§1
Einführung

Die Algebra ist ein Teilgebiet der Mathematik. Sie beschäftigt sich mit speziellen Strukturen wie Gruppen, Ringen oder Körpern und deren Verknüpfungen.

Ein fundamentales Problem ist das Lösen von algebraischen Gleichungen z.B.

$$\text{(*)} \qquad aX^2 + bX + C = 0.$$

Hierbei ist X eine Unbestimmte oder Variable und a, b, c „Zahlen".

Die Lösungsmenge ist:

$$L = \{\alpha, \text{„Zahl"} \mