psi \in A_n$ und somit $\psi \in \varphi A_n$.

(c) Folgt aus (b), da $\begin{array}{rcl} \mu : A_n & \to & \varphi A_n \\ \psi & \mapsto & \varphi\psi \end{array}$ bijektiv ist. qed.

E. Hoffentlich gibt es keine Gruppenhomomorfiesmen!

Leider doch!

11.29 Definition:

Seien G, H zwei Gruppen und $f : G \to H$ eine Abbildung. Die Abbildung f heißt Gruppenhomomorphismus, wenn für alle $g_1, g_2 \in G$ gilt: $f(g_1 \circ g_2) = f(g_1) * f(g_2)$

11.30 Beispiel:

(a) Sei $(G, \circ)$ die Gruppe $(\mathbb{R}, +)$. Sei $(H, *)$ die Gruppe $(\mathbb{R} \setminus \{0\}, \cdot)$.
Dann ist $\begin{array}{rcl} exp : \mathbb{R} & \to & \mathbb{R} \setminus \{0\} \\ x & \mapsto & e^x \end{array}$ ein Gruppenhomomorphismus, denn
$exp(x + y) = e^{x+y} = e^x \cdot e^y = exp(x) \cdot exp(y)$.

(b) Die identische Abbildung $\begin{array}{rcl} id_G : G & \to & G \\ a & \mapsto & a \end{array}$ ist ein Gruppenhomomorphismus.

(c) Ist G eine Gruppe und $U \subseteq G$ eine Untergruppe, so ist die Inklusionsabbildung $\iota : U \to G$ ein Gruppenhomomorphismus.

(d) Sei $(G, \circ)$ die Gruppe $(\mathbb{Z}, +)$ und $a \in \mathbb{Z}$. Dann ist die Multiplikation $\begin{array}{rcl} \mu_a : \mathbb{Z} & \to & \mathbb{Z} \\ z & \mapsto & az \end{array}$ ein Gruppenhomomorphismus, denn $a(z_1 + z_2) = az_1 + az_2$ für alle $z_1, z_2 \in \mathbb{Z}$.

11.31 Bemerkung:

(a) Für einen Gruppenhomomorphismus $\varphi : G \to H$ gilt $\varphi(e_G) = e_H$.

(b) Ist $\varphi : G \to H$ ein Gruppenhomomorphismus, so ist $Kern(\varphi) = \{g \in G \mid \varphi(g) = e_H\}$ eine Untergruppe von G (genannt Kern von φ).
$Bild(\varphi) = \{h \in H \mid$ es gibt ein $g \in G$ mit $\varphi(g) = h\}$ ist eine Untergruppe von H (genannt das Bild von φ).

11.32 Definition:

Sei $n \geq 1$. Für eine Permutation $\sigma \in S_n$ sei

$$sign(\sigma) = \begin{cases} 1 & \text{, falls } \sigma \text{ gerade ist} \\ -1 & \text{, falls } \sigma \text{ ungerade ist} \end{cases}$$ das Signum von σ.

11.33 Satz:

Sei $n \geq 1$.

(a) Für $\sigma, \sigma' \in S_n$ gilt $sign(\sigma\sigma') = sign(\sigma) \cdot sign(\sigma')$.

(b) Die Abbildung $\begin{array}{rcl} sign : S_n & \to & \{1, -1\} \\ \sigma & \mapsto & sign(\sigma) \end{array}$ ist ein Gruppenhomomorphismus.

Beweis:

(a) Schreibe $\sigma = \tau_1 \cdots \tau_k$ und $\sigma' = \tau'_1 \cdots \tau'_l$ mit Transpositionen τ_i, τ'_j. Dann gilt $sign(\sigma) = (-1)^k$ und $sign(\sigma') = (-1)^l$.
Aus $\sigma\sigma' = \tau_1 \cdots \tau_k \cdot \tau'_1 \cdots \tau'_l$ folgt $sign(\sigma\sigma') = (-1)^{k+l}$. Hieraus ergibt sich die Behauptung.

(b) Folgt sofort aus (a). qed.

12 Am Anfang war die Zahl

Wie kann man die Multiplikation in $\mathbb{Z}$ algebraisch verstehen?

Ziel: Untersuche den Ring $(\mathbb{Z}, +, \cdot)$ genauer!
Wiederholung: $\mathbb{Z}$ ist ein kommutativer Ring mit Einselement.

12.1 Definition:

Sei R ein Ring.

(a) Ein Element $r \in R \setminus \{0\}$ heißt Nichtnullteiler, wenn für $s \in R$ aus $rs = 0$ folgt, dass $s = 0$ gilt.
Gibt es jedoch ein $s \in R \setminus \{0\}$ mit $rs = 0$, so heißt r ein Nullteiler.

(b) Der Ring R heißt nullteilerfrei (oder Integritätsbereich), wenn er keinen Nullteiler besitzt (d.h. aus $rs = 0$ folgt $r = 0$ oder $s = 0$).

(c) Ein Element $r \in R$ heißt Einheit, wenn es ein $s \in R$ gibt, mit $rs = 1$.

(d) Die Menge aller Einheiten von R bildet eine (multiplikative) Gruppe. Sie heißt die Einheitengruppe von R und wird mit R^* bezeichnet.

12.2 Beispiele:

(a) Der Ring $\mathbb{Z}$ ist ein Integritätsbereich.

(b) Das Element $\overline{2} \in \mathbb{Z}/6\mathbb{Z}$ ist ein Nullteiler, denn $\overline{2 \cdot 3} = \overline{0}$.

(c) Die Einheitengruppe von $\mathbb{Z}$ ist $\mathbb{Z}^* = \{1, -1\}$.

(d) Ist K ein Körper, so gilt $K^* = K \setminus \{0\}$.

12.3 Satz:

Jeder endliche Integritätsbereich ist ein Körper.

Beweis: vgl. Übungen.

12.4 Satz: (Division mit Rest, vgl. Satz 2.5)

Sei $n \in \mathbb{Z}$ und $b \in \mathbb{N}_+$. Dann gibt es eindeutig bestimmte Zahlen $q, r \in \mathbb{Z}$ mit $a = qb + r$ und $0 \leq r < b$.

Beweis:

Existenz: O.E. betrachten wir nur den Fall $a > 0$.
Sei $M = \{z \in \mathbb{Z} \mid a - zb \geq 0\}$. Wir „zeigen“ drei Zwischenbehauptungen:

(a) Die Menge M ist nicht leer: $0 \in M$.

(b) Die Menge M ist nach oben beschränkt, d.h. es gibt ein $s \in \mathbb{Z}$ mit $z < s$ für alle $z \in M$.
Wegen $a - (a+1)b = a - ab - b < 0$ ist $s = a + 1$ eine obere Schranke von M.

(c) Jede nach oben beschränkte, nicht leere Teilmenge von $\mathbb{Z}$ besitzt ein maximales Element. Sei $m \in M$ und $s > m$ eine obere Schranke für M. Wir schließen mit absteigender Induktion nach s: Entweder ist $s-1$ ebenfalls eine obere Schranke von M oder $s-1 \in M$, d.h. $s-1$ ist ein maximales Element von M.

Sei nun $q \in M$ das maximale Element von M. Dann gilt $r = a - qb \geq 0$ und wegen $q+1 \notin M$ folgt $r - b = a - (q+1)b < 0$, also $r < b$.

Eindeutigkeit: Sei $a = qb + r = q'b + r'$ mit $q, q' \in \mathbb{Z}$ und $r, r' \in \{0, \ldots, b-1\}$.
O.E. gelte $r' \geq r$. Aus $r' - r = qb - q'b = (q-q')b \in b\mathbb{Z}$ und $0 \leq r' - r < b$ folgt $r' - r = 0$, also $r = r'$. Dann liefert $qb = q'b$ dass $(q-q')b = 0$ gilt.
Da $\mathbb{Z}$ Integritätsbereich ist, folgt $q = q'$. qed.

12.5 Definition:

Seien $a, b \in \mathbb{Z}$. Eine Zahl $g \in \mathbb{Z}$ heißt gemeinsamer Teiler von a und b, wenn gilt: $g \mid a$ und $g \mid b$ („g teilt a, d.h. $a = qg + 0$).
Die Zahl g heißt größter gemeinsamer Teiler (ggT bzw. gcd) von a und b, wenn gilt:

(a) $g \mid a$ und $g \mid b$.

(b) Ist $h \in \mathbb{Z}$ mit $h \mid a$ und $h \mid b$, so folgt $h \mid g$.

(c) $g \geq 0$.

Schreibweise: $g = ggT(a, b)$

12.6 Beispiele:

(a) $ggT(10, 15) = 5$

(b) $ggT(64, 81) = 1$

(c) Für $a \neq 0$ gilt $ggT(0, a) = |a|$

(d) $ggT(0, 0) = 0$: Jede Zahl ist ein gemeinsamer Teiler von 0 und 0. Jede Zahl muss den ggT teilen. Die einzige Zahl, die ein Vielfaches jeder Zahl ist, ist 0.

12.7 Satz:

Der ggT zweier ganzen Zahlen existiert und ist eindeutig bestimmt.

Beweis:

Existenz: Folgt aus dem euklidischen Algorithmus oder aus dem Fundamentalsatz der Arithmetik.

Eindeutigkeit: Fall $a = b = 0$: Vgl. Beispiel 12.6.d

Fall $a = 0, b \neq 0$, oder $a \neq 0, b = 0$: Vgl. Beispiel 12.6.c

Fall $a, b \neq 0$: Seien g, g' zwei ggT von a und b. Nach Definition gilt $g \mid g'$ und $g' \mid g$.
Also gibt es $c_1, c_2 \in \mathbb{Z}$ mit $g = c_1 g'$ und $g' = c_2 g$. Dies liefert $g = c_1 c_2 g$ und somit $g(1 - c_1 c_2) = 0$.
Der Fall $g = 0, g' = 0$ ist wegen $a \neq 0$ unmöglich. Also bleibt nur die Möglichkeit $c_1 c_2 = 1$.
Wegen $g, g' \geq 0$ ist nur $c_1 = c_2 = 1$ möglich, also $g = g'$. qed.

12.8 Lemma:

Sei $a \in \mathbb{Z}$ und $b \in \mathbb{N}_+$. Schreibe $a = qb + r$ mit $a \in \mathbb{Z}$ und $0 \leq r < b$. Dann gilt:
$ggT(a, b) = ggT(b, r)$ (falls einer dieser ggT existiert).

Beweis:

(a) Jeder gemeinsame Teiler von a und b ist gemeinsamer Teiler von b und r. Es gelte $g \mid a$ und $g \mid b$. Schreibe $a = \tilde{a}g$ und $b = \tilde{b}g$ mit $\tilde{a}, \tilde{b} \in \mathbb{Z}$.
Dann gilt $r = a - qb = (\tilde{a} - q\tilde{b})g$. Also folgt $g \mid r$.

(b) Jeder gemeinsame Teiler von b und r ist gemeinsamer Teiler von a und b. Es gelte $g \mid b$ und $g \mid r$, also $b = \tilde{b}g$ und $r = \tilde{r}g$ mit $\tilde{b}, \tilde{r} \in \mathbb{Z}$.
Dann folgt $a = qb + r = (q\tilde{b} + \tilde{r})g$ und somit $g \mid a$.

(c) Aus (a) und (b) folgt die Behauptung. qed.

12.9 Satz: (Der euklidische Algorithmus)

Seien $a, b \in \mathbb{Z}$. Betrachte die folgenden Anweisungen:

(a) Gilt $a = b = 0$, so gib $g = 0$ aus und stoppe.

(b) Ist $a = 0$, so gib $g = |a|$ aus und stoppe.

(c) Ist $b = 0$, so gib $g = |b|$ aus und stoppe.

(d) Ist $a < 0$, so ersetze a durch $-a$.

(e) Ist $b < 0$, so ersetze b durch $-b$.

(f) Ist $a < b$, so vertausche a und b.

(g) Berechne eine Darstellung $a = qb + r$ mit $q \geq 0$ und $0 \leq r < b$.

(h) Ist $r = 0$, so gib $g = b$ aus und stoppe.

(i) Ersetze (a, b) durch (b, r) und fahre mit (g) fort.

Dies ist ein Algorithmus, der $g = ggT(a, b)$ berechnet.

Beweis:

Endlichkeit: Kommt die Abarbeitung bis Schritt (i), so gilt $a > b > r > 0$. Beim nächsten Durchlauf von (g) sind also die beiden Zahlen a und b kleiner und immer noch positiv.
Also kann (g) nur endlich oft durchlaufen werden.

Korrektheit: Stoppt der Algorithmus in Schritt (a),(b) oder (c), so ist das Ergebnis nach Beispiel 12.6 korrekt.
Wegen $ggT(a, b) = ggT(-a, b) = ggT(b, a)$ ändern die Schritte (d),(e) und (f) den ggT nicht.
Wegen Lemma 12.8 ändern die Schritte (g),(h) und (i) den ggT nicht.
Stoppt der Algorithmus in Schritt (h), so gilt $a = qb + r$ und $g = ggT(a, b) = b$. qed.

12.10 Beispiel:

(a) Berechnung von $ggT(-10, 15)$:

(d) Setze $a = 10, b = 15$.
(f) Setze $a = 15, b = 10$.
(g) Berechne $15 = 1 \cdot 10 + 5$, also $r = 5$.
(i) Setze $a = 10, b = 5$.
(g) Berechne $10 = 2 \cdot 5 + 0$, also $r = 0$.
(h) Gib $g = 5$ aus und stoppe.

Dies zeigt $ggT(-10, 15) = 5$.

(b) Berechnung von $ggT(5, 0)$:

(c) Gib $g = 5$ aus und stoppe.

Also gilt $ggT(5, 0) = 5$.

Hilfe! Der fragt Hauptidealbereich ab!

12.11 Definition:

Sei R ein Ring.

(a) Eine Teilmenge $I \subseteq R$ heißt Ideal, wenn gilt:

1.) $(I, +)$ ist eine Untergruppe von $(R, +)$.
2.) $R \cdot I \subseteq I$, d.h. für $r \in R$ und $s \in I$ gilt $rs \in I$.

(b) Eine Teilmenge $I \subseteq R$ heißt Hauptideal, wenn es ein Element $r \in R$ gibt, mit $R \cdot r = I$. (Ein Hauptideal ist offenbar ein Ideal).

(c) Der Ring R heißt Hauptidealring, wenn jedes Ideal von R ein Hauptideal ist.

(d) Der Ring R heißt Hauptidealbereich, wenn er Hauptidealring und Integritätsbereich ist.

12.12 Satz:

Der Ring $\mathbb{Z}$ ist ein Hauptidealbereich.

Beweis: Sei $I \subseteq \mathbb{Z}$ ein Ideal. Gilt $I = \{0\}$, so folgt $I = \mathbb{Z} \cdot 0$.
Sei nun $I \neq \{0\}$ und $a \in I \setminus \{0\}$. Ist $I \ni a < 0$, so gilt auch $-a = (-1) \cdot a \in I$. Also gibt es ein Element $a \subseteq I$ mit $a > 0$. Sei nun g die kleinste positive Zahl in I. Wir behaupten, dass $I = \mathbb{Z} \cdot g$ gilt.

„$\supseteq$“ Aus $g \in \mathbb{Z}$ folgt $\mathbb{Z} \cdot g \in I$.

„$\subseteq$“ Sei $b \in I$. Schreibe $b = qg + r$ mit $q \in \mathbb{Z}$ und $0 \leq r < g$.
Dann gilt $r = b - qg \in I$. Wegen der Minimalität von g bedeutet dies $r = 0$, also $b \in \mathbb{Z}g$ qed.

C. Und wie passen Primzahlen in dieses Bild?

12.13 Definition:

Sei R ein Ring.

(a) Ein Element $r \in R \setminus \{0\}$, das nicht Einheit ist, heißt irreduzibel, wenn für jede Darstellung $r = s_1 s_2$ mit $s_1, s_2 \in R$ entweder s_1 oder s_2 eine Einheit ist.

(b) Ein positives, irreduzibles Element von $\mathbb{Z}$ heißt Primzahl.
Mit anderen Worten: Eine Zahl $p > 0$ heißt Primzahl, wenn man sie nicht als Produkt $p = q_1 q_2$ mit $1 < q_1 < p$ und $1 < q_2 < p$ schreiben kann.

(c) Ein Element $r \in R \setminus R^x$ mit $r \neq 0$ heißt Primelement, wenn für $a, b \in R$ aus $r \mid ab$ folgt, dass $r \mid a$ oder $r \mid b$ gilt.

12.14 Satz:

Eine Primzahl $q \in \mathbb{Z}$ ist ein Primelement von $\mathbb{Z}$. Also folgt aus $p \mid ab$, dass $p \mid a$ oder $p \mid b$ gilt.

Beweis: Sei $g = ggT(p, a)$ und $h = ggT(p, b)$. Wegen der Primzahleigenschaft von p ist nur $g \in \{1, p\}$ und $h \in \{1, p\}$ möglich.

1. Fall: $g = p$: Dann gilt $g \mid a$ wie gewünscht.

2. Fall: $h = p$: Dann gilt $h \mid b$ wie gewünscht.

3. Fall: $g = h = 1$: Nach dem Lemma von Bezout (vgl. Übungen) gibt es Darstellungen $1 = r_1 p + r_2 a$ und $1 = s_1 p + s_2 a$ mit $r_1, r_2, s_1, s_2 \in \mathbb{Z}$. Schreibe auch $ab = tp$ mit $t \in \mathbb{Z}$.
Dann folgt $1 = (r_1 p + r_2 a)(s_1 p + s_2 b) = p(r_1 s_1 p + r_2 a s_1 + r_1 s_2 b + r_2 s_2 t) \in p\mathbb{Z}$ ↯ Also kann der 3. Fall nicht eintreten. qed.

12.15 Korollar:

Der Ring $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ ist für eine Primzahl p ein Körper.

Beweis: Nach 12.14 ist $\mathbb{F}_p$ ein Integritätsring. Jetzt folgt die Behauptung aus Satz 12.3. qed.

12.16 Theorem: (Der Fundamentalsatz der Arithmetik)

Jedes $a \in \mathbb{Z} \setminus \{0\}$ besitzt eine eindeutige Darstellung der Form

$a = \varepsilon \cdot p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}$

mit $\varepsilon \in \{1, -1\}$ und $\alpha_i > 0$ und paarweise verschiedenen Primzahlen p_i.
Diese Darstellung nennt man Primfaktorzerlegung von a.

Beweisskizze:

Existenz: O.E. sei $a > 1$. Ist a eine Primzahl, so sind wir fertig.
Sonst schreibe $a = b \cdot c$ mit $1 < b < a$ und $1 < c < a$. Induktiv können wir annehmen, dass b und c bereits Primfaktorzerlegungen besitzen.. Indem wir diese zusammenfügen, erhalten wir eine Primfaktorzerlegung von a.

Eindeutigkeit: Sei $a = \varepsilon \cdot p_1^{\alpha_1} \cdots p_r^{\alpha_r} = \varepsilon' \cdot q_1^{\beta_1} \cdots q_s^{\beta_s}$. Offenbar gilt $\varepsilon = \varepsilon'$.
Wegen $p_1(q_1^{\beta_1} \cdots q_s^{\beta_s})$ und Satz 12.14 gibt es ein $j \in \{1, \ldots, s\}$ mit $p_1 \mid q_j$. Da p_1 und q_j Primzahlen sind, folgt $p_1 = q_j$. Somit folgt $r = s$ und $\{p_1, \ldots, p_r\} = \{q_1, \ldots, q_r\}$.
Nach Umnummerieren folgt $p_i = q_i$ für $i = 1, \ldots, r$ und somit $p_1^{\alpha_1} \cdots p_r^{\alpha_r} = p_1^{\beta_1} \cdots p_r^{\beta_r}$.
Wäre $\alpha_1 < \beta_1$ so wäre $p_2^{\alpha_2} \cdots p_r^{\alpha_r} = p_1^{\beta_1 - \alpha_1} \cdot p_2^{\beta_2} \cdots p_r^{\beta_r}$ ein Widerspruch, da p_1 nur die rechte Seite teilt. Analog liefert $\alpha_1 > \beta_1$ einen Widerspruch. Dies zeigt $\alpha_1 = \beta_1$.
Induktiv folgt $\alpha_i = \beta_i$ für $i = 1, \ldots, r$. qed.

13 Die Kunst des Buchstabenrechnens (Polynomringe)

A. Wie kommen die Buchstaben in die Algebra?

Im Folgenden sei stets K ein Körper.
Die exakte Definition des Polynomrings $K[x]$ (sprich „K adjungiert x“) wird in Beutelspacher §6.2 besprochen. Wir begnügen uns hier mit einer anschaulichen Einführung.

13.1 Bemerkung:

Sei x eine Unbestimmte (oder auch Variable), d.h. ein Buchstabensymbol. Wir bilden weitere Symbole $x^2, x^3, \ldots$.
Die Menge aller endlichen Linearkombinationen $a_o \cdot 1 + a_1 x + a_2 x^2 + \ldots + a_n x^n$ mit $a_i \in K$ heißt der Polynomring über K in der Unbestimmten x.
Eine solche Linearkombination heißt Polynom mit Koeffizienten $a_0, \ldots, a_n \in K$.
Wie ist die algebraische Struktur von $K[x]$ definiert?

(a) Seien $f = a_0 + a_1 x + \ldots + a_n x^n$ und $g = b_0 + b_1 x + \ldots + b_m x^m$ zwei Polynome (mit $a_i, b_j \in K$).
Dann sei $f + g = (a_0 + b_0) + (a_1 + b_1)x + \ldots + (a_k + b_k)x^k$ mit $k = max\{m, n\}$ und $a_i = b_j = 0$ für $i > n$ bzw. $j > m$.
Wie man leicht nachrechnet, wird $(K[x], +)$ hiermit zur Gruppe. Das neutrale Element ist dabei $f = 0$ und das inverse Element zu $g = a_0 + a_1 x + \ldots + a_n x^n$ ist $-g = -a_0 + (-a_1)x + \ldots + (-a_n)x^n$.

(b) Indem wir für $f = a_0 + a_1 x + \ldots + a_n x^n$ und $c \in K$ definieren, dass $c \cdot f = (ca_0) + (ca_1)x + \ldots + (ca_n)x^n$ gelten soll, erhalten wir auf $K[x]$ die Struktur eines Vektorraumes.

(c) Seien $f = a_0 + a_1 x + \ldots + a_n x^n$ und $g = b_0 + b_1 x + \ldots + b_m x^m$ zwei Polynome mit $a_i, b_j \in K$. Wir definieren das Produkt $f \cdot g$ durch die Cauchysche Produktformel:
$f \cdot g = \sum_{k \geq 0} (\sum_{i+j=k} a_i b_j) x^k$
$= (a_0 b_0) + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + \ldots + (a_n b_m)x^{n+m}$
Wobei wir wieder $a_i = 0$ für $i > n$ und $b_j = 0$ für $j > m$ setzen. Man kann nun nachrechnen, dass $K[x]$ hierdurch zu einem kommutativen Ring mit Einselement wird.
Jedes Polynom besitzt eine eindeutige Darstellung als endliche Linearkombination der Elemente $1, x, x^2, \ldots$
Also ist $K[x]$ ein undendlich-dimensionaler K-Vektorraum mit Basis $\{1, x, x^2, \ldots\}$.

13.2 Definition:

Sei $f = a_0 + a_1 x + \ldots + a_n x^n \in K[x] \setminus \{0\}$ mit $a_i \in K$ und $a_n \neq 0$.
Dann heißt $deg(f) = n$ der Grad von f (engl. „degree“).
Für $f = 0$ setzen wir $deg(f) = -1$.

13.3 Satz:

(a) Für jedes $n \geq 0$ ist $K[x]_{\leq n} = \{f \in K[x] \mid deg(f) \leq n\}$ ein K-Untervektorraum von $K[x]$. Der K-Vektorraum $K[x]_{\leq n}$ besitzt die Basis $\{1, x, x^2, \ldots, x^n\}$ und die Dimension $n + 1$.

(b) (Gradformel) Sind $f, g \in K[x] \setminus \{0\}$ so gilt $deg(fg) = deg(f) + deg(g)$.

Beweis:

(a) Ist $f = a_0 + a_1x + \ldots + a_nx^n \in K[x]_{\leq n}$ und $c \in K$, so gilt $cf = (ca_0) + (ca_1)x + \ldots + (ca_n)x^n \in K[x]_{\leq n}$. Die Vektorraumaxiome und Untergruppeneigenschaft bezüglich + sind klar.
Aus der Darstellung $f = a_0 + a_1x + \ldots + a_nx^n$ folgt dass $\{1, x, \ldots, x^n\}$ ein Erzeugendensystem von $K[x]_{\leq n}$ ist. Wegen der Eindeutigkeit dieser Darstellung ist $\{1, x, \ldots, x^n\}$ sogar eine Basis.

(b) Bei der Berechnung von fg in Bemerkung 13.1.c sind alle Summen $\sum_{i+j=k} a_ib_j$ mit $k > m + n$ gleich Null, da $i > n$ oder $j > m$ sein muss und damit $a_i = 0$ oder $b_j = 0$ in jedem Summanden. Somit folgt $deg(fg) \leq m + n$.
Sei nun $deg(f) = n$, also $a_n \neq 0$ und $deg(g) = m$, also $b_m \neq 0$. Dann gilt $\sum_{i+j=m+n} a_ib_j = a_nb_m \neq 0$. Dies zeigt $deg(fg) = n + m = deg(f) + deg(g)$. qed.

13.4 Korollar:

Der Ring $K[x]$ ist ein Integritätsbereich.

Beweis: Ist $deg(f) > 0$ und $deg(g) > 0$, so folgt $deg(fg) > 0$, also $fg \neq 0$.
Ist $f \in K \setminus \{0\}$ und $g \in K[x] \setminus \{0\}$, so gilt $deg(fg) = deg(g)$ und somit $fg \neq 0$.
Ist $f \in K[x] \setminus \{0\}$ und $g \in K \setminus \{0\}$, so folgt ebenso $fg \neq 0$.
Also kann $fg = 0$ nur gelten, falls $f = 0$ oder $g = 0$ erfüllt ist. qed.

13.5 Korollar:

Die Einheitengruppe von $K[x]$ ist $K[x]^x = K^x = K \setminus \{0\}$.

Beweis: Ist $f \in K[x]^x$ und $g \in K[x]$ mit $fg = 1$, so folgt aus $deg(fg) = 0$,
dass $deg(f) = deg(g) = 0$ sein muss.
Dies zeigt $f \in K \setminus \{0\}$. qed.

13.6 Definition:

Ist $f = a_0 + a_1x + \ldots + a_nx^n \in K[x]$ und $c \in K$, so heißt $f(c) = a_0 + a_1c + \ldots + a_nc^n$ der Wert von f an der Stelle c. Das Ergebnis $f(c)$ heißt auch das Ergebnis der Substitution von c (für x) in f. Ist $f(c) = 0$, so heißt c eine Nullstelle von f.

13.7 Satz: (Die Polynomdivision)

Seien $f, g \in K[x]$ und $g \neq 0$. Dann gibt es eindeutig bestimmte Polynome $q, r \in K[x]$ mit $f = qg + r$ und $deg(r) < deg(g)$.

Beweis:

Existenz: Sei $n = deg(f)$ und $m = deg(g)$. Wir schließen mit vollständiger Induktion nach n. Ist $n < m$, so setze $q = 0$ und $r = f$.
Sei nun $n > m$. Schreibe $f = a_0 + a_1x + \ldots + a_nx^n$ mit $a_i \in K$ und $a_n \neq 0$. sowie $g = b_0 + b_1x + \ldots + b_mx^m$ mit $b_i \in K$ und $b_m \neq 0$.

Betrachte: $h = f - \frac{a_n}{b_m}x^{n-m}g = (a_0 + a_1x + \ldots + a_nx^n) - (\frac{a_n}{b_m}b_0x^{n-m} + \frac{a_n}{b_m}b_1x^{n-m+1} + \ldots + a_nx^n)$
Es gilt $deg(h) < n$. Nach Induktionsvoraussetzung gibt es $q', r' \in K[x]$ mit $h = q'g + r'$ und $deg(r') < deg(g)$.
Setze $q = q' + \frac{a_n}{b_m}x^{n-m}$ und $r' = r$. Dann gilt
$f = h + \frac{a_n}{b_m}x^{n-m}g = q'g + r' + \frac{a_n}{b_m}x^{n-m}g = (q' + \frac{a_n}{b_m}x^{n-m})g + r' = qg + r$.
Eindeutigkeit: Sei $f = qg + r = \tilde{q}g + \tilde{r}$ mit $q, \tilde{q}, r, \tilde{r} \in K[x]$ und $deg(r) < deg(g)$ und $deg(\tilde{r}) < deg(g)$. Es folgt $(q - \tilde{q})g = \tilde{r} - r$ wobei $deg(\tilde{r} - r) < deg(g)$ gilt.
Wegen der Gradformel ist entweder $q - \tilde{q} = 0$ oder $deg((q - \tilde{q})g) \geq deg(g)$↯
Somit ist nur $q = \tilde{q}, r = \tilde{r}$ möglich. qed.

13.8 Korollar:

Ist $a \in K$ eine Nullstelle von $f \in K[x]$, so gibt es ein $g \in K[x]$ mit $f = (x - a)g$. Man sagt dazu, dass man eine Nullstelle abspalten kann.

Beweis: Schreibe $f = q(x - a) + r$ mit $deg(r) < 1$, also $r \in K$.
Wegen $0 = f(a) = q(a)(a - a) + r(a) = r(a) = r$ folgt $f = q(x - a)$. qed.

13.9 Bemerkungen:

(a) Ein Polynom $f \in K[x]$ vom Grad n besitzt höchstens n verschiedene Nullstellen.

(b) Ist $f = (x - a)^m \cdot g$ mit $g(a) \neq 0$, so heißt a eine Nullstelle der Vielfachheit m von f.

(c) Man kann f darstellen in der Form $f = (x - a_1)^{m_1} \cdots (x - a_k)^{m_k} \cdot g$ mit paarweise verschiedenen Nullstellen $a_1, \ldots, a_k$ und mit $g \in K[x]$ ohne Nullstellen.
Dabei gilt $m_1 + \ldots + m_k \leq deg(f)$.

13.10 Beispiele:

(a) Das Polynom $x^2 + 1 \in \mathbb{R}[x]$ besitzt keine Nullstellen.

(b) Das Polynom $x^2 + 1 \in \mathbb{C}[x]$ erfüllt $x^2 + 1 = (x - i)(x + i)$.

(c) Das Polynom $x^2 + 1 \in \mathbb{F}_2[x]$ erfüllt $x^2 + 1 = (x + 1)^2$.

(d) In $\mathbb{Q}[x]$ gilt $x^3 - 1 = (x - 1)(x^2 + x + 1)$ und $x^2 + x + 1$ besitzt keine Nullstellen in $\mathbb{Q}$.

13.11 Definition:

Sei $f = a_0 + a_1x + \ldots + a_nx^n \in K[x]$ mit $a_i \in K$ und $a_n \neq 0$.

(a) Die Zahl $LC(f) = a_n$ heißt der Leitkoeffizient (oder Gradkoeffizient, engl. „leading coefficient“) von f.

(b) Das Polynom f heißt normiert, wenn $LC(f) = 1$ gilt.

(c) Sei $g \in K[x]$. Ein Polynom $h \in K[x]$ heißt größter gemeinsamer Teiler (ggT) von f und g, wenn gilt:

1.) $h \mid f$ und $h \mid g$

2.) Ist $\tilde{h} \in K[x]$ mit $\tilde{h} \mid f$ und $\tilde{h} \mid g$, so folgt $\tilde{h} \mid h$.

3.) h ist normiert.

13.12 Satz: (Der euklidische Algorithmus für Polynome)

Seien $f, g \in K[x]$. Betrachte die folgenden Instruktionen:

(a) Ist $f = g = 0$, so gib $h = 0$ aus und stoppe.

(b) Ist $f = 0$, so gib $h = \frac{1}{LC(g)} \cdot g$ aus und stoppe.

(c) Ist $g = 0$, so gib $h = \frac{1}{LC(f)} \cdot f$ aus und stoppe.

(d) Ist $LC(f) \neq 1$, so ersetze f durch $\frac{1}{LC(f)} \cdot f$.

(e) Ist $LC(g) \neq 1$, so ersetze g durch $\frac{1}{LC(g)} \cdot g$.

(f) Ist $deg(f) < deg(g)$, so vertausche f und g.

(g) Berechne eine Darstellung $f = qg + r$ mit $q, r \in K[x]$ und $deg(r) < deg(g)$.

(h) Gilt $r = 0$, so gib $h = g$ aus und stoppe.

(i) Ersetze (f, g) durch $(g, \frac{1}{LC(r)} \cdot r)$ und fahre mit (g) fort.

Dies ist ein Algorithmus, der $h = ggT(f, g)$ berechnet.

Beweis: Analog zum Beweis von Satz 12.9. qed.

13.13 Beispiel:

(a) Wir berechnen $ggT(x^4 - 1, x^3 - x^2 + x - 1)$ in $\mathbb{Q}[x]$:

(g)
$$\begin{array}{rl} \left(x^4 - 1\right) \div \left(x^3 - x^2 + x - 1\right) = x + 1 \\ \underline{-x^4 + x^3 - x^2 + x} \\ x^3 - x^2 + x - 1 \\ \underline{-x^3 + x^2 - x + 1} \\ 0 \end{array}$$

(h) Gib $h = x^3 - x^2 + x - 1$ aus. Dies ist $ggT(f, g)$.

(b) Wir berechnen $ggT(2x^3+2x, x^4+x^3)$ in $\mathbb{Q}[x]$.

(d) Setze $f = x^3+x$, $g = x^4+x^3$

(f) Setze $f = x^4+x^3$, $g = x^3+x$

(g)
$$\begin{array}{rr} \left(x^4+x^3 \right) \div \left(x^3+x\right) = x+1+\dfrac{-x^2-x}{x^3+x} \\ \underline{-x^4 \quad -x^2} \\ x^3-x^2 \\ \underline{-x^3 \quad -x} \\ -x^2-x \end{array}$$

Also gilt $f = qg + r = (x+1)g + (-x^2-x)$

(i) Setze $f = x^3+x$, $g = \dfrac{1}{-1}\cdot(-x^2-x) = x^2+x$

(g)
$$\begin{array}{rr} \left(x^3 \quad +x \right) \div \left(x^2+x\right) = x-1+\dfrac{2x}{x^2+x} \\ \underline{-x^3-x^2} \\ -x^2+x \\ \underline{x^2+x} \\ 2x \end{array}$$

Also gilt $x^3+x = (x-1)(x^2+x)+2x$

(i) Setze $f = x^2+x$, $g = x$

(g) $(x^2+x) \div (x) = x+1$ Rest 0

(h) Gib $h = x$ aus und stoppe.

Also gilt $x = ggT(f,g)$.

13.14 Satz:

Der Ring $K[x]$ ist ein Hauptidealbereich.

Beweis: Wir wissen schon, dass $K[x]$ ein Integritätsbereich ist.
Sei $I \subseteq K[x]$ ein Ideal. O.E. gelte $I \neq \{0\}$. Sei $f \in I \setminus \{0\}$ ein Polynom kleinsten Grades. Dann sei $\tilde{f} = \dfrac{1}{LC(f)} \cdot f$ das normierte Polynom kleinsten Grades in I.
Dieses Polynom $\tilde{f}$ ist eindeutig bestimmt, denn wären $\tilde{f}, \tilde{g} \in I$ zwei verschiedene normierte Polynome kleinsten Grades, so wäre $\tilde{f} - \tilde{g} \in I$ ein Polynom kleineren Grades. $\lightning$
Wir behaupten nun, dass $I = K[x] \cdot \tilde{f}$ gilt.

„$\supseteq$“ klar

„$\subseteq$“ Sei $h \in I \setminus \{0\}$. Wegen der Minimalität von $deg(f)$ gilt $deg(h) \geq deg(f)$. Schreibe $h = q\tilde{f} + r$ mit $q, r \in K[x]$ und $deg(r) < deg(f)$. Wegen $r = h - q\tilde{f} \in I$ und der Minimalität von $deg(\tilde{f})$ folgt $r = 0$. Dies zeigt $h = q\tilde{f} \in K[x] \cdot \tilde{f}$. qed.

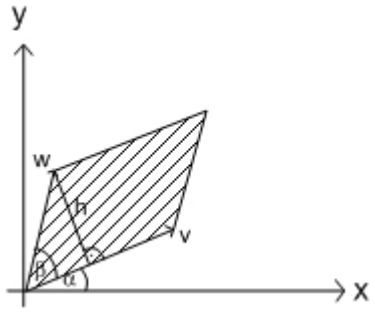
Kapitel IV: Auf zum Hornberger Schießen

14 Die Zahl, die alles wusste (Die Determinante)

A. Was weiß diese Zahl alles?

14.1 Beispiel:

Wir berechnen den Flächeninhalt eines Parallelogramms in der Ebene $\mathbb{R}^2$.
Skizze:



Es gelte $v = (a, b)$ und $w = (c, d)$
mit $a, b, c, d \in \mathbb{R}$

Dann folgt $v = \|v\| \cdot (cos(\alpha), sin(\alpha))$
und $w = \|w\| \cdot (cos(\beta), sin(\beta))$

Dies liefert $A = h \cdot \|v\| = \|v\| \cdot \|w\| \cdot sin(\beta - \alpha)$
$= \|v\| \cdot \|w\| \cdot (cos(\alpha)sin(\beta) - cos(\beta)sin(\alpha)) = ad - bc$
Also $A = |ad - bc|$
(Man nimmt den Absolutbetrag, damit die Fläche ≥ 0 ist.)

14.2 Beispiel:

Gegeben sei ein LGS über $\mathbb{Q}$:

$$\begin{array}{ll} (I) & \left\{ \begin{array}{rcrcl} ax & + & by & = & e \\ cx & + & dy & = & f \end{array} \right. \end{array} \text{ mit } a, b, c, d, e, f \in \mathbb{Q}$$

1.) Bilde $d \cdot (I) - b \cdot (II)$ und erhalte: $(ad - bc)x = ed - bf$

2.) Bilde $a \cdot (II) - c \cdot (I)$ und erhalte: $(ad - bc)y = af - ec$

Gilt $ad - bc \neq 0$, so folgt $x = \dfrac{ed - bf}{ad - bc}$ und $y = \dfrac{af - ec}{ad - bc}$
Gilt $ad - bc = 0$, so besitzt das LGS keine oder unendlich viele Lösungen.

B. Wie kann man dies verallgemeinern?

Im Folgenden sei K ein Körper.

14.3 Definition:

Eine Abbildung $det : Mat_n(K) \to K$ heißt Determinantenfunktion, wenn sie die folgenden Eigenschaften besitzt:

(a) Die Abbildung det ist linear in jeder Zeile. Dies heißt, dass für eine Matrix $A \in Mat_n(K)$ mit den Zeilen $z_1, \ldots, z_n$ gilt:

1.) Ist $z_i = z_i' + z_i''$, so folgt

$$det\begin{pmatrix} z_1 \\ \vdots \\ z_i' + z_i'' \\ \vdots \\ z_n \end{pmatrix} = det\begin{pmatrix} z_1 \\ \vdots \\ z_i' \\ \vdots \\ z_n \end{pmatrix} + det\begin{pmatrix} z_1 \\ \vdots \\ z_i'' \\ \vdots \\ z_n \end{pmatrix}$$

2.) Ist $\lambda \in K$, so folgt

$$det\begin{pmatrix} z_1 \\ \vdots \\ \lambda z_i \\ \vdots \\ z_n \end{pmatrix} = \lambda \cdot det\begin{pmatrix} z_1 \\ \vdots \\ z_i \\ \vdots \\ z_n \end{pmatrix}$$

Man sagt auch, dass *det* n-multilinear in den Zeilen sein muss.

(b) Die Abbildung *det* ist alternierend in den Zeilen, d.h. gilt $z_i = z_j$ mit $i \neq j$, so folgt

$$det\begin{pmatrix} \vdots \\ z_i \\ \vdots \\ z_j \\ \vdots \end{pmatrix} = 0$$

(c) Die Abbildung *det* ist normiert durch $det(I_n) = 1$.

14.4 Beispiel:

Die Abbildung $det : Mat_n(K) \to K$, $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto ad - bc$ ist eine Determinantenfunktion.

(a) 1.) $$det\begin{pmatrix} a' + a'' & b' + b'' \\ c & d \end{pmatrix} = (a' + a'')d - (b' + b'')c = (a'd - b'c) + (a''d - b''c)$$

$$= det\begin{pmatrix} a' & b' \\ c & d \end{pmatrix} + det\begin{pmatrix} a'' & b'' \\ c & d \end{pmatrix}$$

$$det\begin{pmatrix} a & b \\ c' + c'' & d' + d'' \end{pmatrix} = a(d' + d'') - b(c' + c'') = (ad' - bc') + (ad'' - bc'')$$

$$= det\begin{pmatrix} a & b \\ c' & d' \end{pmatrix} + det\begin{pmatrix} a & b \\ c'' & d'' \end{pmatrix}$$

2.) $det\begin{pmatrix} \lambda a & \lambda b \\ c & d \end{pmatrix} = \lambda ad - \lambda bc = \lambda(ad-bc) = \lambda \cdot det\begin{pmatrix} a & b \\ c & d \end{pmatrix}$

$det\begin{pmatrix} a & b \\ \lambda c & \lambda d \end{pmatrix} = a(\lambda d) - b(\lambda c) = \lambda(ad-bc) = \lambda \cdot det\begin{pmatrix} a & b \\ c & d \end{pmatrix}$

(b) $det\begin{pmatrix} a & b \\ a & b \end{pmatrix} = ab - ab = 0$

(c) $det\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1 \cdot 1 - 0 \cdot 0 = 1$

Ziel: Zeige, dass es für jedes $n \geq 1$ eine Determinantenfunktion $det : Mat_n(K) \to K$ gibt und diese eindeutig bestimmt ist.

14.5 Satz: (Eigenschaften einer Determinantenfunktion)

Sei $det : Mat_n(K) \to K$ eine Determinantenfunktion und $A \in Mat_n(K)$.

(a) Für $\lambda \in K$ gilt $det(\lambda A) = \lambda^n \cdot det(A)$.

(b) Ist eine Zeile von A gleich Null, so gilt $det(A) = 0$.

(c) Entsteht B aus A durch Vertauschung zweier Zeilen, so gilt $det(B) = -det(A)$.

(d) Entsteht B aus A indem man das λ-fache der i-ten Zeile zur j-ten Zeile addiert (mit $i \neq j$ und $\lambda \in K$), so gilt $det(B) = det(A)$.

(e) Ist A eine Diagonalmatrix, d.h.

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ & \ddots & \ddots & \vdots \\ & & \ddots & a_{n-1,n} \\ 0 & & & a_{nn} \end{pmatrix}, \text{ so gilt } det(A) = a_{11} \cdot a_{22} \cdots a_{nn}.$$

Beweis: Seien $z_1, \ldots, z_n$ die Zeilen von A.

(a) $det(\lambda A) = det\begin{pmatrix} \lambda z_1 \\ \vdots \\ \lambda z_n \end{pmatrix} = \lambda \cdot det\begin{pmatrix} z_1 \\ \lambda z_2 \\ \vdots \\ \lambda z_n \end{pmatrix} = \ldots = \lambda^n \cdot det\begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} = \lambda^n \cdot det(A)$

(b) Sei $z_i = 0$. Dann gilt:

$$0 = 0 \cdot det(A) = det\begin{pmatrix} z_1 \\ \vdots \\ 0 \cdot z_i \\ \vdots \\ z_n \end{pmatrix} = det\begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} = det(A)$$

(c) Sei $1 \leq i < j \leq n$. Dann gilt:

$$det(A) + det(B) = det \begin{pmatrix} \vdots \\ z_i \\ \vdots \\ z_j \\ \vdots \end{pmatrix} + det \begin{pmatrix} \vdots \\ z_j \\ \vdots \\ z_i \\ \vdots \end{pmatrix} + det \begin{pmatrix} \vdots \\ z_i \\ \vdots \\ z_i \\ \vdots \end{pmatrix} + det \begin{pmatrix} \vdots \\ z_j \\ \vdots \\ z_j \\ \vdots \end{pmatrix}$$

$$= det \begin{pmatrix} \vdots \\ z_i + z_j \\ \vdots \\ z_j \\ \vdots \end{pmatrix} + det \begin{pmatrix} \vdots \\ z_i + z_j \\ \vdots \\ z_i \\ \vdots \end{pmatrix} = det \begin{pmatrix} \vdots \\ z_i + z_j \\ \vdots \\ z_i + z_j \\ \vdots \end{pmatrix} = 0$$

(d) Die j-te Zeile von B ist $z_j + \lambda z_i$. Es gilt:

$$det(B) = det \begin{pmatrix} \vdots \\ z_i \\ \vdots \\ z_j + \lambda z_i \\ \vdots \end{pmatrix} = det \begin{pmatrix} \vdots \\ z_i \\ \vdots \\ z_j \\ \vdots \end{pmatrix} + \lambda \cdot det \begin{pmatrix} \vdots \\ z_i \\ \vdots \\ z_i \\ \vdots \end{pmatrix} = det(A)$$

(e) Sind alle $a_{ii} \neq 0$, so kann man A mit elementaren Zeilenoperatioen vom Typ E in eine Diagonalmatrix

$A = \begin{pmatrix} a_{11} & & 0 \\ & \ddots & \\ 0 & & a_{nn} \end{pmatrix}$ überführen. Also gilt:

$$det(A) = det \begin{pmatrix} a_{11} & & 0 \\ & \ddots & \\ 0 & & a_{nn} \end{pmatrix} = a_{11} \cdots a_{nn} \cdot det(I_n) = a_{11} \cdots a_{nn}$$

Sei nun $a_{ii} = 0$ mit i maximal. Mit Hilfe elementarer Zeilenoperationen vom Typ E kann man dann die i-te Zeile ausräumen und (b) liefert die Behauptung. qed.

14.6 Korollar:

Für jedes $n \geq 1$ gibt es höchstens eine Determinantenfunktion $det : Mat_n(K) \to K$.

Beweis: Sei $A \in Mat_n(K)$. Mit Hilfe von elementaren Zeilenumformungen kann man A in eine Matrix B in Zeilenstufenform überühren. Nach Satz 14.5 ist $det(A)$ durch $det(B)$ eindeutig bestimmt. Nach Teil (e) des Satzes ist $det(B)$ eindeutig bestimmt. qed.

14.7 Theorem: (Leibnizsche Determinantenformel)

Für $A \in Mat_n(K)$ definiere $det(A) = \sum_{\sigma \in S_n} sign(\sigma) \cdot a_{1,\sigma(1)} \cdot a_{2,\sigma(2)} \cdots a_{n,\sigma(n)}$

Dann ist $det : Mat_n(K) \to K$ eine Determinantenfunktion.

Beweis:

n-multilinear / alternierend: Nachrechnen, vgl. Beutelspacher

normiert: Was ist $det(I_n)$?
Für jede Permutation $\sigma \in S_n$ mit $\sigma \neq id$ gibt es ein i mit $\sigma(i) \neq i$. Für ein solches i gilt $a_{i,\sigma(i)} = 0$. Also bleibt nur der eine Summand mit $\sigma = id$ übrig und es gilt
$det(I_n) = sign(id) \cdot a_{11} \cdots a_{nn} = 1 \cdot 1 \cdots 1 = 1.$ qed.

14.8 Beispiel:

Sei $n = 2$ und $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$

Dann gilt: $det(A) = sign(id)a_{11}a_{22} + sign(\tau)a_{12}a_{21} = a_{11}a_{22} - a_{12}a_{21}$
(Unser guter alter Bekannter!), denn $S_2 = \{id, \tau\}$ mit $\tau = \begin{pmatrix} 1 & 2 \end{pmatrix}$

14.9 Bemerkung:

Die Leibniz-Formel ist für die Berechnung von Determinanten ungeeignet, da sie $\#S_n = n!$ Summanden hat.

C. Wie kann man Determinanten bestimmen?

14.10 Bemerkung: (Determinantenberechnung, die erste)

Sei $A \in Mat_n(K)$.

(a) Mit elementaren Zeilenumformungen kann man A in Zeilenstufenform bringen.

- Beim Typ P ändert sich das Vorzeichen von $det(A)$.
- Beim Typ D wird $det(A)$ mit einer Zahl $\lambda \in K$ multipliziert.
- Beim Typ E ändert sich $det(A)$ nicht.

(b) Am Ende erhalten wir eine Matrix B in Zeilenstufenform. Nach Satz 14.5.e ist $det(B)$ das Produkt der Elemente auf der Hauptdiagonalen.

14.11 Beispiel:

Sei $A = \begin{pmatrix} 1 & 2 & 5 \\ 3 & 0 & -1 \\ 2 & 4 & 9 \end{pmatrix}$ Dann gilt:

$$det(A) = det \begin{pmatrix} 1 & 2 & 4 \\ 0 & -6 & -16 \\ 0 & 0 & -1 \end{pmatrix} = 1 \cdot (-6) \cdot (-1) = 6$$

14.12 Notation:

Sei $A = (a_{ij}) \in Mat_n(K)$ und seien $i, j \in \{1, \ldots, n\}$
Mit A'_{ij} bezeichnen wir die Matrix, die dadurch entsteht, dass man in A die i-te Zeile und die j-te Spalte streicht.

Skizze:

$$A'_{ij} = \begin{pmatrix} a_{11} & \cdots & \cancel{a_{1j}} & \cdots & a_{1n} \\ \vdots & & \vdots & & \vdots \\ \cancel{a_{i1}} & \cdots & \cancel{a_{ij}} & \cdots & \cancel{a_{in}} \\ \vdots & & \vdots & & \vdots \\ a_{n1} & & \cancel{a_{nj}} & & a_{nn} \end{pmatrix} \in Mat_n(K)$$

14.13 Satz: (Entwicklungssatz nach Laplace)

Sei $n \geq 2$ und $A \in Mat_n(K)$.

(a) (Entwicklung nach der i-ten Zeile) Sei $i \in \{1, \ldots, n\}$
Es gilt: $det(A) = \sum_{j=1}^{n} (-1)^{i+j} \cdot a_{ij} \cdot det(A'_{ij})$

(b) (Entwicklung nach der j-ten Zeile) Sei $j \in \{1, \ldots, n\}$
Es gilt: $det(A) = \sum_{i=1}^{n} (-1)^{i+j} \cdot a_{ij} \cdot det(A'_{ij})$

Die Vorzeichen merkt man sich dabei nach der Schachbrettregel:

$$\begin{matrix} + & - & + & - & \cdots \\ - & + & - & + & \cdots \\ + & - & + & - & \cdots \\ \vdots & \vdots & \vdots & \vdots & \end{matrix}$$

Beweisidee: Zeige jeweils, dass die Formel auf der rechten Seite eine Determinantenfunktion darstellt. qed.

14.14 Beispiel:

Wir berechnen $det \begin{pmatrix} 1 & 2 & 5 \\ 3 & 0 & -1 \\ 2 & 4 & 9 \end{pmatrix}$ durch Entwicklung nach der zweiten Zeile:

$$det \begin{pmatrix} 1 & 2 & 5 \\ 3 & 0 & -1 \\ 2 & 4 & 9 \end{pmatrix} = -3 \cdot det \begin{pmatrix} 2 & 5 \\ 4 & 9 \end{pmatrix} + 0 \cdot \begin{pmatrix} 1 & 5 \\ 2 & 9 \end{pmatrix} - (-1) \cdot det \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}$$

$$= -3 \cdot (18 - 20) - (-1) \cdot 0 = 6$$

14.15 Satz:

Für $A \in Mat_n(K)$ gilt: $det(A^{tr}) = det(A)$.

Beweis: Sei $A = (a_{ij})$. Dann gilt $A^{tr} = (\tilde{a}_{ij})$ mit $\tilde{a}_{ij} = a_{ji}$ und
$det(A^{tr}) = \sum_{\sigma \in S_n} sign(\sigma) \tilde{a}_{1,\sigma(1)} \cdots \tilde{a}_{n,\sigma(n)} = \sum_{\sigma \in S_n} sign(\sigma) a_{\sigma(1),1} \cdots a_{\sigma(n),n}$
$= \sum_{\sigma \in S_n} sign(\sigma^{-1}) a_{1,\sigma^{-1}(1)} \cdots a_{n,\sigma^{-1}(n)} = \sum_{\sigma \in S_n} sign(\sigma) a_{1,\sigma(1)} \cdots a_{n,\sigma(n)}$ qed.

Dabei haben wir folgendes verwendet:

1.) $sign(\sigma^{-1}) = sign(\sigma)$, denn $sign(\sigma^{-1}) \cdot sign(\sigma) = sign(\sigma^{-1} \cdot \sigma) = sign(id) = 1$

2.) $a_{\sigma(1),1} \cdots a_{\sigma(n),n} = a_{1,\sigma^{-1}(1)} \cdots a_{n,\sigma^{-1}(n)}$ mit permutierten Faktoren

3.) Wenn σ die Gruppe S_n durchläuft, dann durchläuft auch σ^{-1} die Gruppe S_n genau einmal.

14.16 Satz: (Determinanten und elementare Spaltenoperationen)

Sei $A \in Mat_n(K)$ eine Matrix mit den Spalten $s_1, \ldots, s_n$. Dann gilt:

(a) Entsteht eine Matrix B aus A, indem man die j-te Spalte von A mit $\lambda \in K$ multipliziert, d.h. gilt $B = (s_1, \ldots, \lambda s_j, \ldots, s_n)$, so folgt $det(B) = \lambda det(A)$.

(b) Entsteht B aus A, indem man die i-te und die j-te Spalte von A vertauscht, d.h. gilt $B = (\ldots, \underbrace{s_j}_{\text{i-te Spalte}}, \ldots, \underbrace{s_i}_{\text{j-te Spalte}}, \ldots)$, so folgt $det(B) = -det(A)$.

(c) Entsteht B aus A, indem man das λ-fache der j-ten Spalte von A zur k-ten Spalte von B addiert, d.h. gilt $B = (\ldots, s_j, \ldots, \underbrace{s_k + \lambda s_j}_{\text{k-te Spalte}}, \ldots)$, so folgt $det(B) = det(A)$.

Beweis: Verwende $det(A) = det(A^{tr})$ und $det(B) = det(B^{tr})$ und Satz 14.5. qed.

14.17 Beispiel:

Wir berechnen $det \begin{pmatrix} 1 & 2 & 3 \\ 1 & 4 & 9 \\ 1 & 8 & 27 \end{pmatrix}$ mit Spaltenoperationen:

$$det \begin{pmatrix} 1 & 2 & 3 \\ 1 & 4 & 9 \\ 1 & 8 & 27 \end{pmatrix} = det \begin{pmatrix} 1 & 0 & 0 \\ 1 & 2 & 6 \\ 1 & 6 & 24 \end{pmatrix} = \ldots = det \begin{pmatrix} 1 & 0 & 0 \\ 1 & 2 & 0 \\ 1 & 6 & 6 \end{pmatrix} = 1 \cdot 2 \cdot 6 = 12$$

14.18 Satz: (Der Multiplikationssatz für Determinanten)

Für $A, B \in Mat_n(K)$ gilt: $det(AB) = det(A) \cdot det(B)$.

Beweis: Wir bringen A mit elementaren Zeilen- und Spaltenoperationen vom Typ E in Diagonalgestalt. Für die Ergebnismatrix D gilt $det(D) = det(A)$ und $rang(D) = rang(A)$.

1. Fall: $rang(A) < n$. Seien $f_A, f_B : K^n \to K^n$ die assoziierten linearen Abbildungen. Dann gilt $rang(A) = dim_K(Bild(f_A))$ und $Bild(f_A \circ f_B) \subseteq Bild(f_A)$.
Also ergibt sich $rang(AB) = dim_K(Bild(f_A \circ f_B)) \subseteq dim_K(Bild(f_A)) = rang(A)$.
Somit sind die Spalten von AB linear abhängig. Durch geeignete Spaltenoperationen kann man in AB eine Nullspalte erzeugen. Dies liefert $det(AB) = 0$.
Ebenso gilt $det(A) = 0$, also die Behauptung.

2. Fall: $rang(A) = n$. In der Diagonalmatrix D stehen auf der Hauptdiagonalen nur Elemente ungleich Null. Dies zeigt $det(A) = det(D) \neq 0$. Schreibe $A = E_1 \cdots E_s \cdot D$ mit Elementarmatrizen E_i. Dann gilt $AB = E_1 \cdots E_s \cdot D \cdot B$, d.h. auch AB entsteht aus DB durch elementare Zeilenumformungen vom Typ E.

Somit folgt $det(A) = det(D)$ und $det(AB) = det(DB)$. Schreibe $D = \begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{pmatrix}$.

Die Multiplikation DB bewirkt, dass die i-te Zeile von B mit d_i multipliziert wird. Also folgt $det(DB) = d_1 \cdots d_n \cdot det(B) = det(D) \cdot det(B)$. qed.

14.19 Korollar: (Determinante der inversen Matrix)

(a) Ist $A \in GL_n(K)$, so gilt $det(A^{-1}) = det(A)^{-1}$.

(b) Die Abbildung $det : GL_n(K) \to K^x$ ist ein Gruppenhomomorphismus.

Beweis:

(a) Nach Satz 14.18 gilt $det(A) \cdot det(A^{-1}) = det(A \cdot A^{-1}) = det(I_n) = 1$.

(b) Folgt sofort aus Satz 14.18. qed.

14.20 Bemerkung:

Aus Satz 14.18 folgt, dass $SL_n(K) = \{A \in GL_n(K) \mid det(A) = 1\}$ eine Gruppe ist. Sie heißt die spezielle lineare Gruppe.

D. Was weiß die Zahl $det(A)$ denn nun wirklich?

14.21 Satz:

Für $A \in Mat_n(K)$ sind die folgenden Bedingungen äquivalent:

(a) $det(A) \neq 0$

(b) A ist invertierbar, d.h. $A \in Mat_n(K)$ ist eine Einheit.

(c) Die Zeilen von A sind linear unabhängig.

(d) Die Spalten von A sind linear unabhängig.

(e) Es gilt $rang(A) = n$.

Beweis: „(c)⇔(d)“ Folgt aus 7.16.c (Spaltenrang = Zeilenrang).

„(d)⇔(e)“ Ist die Definition von $rang(A)$.

„(a)⇒(b)“ Bringe A mit elementaren Zeilenumformungen vom Typ E und P in Zeilenstufenform und erhalte die Matrix D. Es gilt $det(D) = \pm det(A) \neq 0$. Also sind die Hauptdiagonalelemente von D alle $\neq 0$ und D ist invertierbar. Da A sich von D nur um ein Produkt von Elementarmatrizen unterscheidet, ist auch A invertierbar.

„(b)⇒(d)“ Ist A invertierbar, so ist die bezüglich der Standardbasis assoziierte lineare Abbildung $f_A : K^n \to K^n$ ein Isomorphismus von Vektorräumen. Insbesondere gilt $Bild(f_A) = K^n$, d.h. die Spalten von A sind eine Basis des K^n.

„(d)⇒(a)“ Nach Vorraussetzung ist die zu A assoziierte lineare Abbildung $f_A : K^n \to K^n$ surjektiv. Also ist f_A auch bijektiv, d.h. f_A ist ein Isomorphismus und A ist invertierbar. Aus $det(A) \cdot det(A^{-1}) = det(AA^{-1}) = det(I_n) = 1$ folgt dann $det(A) \neq 0$. qed.

14.22 Satz:

Gegeben sei das LGS:

$$(*) \qquad A \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \text{ mit } b_1, \ldots, b_n \in K \text{ und } A \in Mat_n(K).$$

(a) Genau dann besitzt (*) eine Lösung, wenn $det(A) \neq 0$ gilt.

(b) (Cramersche Regel)

Sei $det(A) \neq 0$ und seien $s_1, \ldots, s_n \in K^n$ die Spalten von A. Dann ist die eindeutige Lösung von (*) gegeben durch:

$$x_1 = \frac{1}{det(A)} \cdot det((b, s_2, \ldots, s_n))$$

$$x_2 = \frac{1}{det(A)} \cdot det((s_1, b, s_3 \ldots, s_n))$$

$$\vdots$$

$$x_n = \frac{1}{det(A)} \cdot det((s_1, \ldots, s_{n-1}, b))$$

$$\text{mit } b = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$$

Beweis:

(a) Gilt $det(A) \neq 0$, so ist die Matrix A invertierbar und es gilt:

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = A^{-1} \cdot \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$$ Also besitzt (*) wie gewünscht eine eindeutige Lösung.

Umgekehrt besitze nun (*) eine eindeutige Lösung. Die Lösungen eines inhomogenen LGS sind von der Form

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} + \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix}$$

wobei $(y_1, \ldots, y_n)$ eine feste Lösung ist und $(z_1, \ldots, z_n)$ eine beliebige Lösung des zugehörigen homogenen LGS. Also besitzt auch das homogene LGS

$A \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0$ eine eindeutige Lösung, nämlich $(0, \ldots, 0)$.

Somit ist die zu A assoziierte lineare Abbildung $f_A : K^n \to K^n$ injektiv. Also ist f_A sogar bijektiv und A invertierbar. Dies liefert $det(A) \neq 0$ nach Satz 14.21.

(b) Für $i, j \in \{1, \ldots, n\}$ sei A_{ij} die Matrix

$$A_{ij} = \begin{pmatrix} a_{11} & \cdots & a_{1,j-1} & 0 & a_{1,j+1} & \cdots & a_{1n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{i-1,1} & \cdots & a_{i-1,j-1} & 0 & a_{i-1,j+1} & \cdots & a_{i-1,n} \\ 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \\ a_{i+1,1} & \cdots & a_{i+1,j-1} & 0 & a_{i+1,j+1} & \cdots & a_{i+1,n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{n1} & & & 0 & & & a_{nn} \end{pmatrix}$$

Indem man in A_{ij} geeignete Vielfache der j-ten Spalte zu den anderen Spalten addiert, erhält man die Matrix $(s_1, \ldots, s_{j-1}, e_i, s_{j+1}, \ldots, s_n)$.
Entwickelt man A_{ij} nach der i-ten Zeile, so folgt $det(A_{ij}) = (-1)^{i+j} det(A'_{ij})$. Seien $z_1, \ldots, z_n$ die Zeilen von A. Es folgt durch Entwicklung nach der k-ten Zeile

$$det \begin{pmatrix} z_1 \\ \vdots \\ z_i \\ \vdots \\ z_i \\ \vdots \\ z_n \end{pmatrix} = \sum_{j=1}^{n} (-1)^{k+j} a_{ij} det(A'_{kj}) = \delta_{ik} \cdot det(A)$$

Insgesamt erhalten wir für $i \in \{1, \ldots, n\}$

$$\sum_{j=1}^{n} a_{ij} \cdot \frac{1}{det(A)} \cdot det((s_1, \ldots, s_{j-1}, b, s_{j+1}, \ldots, s_n)) = \sum_{j=1}^{n} \sum_{k=1}^{n} a_{ij} \cdot \frac{1}{det(A)} (-1)^{k+j} b_k \cdot det(A'_{kj})$$

$$= \sum_{k=1}^{n} \frac{1}{det(A)} b_k \sum_{j=1}^{n} a_{ij} \cdot (-1)^{k+j} \cdot det(A'_{kj}) = \sum_{k=1}^{n} \frac{1}{det(A)} b_k \cdot \delta_{ik} \cdot det(A) = b_i$$

Also ist der gegebene Vektor $(x_1, \ldots, x_n)$ eine Lösung von (*). qed.

E. Ist das alles nicht viel zu Abstrakt?

Im Gegenteil. Es ist noch nicht abstrakt genug. Wir müssen die Determinante noch auf die besagten zwei Arten verallgemeinern.

14.23 Satz:

Sei V ein endlich-dimensionaler K-Vektorraum, seien B, C zwei Basen von V und $f : V \to V$ ein Endomorphismus.

(a) Für die Darstellungsmatrizen $M_B^B(f)$ und $M_C^C(f)$ gilt $det(M_B^B(f)) = det(M_C^C(f))$.

(b) Die Zahl $det(f) = det(M_B^B(f))$ ist wohldefiniert, d.h. sie hängt nicht von der Wahl der Basis B von V ab. Sie heißt die Determinante des Endomorphismus f.

Beweis:

(a) Nach der Basistransformationsformel gilt:
$M_C^C(f) = T_C^B \cdot M_B^B(f) \cdot (T_C^B)^{-1}$
Also folgt: $det(M_C^C(f)) = det(T_B^B) \cdot det(M_B^B(f)) \cdot det(T_B^B)^{-1} = det(M_B^B(f))$.

(b) Folgt aus (a). qed.

14.24 Definition:

Sei R ein kommutativer Ring mit Einselement und $n \geq 1$. Die Abbildung

$$\begin{array}{rcll} det : Mat_n(R) & \to & R & \text{heißt die Determinante über } R. \\ (a_{ij}) & \mapsto & \sum\limits_{\sigma \in S_n} sign(\sigma) \cdot a_{1,\sigma(1)} \cdots a_{n,\sigma(n)} & \end{array}$$

14.25 Satz:

Sei R ein Ring. Dann besitzt die Abbildung $det : Mat_n(R) \to R$ die folgenden Eigenschaften:

(a) Sie ist n-multilinear in den Zeilen von $A = (a_{ij})$.

(b) Sie ist alternierend in den Zeilen von A, d.h. besitzt A zwei gleiche Zeilen, so gilt $det(A) = 0$.

(c) Sie ist normiert durch $det(I_n) = 1$.

(d) Sie ist n-multilinear in den Spalten von A.

(e) Sie ist alternierend in den Spalten von A.

Beweis: Dies kann man wie im Fall eines Körpers mit Hilfe der Leibniz-Formel nachrechnen. qed.

14.26 Bemerkung:

Im nächsten Abschnitt benötigen wir diese allgemeine Definition. Wir werden das charakteristische Polynom eines Endomorphismus als Determinante einer Matrix über den Ring $R = K[x]$ definieren.

15 Über Charakterfragen und innere Werte (Das Charakteristische Polynom und Eigenwerte)

In diesem Abschnitt sei K ein Körper, V ein endlich-dimensionaler K-Vektorraum mit Basis $B = \{v_1, \ldots, v_n\}$ und $f : V \to V$ ein Endomorphismus mit Darstellungsmatrix $A = M_B^B(f) = (a_{ij}) \in Mat_n(K)$.

A. Was sind Eigenwerte und wieso braucht man sie?

15.1 Definition:

Ein Element $\lambda \in K$ heißt ein Eigenwert der Abbildung $f : V \to V$, wenn es einen Vektor $v \in V \setminus \{0\}$ gibt mit $f(v) = \lambda v$.

15.2 Beispiel:

Die Zahl $0 \in K$ ist genau dann ein Eigenwert von f, wenn es einen Vektor $v \in V \setminus \{0\}$ gibt mit $f(v) = 0$. Dies ist genau dann der Fall, wenn $Kern(f) \neq \{0\}$ gilt, d.h. wenn f nicht injektiv ist.

15.3 Beispiel:

Die Zahl $1 \in K$ ist genau dann ein Eigenwert von f, wenn es einen Vektor $v \in V \setminus \{0\}$ gibt mit $f(v) = v$. Ein solcher Vektor heißt Fixpunkt von f.

15.4 Beispiel:

Die $\mathbb{Q}$-lineare Abbildung $f : \mathbb{Q}^2 \to \mathbb{Q}^2$ mit $f(e_1) = e_2$ und $f(e_2) = -e_1$ ist die Drehung um 0 um 90°. Der einzige Vektor, der auf ein Vielfaches von sich abgebildet wird, ist $v = 0$. Also besitzt f keine Eigenwerte.

15.5 Beispiel:

Die $\mathbb{Q}$-lineare Abbildung $f : \mathbb{Q}^2 \to \mathbb{Q}^2$ mit $f(e_1) = e_2$ und $f(e_2) = e_1$ ist die Spiegelung an der Geraden $G = \{(a, a) \in \mathbb{Q}^2 \mid a \in \mathbb{Q}\}$. Die Vektoren, die auf ein Vielfaches von sich selbst abgebildet werden, sind dabei genau die Vektoren in G und die Vektoren in $H = \{(a, -a) \in \mathbb{Q}^2 \mid a \in \mathbb{Q}\}$. Also besitzt f die Eigenwerte λ und $-\lambda$.

15.6 Definition:

Sei $\lambda \in K$ ein Eigenwert von f.

(a) Ein Vektor $v \in V$ heißt Eigenvektor zum Eigenwert λ, wenn gilt: $f(v) = \lambda v$.

(b) Die Menge $Eig(f, \lambda) = \{v \in V \mid f(v) = \lambda v\}$ heißt der Eigenraum von f zum Eigenwert λ.

15.7 Satz:

Jeder Eigenraum von f ist ein K-Untervektorraum von V.

Beweis: Seien $v_1, v_2 \in Eig(f, \lambda)$ und $a_1, a_2 \in K$. Dann gilt:
$f(a_1v_1 + a_2v_2) = a_1f(v_1) + a_2f(v_2) = a_1\lambda v_1 + a_2\lambda v_2 = \lambda(a_1v_1 + a_2v_2)$,
d.h. es gilt $a_1v_1 + a_2v_2 \in Eig(f, \lambda)$. qed.

15.8 Beispiel:

Sei $f : \mathbb{Q}^2 \to \mathbb{Q}^2$ die Abbildung mit $f(e_1) = e_2$ und $f(e_2) = e_1$ die Spiegelung an der Winkelhalbierenden $G =< e_1 + e_2 >$. Dann gilt $Eig(f, 1) =< e_1 + e_2 >$ und $Eig(f, -1) =< e_1 - e_2 >$.

15.9 Beispiel:

Sei $\alpha \in [0, 2\pi)$. Die $\mathbb{R}$-lineare Abbildung $f : \mathbb{R}^3 \to \mathbb{R}^3$ mit Darstellungsmatrix

$M_E^E(f) = \begin{pmatrix} cos(\alpha) & -sin(\alpha) & 0 \\ sin(\alpha) & cos(\alpha) & 0 \\ 0 & 0 & 1 \end{pmatrix}$ ist die Drehung um die z-Achse um den Winkel α.

Der einzige Eigenwert ist $\lambda = 1$ und es gilt $Eig(f, 1) =< e_3 >$.

15.10 Definition:

(a) Ein Endomorphismus $f : V \to V$ heißt diagonalisierbar, wenn es eine Basis B von V gibt, so dass $M_B^B(f)$ eine Diagonalmatrix ist.

(b) Eine Matrix $A \in Mat_n(K)$ heißt diagonalisierbar, wenn es eine invertierbare Matrix $T \in GL_n(K)$ gibt, so dass TAT^{-1} eine Diagonalmatrix ist.

15.11 Satz:

(a) Ein Endomorphismus $f : V \to V$ ist genau dann diagonalisierbar, wenn eine (bzw. jede) seiner Darstellungsmatrizen diagonalisierbar ist.

(b) Ein Endomorphismus $f : V \to V$ ist genau dann diagonalisierbar, wenn es eine Basis von V gibt, die aus Eigenvektoren von f besteht.

Beweis:

(a) Folgt sofort aus der Transformationsformel.

(b) „⇒“ Sei $B = \{v_1, \ldots, v_n\}$ eine Basis von V, so dass

$M_B^B(f) = \begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{pmatrix}$ mit $d_1, \ldots, d_n \in K$ gilt. Dann gilt $f(v_i) = d_i \cdot v_i$ für $i = 1, \ldots, n$.

Somit besteht die Basis B aus Eigenvektoren von f.

„⇐“ Sei $B = \{v_1, \ldots, v_n\}$ eine Basis von V aus Eigenvektoren von f. Schreibe $f(v_i) = \lambda_i \cdot v_i$ mit $\lambda_i \in K$ für $i = 1, \ldots, n$ (die λ_i sind dabei nicht notwendigerweise verschieden). Dann gilt:

$$M_B^B(f) = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$$

qed.

15.12 Bemerkung:

Eigenwerte und Eigenvektoren spielen beim Lösen von Differentialgleichungssystemen eine große Rolle. Sei $I \subseteq \mathbb{R}$ ein offenes Intervall und $A = (a_{ij}) \in Mat_n(\mathbb{R})$. Gesucht sei der $\mathbb{R}$-Vektorraum aller Tupel $(f_1, \ldots, f_n) \in \underbrace{C^1(I, \mathbb{R})^n}$, die das folgende Differentialgleichungssystem lösen:

$$\begin{array}{rcl} \text{Vektorraum aller Funktionen } \varphi : I & \to & \mathbb{R} \\ t & \mapsto & \varphi(t) \end{array}$$

$$(*) \begin{cases} f_1' &= a_{11}f_1 + \ldots + a_{1n}f_n \\ \vdots & \\ f_n' &= a_{n1}f_1 + \ldots + a_{nn}f_n \end{cases}$$

Wir machen folgenden Lösungsansatz:

$\begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix} = \begin{pmatrix} c_1 e^{\lambda t} \\ \vdots \\ c_n e^{\lambda t} \end{pmatrix}$ mit $c_1, \ldots, c_n, \lambda \in \mathbb{R}$. Dann gilt $\begin{pmatrix} f_1' \\ \vdots \\ f_n' \end{pmatrix} = \begin{pmatrix} \lambda c_1 e^{\lambda t} \\ \vdots \\ \lambda c_n e^{\lambda t} \end{pmatrix} = \lambda \begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix}$

Dies bedeutet, dass folgende Gleichung gelten soll:

$\lambda e^{\lambda t} \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = A e^{\lambda t} \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}$ Somit ist $\lambda \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = A \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}$ zu lösen,

d.h. wir suchen einen Eigenvektor $v = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}$ zu einem Eigenwert λ von A.

15.13 Beispiel:

Gesucht seien die Lösungen in $C^1(\mathbb{R}, \mathbb{R})$ des Systems

$$(*) \begin{cases} f_1'(t) &= f_1(t) - f_2(t) \\ f_2'(t) &= 2f_1(t) + 4f_2(t) \end{cases}$$

Wir suchen also die Eigenwerte und Eigenvektoren von $A = \begin{pmatrix} 1 & -1 \\ 2 & 4 \end{pmatrix}$

Die Eigenwerte sind $\lambda_1 = 2$ und $\lambda_2 = 3$. Dabei gilt $Eig(f_A, 2) =< (1, -1) >$ und $Eig(f_A, 3) =< (1, -2) >$.

Damit sind die Funktionen $\begin{pmatrix} f_1 \\ f_2 \end{pmatrix} = c_1 e^{\lambda t} \begin{pmatrix} 1 \\ -1 \end{pmatrix} + c_2 e^{\lambda t} \begin{pmatrix} 1 \\ -2 \end{pmatrix} = \begin{pmatrix} c_1 e^{2t} + c_2 e^{3t} \\ -c_1 e^{2t} - 2c_2 e^{3t} \end{pmatrix}$

mit $c_1, c_2 \in \mathbb{R}$ Lösungen von $(*)$.

B. Wie kann man Eigenwerte und Eigenvektoren berechnen?

15.14 Satz:

(a) Seien $\lambda_1, \ldots, \lambda_m \in K$ paarweise verschiedene Eigenwerte von f und sei $v_i \in V \setminus \{0\}$ ein Eigenvektor zu λ_i für $i = 1, \ldots, m$. Dann ist $\{v_1, \ldots, v_m\}$ linear unabhängig.

(b) Die Summe von Untervektorräumen $\sum_{i=1}^{m} Eig(f, \lambda_i)$ ist direkt,
d.h. für $i = 1, \ldots, m$ gilt $Eig(f, \lambda_i) \cap \sum_{j \neq i}^{m} Eig(f, \lambda_j) = \{0\}$.
(Schreibweise: $Eig(f, \lambda_1) \oplus \ldots \oplus Eig(f, \lambda_m) \subseteq V$)

Beweis:

(a) Wir schließen mit vollständiger Induktion nach m.

$m = 1$: Aus $v_1 \neq 0$ folgt, dass $\{v_1\}$ linear unabhängig ist.

$m > 1$: Seien $a_1, \ldots, a_m \in K$ und $a_1 v_1 + \ldots + a_m v_m = 0$. Dann gilt
$0 = f(a_1 v_1 + \ldots + a_m v_m) = a_1 f(v_1) + \ldots + a_m f(v_m) = a_1 \lambda_1 v_1 + \ldots + a_m \lambda_m v_m$
und $0 = a_1 \lambda_m v_1 + \ldots + a_m \lambda_m v_m$
Daraus folgt: $(\lambda_1 - \lambda_m) a_1 v_1 + \ldots + (\lambda_{m-1} - \lambda_m) a_{m-1} v_{m-1} = 0$.
Die Induktionsvoraussetzung liefert $(\lambda_1 - \lambda_m) a_1 = 0, \ldots, (\lambda_{m-1} - \lambda_m) a_{m-1} = 0$.
Wegen $\lambda_i \neq \lambda_1$ für $i = 1, \ldots, m$ folgt $a_1 = \ldots = a_{m-1} = 0$. Nun zeigt $a_m v_m = 0$, dass auch $a_m = 0$ gilt.

(b) Ergibt sich wie folgt aus (a):

Angenommen, es existiert ein Vektor $v \neq 0$ mit $v \in Eig(f, \lambda_i)$ und $v \in \sum_{j \neq i}^{m} Eig(f, \lambda_j)$.

Schreibe $v = v_1 + \ldots + \widehat{v_i} + \ldots + v_m$ mit $v_j \in Eig(f, \lambda_i)$.
Nun liefert $v - v_1 - \ldots - v_m = 0$ einen Widerspruch zu (a). qed.

15.15 Satz:

Sei $\lambda \in K$ ein Eigenvektor von f. Dann gilt:
$Eig(f, \lambda) = Kern(f - \lambda \cdot id_V)$.

Beweis: Für $v \in V$ gilt $v \in Eig(f, \lambda)$ genau dann, wenn $f(v) = \lambda v$ ist, also $(f - \lambda id_V)(v) = 0$ erfüllt ist. Dies ist somit äquivalent mit $v \in Kern(f - \lambda id_V)$. qed.

15.16 Definition:

Sei $A = (a_{ij}) \in Mat_n(K)$ und sei x eine Unbestimmte. Dann gilt:

$$A - x \cdot I_n = \begin{pmatrix} a_{11} - x & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} - x & \ddots & \vdots \\ \vdots & \ddots & \ddots & a_{n-1,n} \\ a_{n1} & \cdots & a_{n,n-1} & a_{nn} - x \end{pmatrix} \in Mat_n(K[x]).$$

Das Polynom $\chi_A(x) = det(A - xI_n)$ heißt das charakteristische Polynom der Matrix A.

15.17 Beispiel:

Für die Matrix $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in Mat_2(\mathbb{Q})$ gilt:

$\chi_A(x) = det \begin{pmatrix} -x & 1 \\ 1 & -x \end{pmatrix} = x^2 - 1.$

15.18 Satz:

Seien B, C zwei Basen von V. Dann gilt:
$\chi_{M_B^B(f)}(x) = \chi_{M_C^C(f)}(x)$. Dieses Polynom heißt das charakteristische Polynom von f und wird mit $\chi_f(x)$ bezeichnet. Es gilt also $\chi_f(x) = det(f - x \cdot id_V)$.

Beweis: Nach der Transformationsformel gilt $M_C^C(f) = T_C^B \cdot M_B^B(f) \cdot T_B^C$. Also folgt:
$\chi_{M_C^C(f)}(x) = det(M_C^C(f) - xI_n) = det(T_C^B \cdot M_B^B(f) \cdot T_B^C - T_C^B \cdot x \cdot T_B^C)$
$= det(T_C^B(M_B^B(f) - xI_n)T_B^C) = det(T_C^B) \cdot det(M_B^B(f) - xI_n) \cdot det(T_C^B)^{-1} = \chi_{M_B^B(f)}(x)$ qed.

15.19 Beispiel:

(a) Ist $f : \mathbb{R}^2 \to \mathbb{R}^2$ die Spiegelung an der Winkelhalbierenden $G =< e_1 + e_2 >$, so gilt
$\chi_f(x) = x^2 - 1$ (vgl. Beispiel 15.17 und verwende $M_E^E(f) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$)

(b) Ist $g : \mathbb{R}^2 \to \mathbb{R}^2$ die Drehung um 0 um einen Winkel $\alpha \in [0, 2\pi)$, so gilt:
$M_E^E(g) = \begin{pmatrix} cos(\alpha) & -sin(\alpha) \\ sin(\alpha) & cos(\alpha) \end{pmatrix}$ Dann folgt:
$\chi_g(x) = det \begin{pmatrix} cos(\alpha) - x & -sin(\alpha) \\ sin(\alpha) & cos(\alpha) - x \end{pmatrix} = (cos(\alpha) - x)^2 + sin^2(\alpha)$
$= cos^2(\alpha) - 2cos(\alpha)x + x^2 + sin^2(\alpha) = x^2 - 2cos(\alpha)x + 1$
(Beachte: Die Diskriminante ist $4cos^2(\alpha) - 4 \leq 0$)

15.20 Satz:

Eine Zahl $\lambda \in K$ ist genau dann ein Eigenwert von f, wenn $\chi_f(x) = 0$ gilt, d.h. wenn λ eine Nullstelle des charakteristischen Polynoms von f ist.

Beweis: Genau dann ist λ ein Eigenwert, wenn $Eig(f, \lambda) = Kern(f - \lambda id_V)$ gilt. Dies ist genau dann der Fall, wenn $f - \lambda id_V$ nicht injektiv ist, also wenn $\chi_f(x) = det(f - \lambda id_V) = 0$ gilt. qed.

15.21 Bemerkung:

Ein Polynom $f \in K[x] \setminus K$ braucht keine Nullstellen zu haben. Z.B. besitzt das Polynom $x^2 + a \in \mathbb{R}[x]$ keine Nullstellen. Über dem Körper $\mathbb{C}$ besitzt jedes Polynom $f \in \mathbb{C}[x] \setminus \mathbb{C}$ eine Darstellung $f = c(x - a_1) \cdots (x - a_n)$ mit $c, a_1, \ldots, a_n \in \mathbb{C}$
(„Fundamentalsatz der Algebra“ ↗ Analysis, Funktionentheorie).

15.22 Beispiel:

(a) Im Beispiel 15.19.a gilt $\chi_f = (x+1)(x-1)$. D.h. die Spiegelung an der Geraden $G =< e_1 + e_2 >$ besitzt die Eigenwerte $\lambda = 1$ und $\lambda = -1$.

(b) Im Beispiel 15.19.b besitzt die Drehung um O um den Winkel $\alpha \in [0, 2\pi)$ das charakteristische Polynom $\chi_g = x^2 - 2cos(\alpha)x + 1$. Dieses Polynom besitzt nur im Fall $cos(\alpha) = \pm 1$ eine Nullstelle. Somit besitzt g für $\alpha \notin \{0, \pi\}$ keine Eigenwerte.
Für $\alpha = 0$ ist $\lambda = 1$ der einzige Eigenwert von g.
Für $\alpha = \pi$ ist $\lambda = -1$ der einzige Eigenwert von g.

15.23 Satz:

Sei χ_f das charakteristische Polynom von f.

(a) Der Leitkoeffizient von χ_f ist $(-1)^n$ und es gilt $deg(\chi_f) = n$. Somit hat χ_f die Gestalt $\chi_f(x) = (-1)^n x^n + c_{n-1}x^{n-1} + \ldots + c_1 x + c_0$ mit $c_0, \ldots, c_{n-1} \in K$.

(b) Es gilt $\chi_f(0) = c_0 = det(f)$.

Beweis:

(a) Sei $A = (a_{ij}) \in Mat_n(K)$ die Darstellungsmatrix von f. Dann gilt:

$$\chi_f(x) = det \begin{pmatrix} a_{11} - x & a_{12} & \cdots & a_{1n} \\ a_{21} & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ a_{n1} & \cdots & \cdots & a_{nn} - x \end{pmatrix}$$

$= (a_{11} - x) \cdots (a_{nn} - x) + [\text{Terme niedrigeren Grades}] = (-x)^n + [\text{Terme niedrigeren Grades}]$.

(b) Es gilt $\chi_f(0) = det(a_{ij}) = det(f)$. qed.

15.24 Bemerkung:

Schreibe $\chi_f(x) = (-1)^n x^n + c_{n-1}x^{n-1} + \ldots + c_1 x + c_0$ mit $c_0, \ldots, c_{n-1} \in K$. Dann heißt der Koeffizient $tr(f) = (-1)^{n-1} c_{n-1}$ die Spur von f (engl. „trace“). Sie hängt nicht von der Wahl der Darstellungsmatrix von f ab. Ist $A = (a_{ij})$ eine Darstellungsmatrix von f, so gilt $tr(f) = a_{11} + \ldots + a_{nn}$.

16 Wenn jeder Vektor eine Menge ist (Restklassenvektorräume)

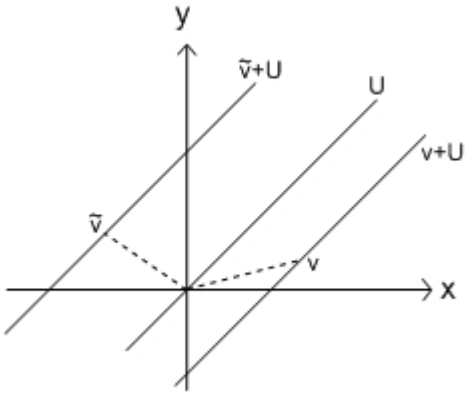
Im Folgenden sei K ein Körper, V ein (endlich-dimensionaler) K-Vektorraum und $U \subseteq V$ ein K-Untervektorraum.

16.1 Definition:

Für jeden Vektor $v \in V$ heißt $v + U = \{v + u \mid u \in U\}$ eine Nebenklasse von U und V. Jedes Element von $v + U$ heißt ein Repräsentant dieser Nebenklasse.

16.2 Beispiel:

Sei $K = \mathbb{R}$ und $V = \mathbb{R}^2$ die Zeichenebene.



Sei $U \subseteq \mathbb{R}$ eine Gerade durch O.
Dann sind die Nebenklassen von U grade die Parallelen zu U.

16.3 Satz: (Gleichheit von Nebenklassen)

(a) Für $v, \tilde{v} \in V$ gilt $v + U = \tilde{v} + U$ genau dann, wenn $v - \tilde{v} \in U$ erfüllt ist.

(b) Definiert man auf V eine Relation $\sim$ durch $v \sim \tilde{v} \Leftrightarrow v - \tilde{v} \in U$, so ist $\sim$ eine Äquivalenzrelation auf V (d.h. $\sim$ ist reflexiv, symmetrisch und transitiv).

Beweis:

(a) „$\Rightarrow$“ Seien $v, \tilde{v}$ mit $v + U = \tilde{v} + U$. Wegen $v = v + 0 \in \tilde{v} + U$ gibt es ein $\tilde{u} \in U$, mit $v = \tilde{v} + \tilde{u}$. Dann folgt $v - \tilde{v} = \tilde{u} \in U$.

„$\Leftarrow$“ Sei $v - \tilde{v} = \tilde{u} \in U$. Dann folgt $v = \tilde{v} + \tilde{u} \in \tilde{v} + U$. Für jedes $u \in U$ ergibt sich $v + u = \tilde{v} + \tilde{u} + u \in U$, also $v + U \subseteq \tilde{v} + U$. Andererseits gilt auch $\tilde{v} = v - \tilde{u} \in v + U$. Für jedes $u \in U$ erhalten wir somit $\tilde{v} + a = v - \tilde{u} + u \in v + U$, also $\tilde{v} + U \subseteq v + U$. Insgesamt haben wir $v + U = \tilde{v} + U$ gezeigt.

(b) *reflexiv:* $v + U = v + U$

symmetrisch: Aus $v + U = \tilde{v} + U$ folgt $\tilde{v} + U = v + U$

transitiv: Aus $v + U = v' + U$ und $v' + U = v'' + U$ folgt $v + U = v'' + U$. qed.

16.4 Definition:

Sei $V/U = \{v + U \mid v \in V\}$ die Menge aller Nebenklassen von U in V (sprich „V modulo U“).
Wir definieren eine Addition $+ : V/U \times V/U \to V/U$ und eine skalare Multiplikation

$$(v + U, \tilde{v} + U) \mapsto v + \tilde{v} + U$$

$$\cdot : K \times V/U \to V/U$$
$$(a, v + U) \mapsto av + U$$

Dann heißt $(V/U, +, \cdot)$ der Restklassenvektorraum (oder Quotientenraum oder Faktorraum) von V modulo U.

16.5 Satz:

(a) Die Abbildungen $+ : V/U \times V/U \to V/U$ und $\cdot : K \times V/U \to V/U$ sind wohldefiniert.

(b) $(V/U, +, \cdot)$ ist ein K-Vektorraum.

Beweis:

(a) Seien $v, \tilde{v} \in V$ und $w, \tilde{w} \in W$ mit $v + U = w + U$ und $\tilde{v} + U = \tilde{w} + U$.
Dann gilt $v - w = u \in U$ und $\tilde{v} - \tilde{w} = \tilde{u} \in U$.
Somit folgt $(v + \tilde{v}) - (w + \tilde{w}) = (v - w) + (\tilde{v} - \tilde{w}) = u + \tilde{u} \in U$.
Dies zeigt $v + \tilde{v} + U = w + \tilde{w} + U$.
Ferner gilt: $av - aw = a(v - w) = au \in U$ und somit
$a(v + U) = av + U = aw + U = a(w + U)$.

(b) Nachrechnen. qed.

16.6 Beispiel:

Sei $I \subseteq \mathbb{R}$ ein Intervall und $\mathscr{L}(I) = \{f : I \to \mathbb{R} \mid f \text{ ist differenzierbar}\}$ (z.B. bezüglich des Riemann- oder des Lebesque-Integrals). Dann ist $\mathscr{L}(I)$ ein $\mathbb{R}$-Vektorraum.
Die Menge $\mathscr{N}(I) = \{f \in \mathscr{L}(I) \mid \int_I |f(x)|\,dx = 0\}$ ist ein $\mathbb{R}$-Untervektorraum von $\mathscr{L}(I)$, denn
aus $\int_I |f(x)|\,dx = 0$ und $\int_I |g(x)|\,dx = 0$ folgt
$\int_I |f(x) + g(x)|\,dx \leq \int_I (|f(x)| + |g(x)|)dx = \int_I |f(x)|\,dx + \int_I |g(x)|\,dx = 0,$
also $\int_I |f(x) + g(x)|\,dx = 0$.
Der Restklassenvektorraum $L(I) = \mathscr{L}(I) \setminus \mathscr{N}(I)$ besteht aus den Klassen von „fast überall gleichen“ Funktionen und spielt in der Analysis eine große Rolle.

16.7 Satz:

Ist V endlich-dimensional, so gilt $dim_K(V/U) = dim_K(V) - dim_K(U)$.

Beweis: Sei $\{u_1, \ldots, u_k\}$ eine Basis von U. Ergänze sie zu einer Basis $\{v_1, \ldots, v_l\}$ von V. Es genügt zu zeigen, dass $\{v_1 + U, \ldots, v_l + U\}$ eine Basis von V/U ist.

Erzeugendensystem: Sei $v + U \in V/U$. Schreibe $v = a_1u_1 + \ldots + a_ku_k + b_1v_1 + \ldots + b_lv_l$ mit $a_i, b_j \in K$. Dann gilt $u_i + U = 0 + U$ und folglich
$v + U = a_1(u_1 + U) + \ldots + a_k(u_k + U) + b_1(v_1 + U) + \ldots + b_l(v_l + U)$.

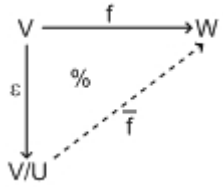
Lineare Unabhängigkeit: Seien $a_1, \ldots, a_l \in K$ mit $a_1(v_1 + U) + \ldots + a_l(v_l + U) = 0$. Dann folgt $(a_1v_1 + \ldots + a_lv_l) + U = 0$, also $a_1v_1 + \ldots + a_lv_l \in U$.
Schreibe $a_1v_1 + \ldots + a_lv_l = b_1u_1 + \ldots + b_ku_k$ mit $b_1, \ldots, b_k \in K$.
Aus $a_1v_1 + \ldots + a_lv_l - b_1u_1 - \ldots - b_ku_k = 0$ folgt $a_1 = \ldots = a_l = 0$ und $b_1 = \ldots = b_k = 0$. qed.

16.8 Satz: (Der kanonische Epimorphismus)

(a) Die Abbildung $\varepsilon : V \to V/U$, $v \mapsto v + U$ ist K-linear und surjektiv. Sie heißt der kanonische Epimorphismus von V nach V/U.

(b) (Universelle Eigenschaft von V/U)

Ist W ein weiterer K-Vektorraum und $f : V \to W$ eine K-lineare Abbildung mit $U \subseteq Kern(f)$ (d.h. mit $f(U) = 0$), so gibt es eine eindeutig bestimmte K-lineare Abbildung $\overline{f} : V/U \to W$ mit $f = \overline{f} \circ \varepsilon$.
Skizze:



Beweis:

(a) *K-Linearität:* $\varepsilon(v + \tilde{v}) = v + \tilde{v} + U = (v + U) + (\tilde{v} + U) = \varepsilon(v) + \varepsilon(\tilde{v})$
$\varepsilon(av) = av + U = a(v + U) = a \cdot \varepsilon(v)$

Surjektivität: Klar.

(b) Vgl. Übungen. qed.

Kapitel V: Und zum Schluss der Patherschuss

17 Das Spiel mit den Pfeilen (Exakte Sequenzen)

Sei K ein Körper und seien U, V, W K-Vektorräume sowie $g : U \to V$ und $f : V \to W$ lineare Abbildungen.

17.1 Definition:

(a) Die Sequenz $U \xrightarrow{g} V \xrightarrow{f} W$ heißt eine exakte Sequenz, wenn gilt: $Bild(g) = Kern(f)$.

(b) Ein (längere) Sequenz $\ldots \to V_{i-1} \xrightarrow{f_{i-1}} V_i \xrightarrow{f_i} V_{i+1} \xrightarrow{f_{i+1}} V_{i+2} \to \ldots$ von Vektorräumen V_j und linearen Abbildungen $f_j : V_j \to V_{j+1}$ heißt lange exakte Sequenz, wenn sie an jeder Stelle exakt ist, d.h. für alle j gilt $Bild(f_j) = Kern(f_{j+1})$.

17.2 Beispiele:

(a) Sei $U \subseteq V$ ein K-Untervektorraum und $i : U \to V$ die Inklusionsabbildung. Dann ist die Sequenz $0 \to U \xrightarrow{i} V$ exakt.

(b) Eine Sequenz $0 \to V \xrightarrow{f} W$ ist exakt, wenn f injektiv ist.

(c) Eine Sequenz $V \xrightarrow{f} W \to 0$ ist exakt, wenn f surjektiv ist.

(d) Eine Sequenz $0 \to V \xrightarrow{f} W \to 0$ ist exakt, wenn f bijektiv ist.

(e) Sei $U \subseteq V$ ein K-Untervektorraum und $\begin{array}{rcll} \varepsilon : V & \to & V/U & \\ v & \mapsto & v + U =: \overline{v} & \end{array}$ der kanonische Epimorphismus. Dann ist die Sequenz $V \xrightarrow{\varepsilon} V/U \to 0$ exakt.

17.3 Satz:

Sei $f : V \to W$ eine K-lineare Abbildung. Dann hat man eine exakte Vierersequenz $0 \to Kern(f) \xrightarrow{i} V \xrightarrow{f} W \xrightarrow{\varepsilon} W/Bild(f) \to 0$, wobei i die kanonische Inklusion und ε der kanonische Epimorphismus ist.

Beweis:

- *Exaktheit* bei $Kern(f)$: i ist injektiv.
- *Exaktheit* bei V: $Bild(i) = Kern(f)$
- *Exaktheit* bei W: $Bild(f) = Kern(\varepsilon)$
- *Exaktheit* bei $W/Bild(f)$: ε ist surjektiv. qed.

In der Situation des Satzes heißt $W/Bild(f)$ auch der Kokern von f und wird mit $Kokern(f)$ bezeichnet.

17.4 Satz:

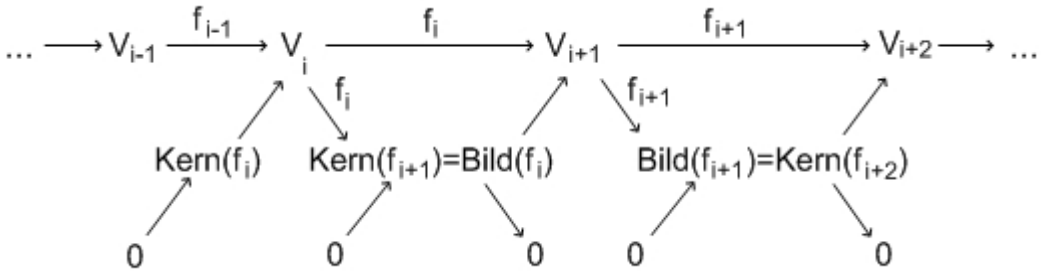
Sei $U \subseteq V$ ein K-Untervektorraum. Dann hat man eine exakte Dreiersequenz oder kurze exakte Sequenz $0 \to U \xrightarrow{i} V \xrightarrow{\varepsilon} V/U \to 0$, wobei i die kanonische Inklusion und ε der kanonische Epimorphismus ist.

Beweis:

- *Exaktheit* bei U: i ist injektiv.
- *Exaktheit* bei V: $Bild(i) = U = Kern(\varepsilon)$
- *Exaktheit* bei V/U: ε ist surjektiv. qed.

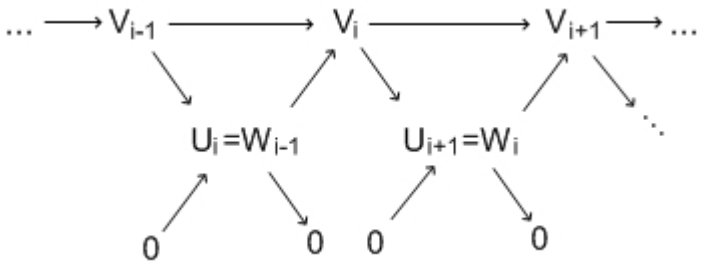
17.5 Bemerkung:

(a) Eine lange exakte Sequenz



kann man in kurze exakte Sequenzen $0 \to Kern(f_i) \to V_i \xrightarrow{f_i} Bild(f_i) \to 0$ aufbrechen.

(b) Kurze exakte Sequenzen $0 \to U_i \to V_i \to W_i \to 0$ mit $U_{i+1} = W_i$ kann man wieder zu einer langen exakten Sequenz zusammenfügen:



17.6 Satz: (Eulersche Gleichung)

Sei $0 \to V_1 \xrightarrow{f_1} V_2 \xrightarrow{f_2} V_3 \to \ldots \xrightarrow{f_{n-1}} V_n \to 0$ eine lange exakte Sequenz endlich dimensionaler K-Vektorräume und linearer Abbildungen.
Dann gilt $dim_K(V_1) - dim_K(V_2) + - \ldots + (-1)^{n-1} dim_K(V_n) = 0$

Beweis: Wir schließen mit vollständiger Induktion nach n.

$n = 1$: $0 \to V_1 \to 0$ bedeutet $V_1 = 0$

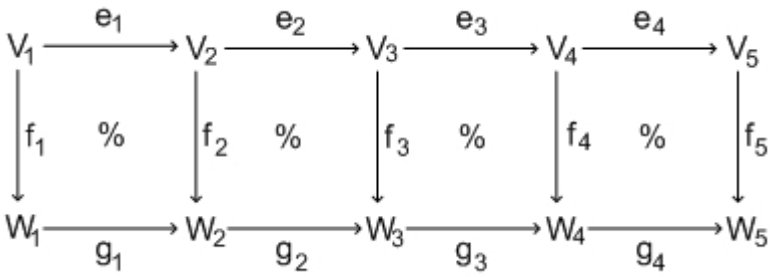
$n = 2$: $0 \to V_1 \xrightarrow{f_1} V_2 \to 0$ bedeutet, dass f_1 ein Isomorphismus ist, also $dim_K(V_1) = dim_K(V_2)$

$n = 3$: $0 \to V_1 \xrightarrow{f_1} V_2 \xrightarrow{f_2} V_3 \to 0$ exakt bedeutet:
$V_1 \cong Bild(f_1) = Kern(f_2)$ und $V_3 \cong V_2/Kern(f_2)$ nach dem Homomorphiesatz. Also folgt:
$dim_K(V_3) = dim_K(V_2) - dim_K(Kern(f_2)) = dim_K(V_2) - dim_K(V_1)$.
$\Rightarrow dim_K(V_1) - dim_K(V_2) + dim_K(V_3) = 0$.

$n > 3$: Wir spalten die Sequenz auf in
$0 \to V_1 \to V_2 \to \ldots \to V_{n-2} \to \underbrace{Bild(f_{n-2})}_{Kern(f_{n-1})} \to 0$ und $0 \to Kern(f_{n-1}) \to V_{n-1} \xrightarrow{f_{n-1}} V_n \to 0$
Nach Induktionsvoraussetzung gilt:
$dim_K(V_1) - dim_K(V_2) + - \ldots + (-1)^{n-3} dim_K(V_{n-2}) + (-1)^{n-2} dim_K(Bild(f_{n-2})) = 0$ und
$dim_K(Bild(f_{n-2})) = dim_K(Kern(f_{n-1})) = dim_K(V_{n-1}) - dim_K(V_n)$. Es folgt:
$dim_K(V_1) - dim_K(V_2) + - \ldots + (-1)^{n-3} dim_K(V_{n-2}) + (-1)^{n-2} dim_K(V_{n-1}) + (-1)^{n-1} dim_K(V_n) = 0$
qed.

17.7 Satz: (Fünfer Lemma)

Seien V_i, W_j Vektorräume. Das Diagramm



habe exakte Sequenzen und sei kommutativ. Dann gilt:

(a) Sind f_2, f_4 injektiv und f_1 surjektiv, so ist f_3 injektiv.

(b) Sind f_2, f_4 surjektiv und f_5 injektiv, so ist f_3 surjektiv.

(c) Sind f_1, f_2, f_4, f_5 bijektiv, so ist auch f_3 bijektiv.

Beweis:

(a) Beweis mit Diagrammjagd:

Sei $v_3 \in V_3$ mit $f_3(v_3) = 0$. Aus $g_3(f_3(v_3)) = 0$ folgt $f_4(e_3(v_3)) = 0$.
Also ist $e_3(v_3) \in Kern(f_4) = \{0\}$, d.h. $e_3(v_3) = 0$. Da die erste Zeile bei V_3 exakt ist, folgt, dass es ein $v_2 \in V_2$ gibt mit $v_3 = e_2(v_2)$. Aus $f_3(e_2(v_2)) = 0$ folgt $g_2(f_2(v_2)) = 0$.
Für das Element $w_2 = f_2(v_2) \in Kern(g_2)$ folgt, dass es ein $w_1 \in W_1$ gibt, mit $g_1(w_1) = w_2$.
Da f_1 surjektiv ist, gibt es ein $v_1 \in V_1$ mit $f_1(v_1) = w_1$. Also folgt
$w_2 = g_1(f_1(v_1)) = f_2(e_1(v_1))$. Weil sowohl $f_2(e_1(v_1)) = w_2$ und $f_2(v_2) = w_2$ gilt und weil f_2 injektiv ist, folgt $v_2 = e_1(v_1)$.
Nun gilt $Bild(e_1) \subseteq Kern(e_2)$, also $w_2 = e_2(v_2) = e_2(e_1(v_1)) = 0$.

(b) Analog mit Diagrammjagd, vgl. Übungen.

(c) Folgt aus (a) und (b). qed.

18 Alles umdrehen, bitte! (Duale Vektorräume)

Ziel: Betrachte Vektorräume, deren Elemente lineare Funktionen sind!
Im Folgenden sei K ein Körper und V ein K-Vektorraum.

18.1 Definition:

(a) Eine K-lineare Abbildung $l : V \to K$ heißt eine Linearform auf V.

(b) Die Menge aller Linearformen auf V ist ein K-Vektorraum $V^* = Hom_K(V, K)$ und heißt der duale Vektorraum von V.

18.2 Bemerkung:

Ist $l : V \to K$ eine Linearform mit $l \neq 0$, so gilt $Bild(l) = K$, d.h. l ist surjektiv und $dim_K(Kern(f)) = dim_K(V) - 1$.

18.3 Satz:

Sei $B = \{v_1, \ldots, v_n\}$ eine Basis von V. Für $i = 1, \ldots, n$ betrachte die K-lineare Abbildung $v_i^* : V \to K$, $v_j \mapsto \delta_{ij}$ (Für $v = a_1v_1 + \ldots + a_nv_n$ gilt somit $v_i^*(v) = a_i$). Dann ist $\{v_1^*, \ldots, v_n^*\}$ eine Basis vom dualen Vektorraum und sie heißt die duale Basis zu B.

Beweis: *Erzeugendensystem:* Sei $l : V \to K$ eine Linearform. Für $i = 1, \ldots, n$ setze $a_i = l(v_i) \in K$. Die Linearform $a_1v_1^* + \ldots + a_nv_n^*$ erfüllt $(a_1v_1^* + \ldots + a_nv_n^*)(v_i) = a_1v_1^*(v_i) + \ldots + a_nv_n^*(v_i) = a_i = l(v_i)$ für $i = 1, \ldots, n$. Da l und $a_1v_1^* + \ldots + a_nv_n^*$ auf einer Basis dieselben Werte annehmen, folgt $l = a_1v_1^* + \ldots + a_nv_n^*$.

Lineare Unabhängigkeit: Sei $a_1, \ldots, a_n \in K$ mit $a_1v_1^* + \ldots + a_nv_n^* = 0$. Für $i = 1, \ldots, n$ folgt $(a_1v_1^* + \ldots + a_nv_n^*)(v_i) = a_i$. qed.

18.4 Korollar:

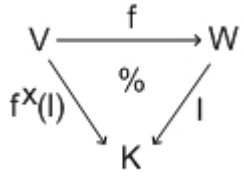
Zu jeder Basis $B = \{v_1, \ldots, v_n\}$ von V gibt es einen Isomorphismus $\varphi_B : V \to V^*$, $v_i \mapsto v_i^*$

(Beachte: Dieser Isomorphismus ist nicht kanonisch, d.h. er hängt von der Wahl der Basis B ab!)

18.5 Definition:

Seien V, W zwei K-Vektorräume und sei $f : V \to W$ eine K-lineare Abbildung.

(a) Für jede Linearform $l : W \to K$ ist $f^*(l) = l \circ f : V \to K$ eine Linearform auf V.
Skizze:



(b) Die K-lineare Abbildung $f^* : W^* \to V^*$, $l \mapsto l \circ f$ heißt die zu f duale Abbildung.

18.6 Satz:

Sei $f : V \to W$ eine K-lineare Abbildung, sei $B = \{v_1, \ldots, v_n\}$ eine Basis von V und $C = \{w_1, \ldots, w_m\}$ eine Basis von W. Dann gilt: $M^{C^*}_{B^*}(f^*) = (M^B_C(f))^{tr}$.

Beweis: Sei $M^B_C(f) = (a_{ij}) \in Mat_{m,n}(K)$, d.h. für $i = 1, \ldots, n$ gilt $f(v_j) = a_{1j}w_1 + \ldots + a_{mj}w_m$. Somit folgt $a_{ij} = w_i^*(f(v_j)) = f^*(w_i^*)(v_j)$.
Sei $M^{C^*}_{B^*}(f^*) = (b_{ij}) \in Mat_{n,m}(K)$. Dann gilt $f^*(w_i^*) = b_{1i}v_1^* + \ldots + b_{ni}v_n^*$ für $i = 1, \ldots, m$. Also ergibt sich $b_{ji} = (b_{1i}v_1^* + \ldots + b_{ni}v_n^*)(v_j) = f^*(w_i^*)(v_j) = (w_i^* \circ f)(v_j) = a_{ij}$.
Dies bedeutet $(b_{ij}) = (b_{ji})^{tr} = (a_{ij})^{tr}$. qed.

18.7 Korollar:

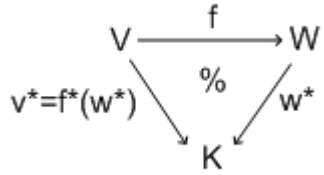
Es gilt $rang(f^*) = rang(f)$.

Beweis: Es gilt $rang(f^*) = dim_K(Bild(f^*)) = Spaltenrang(M^{C^*}_{B^*}(f^*))$
$= Spaltenrang(M^B_C(f)^{tr}) = Zeilenrang(M^B_C(f)) = Spaltenrang(M^B_C(f)) = rang(f)$. qed.

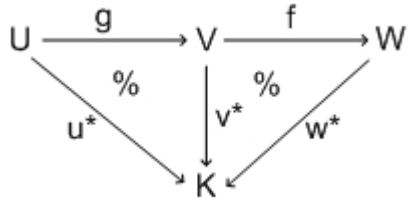
18.8 Satz:

Sei $U \xrightarrow{g} V \xrightarrow{f} W$ eine exakte Sequenz von K-Vektorräumen, d.h. $Bild(g) = Kern(f)$. Dann ist auch die duale Sequenz $W^* \xrightarrow{f^*} V^* \xrightarrow{g^*} U^*$ eine exakte Sequenz.

Beweis: „$Bild(f^*) \subseteq Kern(g^*)$“ Sei $v^* \in V^*$ mit $v^* = f^*(w^*)$, d.h. es gelte:



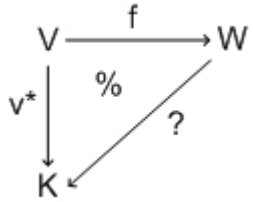
Nun bilden wir $u^* = g^*(v^*)$ und erhalten:



Für alle $u \in U$ folgt $u^*(u) = w^* \circ f \circ g)(u) = w^*(\underbrace{fg(u)}) = w^*(0) = 0$.

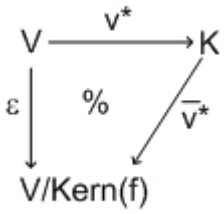
Wegen $Bild(g) \subseteq Kern(f)$ ist $fg = 0$

„$Kern(g^*) \subseteq Bild(f^*)$“ Sei $v^* \in V^*$ mit $g^*(v^*) = 0$. Skizze:

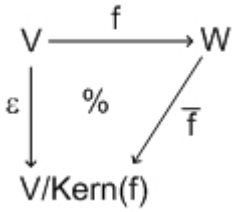


Die Vorraussetzung bedeutet $v^* \circ g = 0$ und $Kern(f) = Bild(g) \subseteq Kern(v^*)$.

Nach der universellen Eigenschaft des Restklassen Vektorraums erhalten wir:



Ferner gilt:



wobei $\overline{f}$ injektiv ist.
Sei $\tilde{W} = Bild(f) = Bild(\overline{f})$. Ergänze eine Basis $\{\tilde{w_1}, \ldots, \tilde{w_k}\}$ von $\tilde{W}$ zu einer Basis $\{\tilde{w_1}, \ldots, \tilde{w_k}, w_1, \ldots, w_l\}$ von W. Die Abbildung $\overline{f} : V/Kern(f) \to \tilde{W}$ ist ein Isomorphismus.
Definiere nun $w^* : W \to W$.

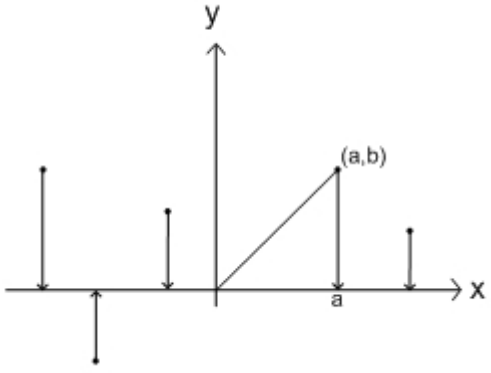
$$\begin{aligned} \tilde{w_j} &\mapsto \overline{v^*}(\overline{f^{-1}}(\tilde{w_j})) \\ w_j &\mapsto 0 \end{aligned}$$

Zu zeigen: $f^*(w^*) = v^*$, also $w^* \circ f = v^*$. Sei $v \in V$.
Schreibe $f(v) = a_1\tilde{w_1} + \ldots + a_k\tilde{w_k} + b_1w_1 + \ldots + b_lw_l$ mit $a_i, b_j \in K$.
Dann gilt $w^*(f(v)) = a_1w^*(\tilde{w_1}) + \ldots + a_kw^*(\tilde{w_k}) = a_1\overline{v^*}\overline{f^{-1}}(\tilde{w_1}) + \ldots + a_k\overline{v^*}\overline{f^{-1}}(\tilde{w_k}) \overset{!}{=} \overline{v^*}(\varepsilon(v))$, denn $\varepsilon(v) = a_1\overline{f^{-1}}(\tilde{w_1}) + \ldots + a_k\overline{f^{-1}}(\tilde{w_k})$, denn $f(v) = \overline{f}(\varepsilon(v)) = a_1\tilde{w_1} + \ldots + a_k\tilde{w_k}$ und $b_j = 0$ für $j = 1, \ldots, l$, da $f(v) \in \tilde{w} \in Bild(f)$ gilt.
Insgesamt erhalten wir $f^*(w^*) = v^*$, also $v^* \in Bild(f^*)$. qed.

18.9 Beispiel:

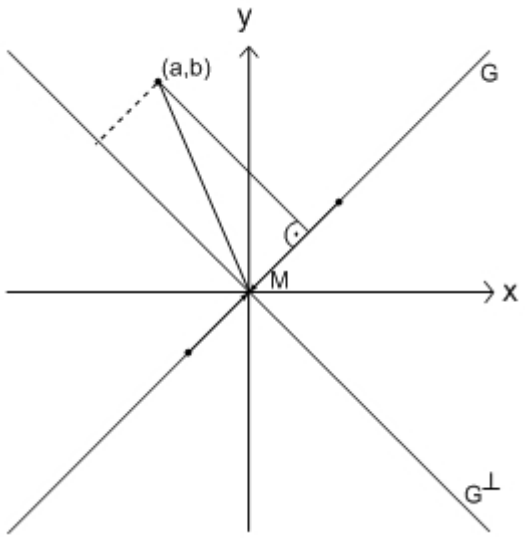
Sei $K = \mathbb{R}$ und $V = \mathbb{R}^2$ die Zeichenebene. Wir verwenden die Basis $E = \{e_1, e_2\}$ und die duale Basis $\{e_1^*, e_2^*\} \in V^*$.

(a) Für $(a, b) \in \mathbb{R}^2$ gilt $e_1^*((a, b)) = e_1^*(ae_1 + be_2) = a$. Also ist $e_1^* : \mathbb{R}^2 \to \mathbb{R}$ die Projektion auf die x-Achse.
Skizze:



(b) Ebenso zeigt $e_2^*((a, b)) = b$, dass $e_2^* : \mathbb{R}^2 \to \mathbb{R}$ die Projektion auf die y-Achse ist.

(c) Sein nun $l = c_1 e_1^* + c_2 e_2^* \in V^*$ gegeben, wobei $c_1^2 + c_2^2 = 1$ gelte. Für $(a, b) \in \mathbb{R}^2$ gilt dann $l((a, b)) = (c_1 e_1^* + c_2 e_2^*)(ae_1 + be_2) = c_1 e_1^*(ae_1 + be_2) + c_2 e_2^*(ae_1 + be_2) = c_1 a + c_2 b$.
Insbesondere folgt $l((a, b)) = 0 \Leftrightarrow (a, b) \in G = \{(x, y) \in \mathbb{R}^2 \mid c_1 x + c_2 y = 0\}$.
Skizze:



Ist $(a, b) \notin G$, so schreibe
$(a, b) = \lambda(c_1, c_2) + \mu(c_2, -c_1)$
mit $\lambda, \mu \in \mathbb{R}$.

Es folgt:
$l((a, b)) = \lambda l((c_1, c_2)) + \mu l((c_2, -c_1))$
$= \lambda(c_1^2 + c_2^2) = \lambda$.

Also ist l die Projektion auf $G^\perp$ längs G.

Hallo liebe Mitstudenten!

Fehler beim Abtippen der Vorlesungsmitschrift lassen sich natürlich nicht grundsätzlich vermeiden. Solltet ihr Fehler finden so teilt mir diese doch bitte mit (sowohl Rechtschreibfehler als auch inhaltliche Fehler, wie z.B. falsche Indizes o.ä.). Am besten immer mit Seitenzahl und Nummer des entsprechenden Satzes/Korollars/... unter der Emailadresse:

patrick.vorderstemann@uni-dortmund.de

Mit freundlichen Grüßen,
Patrick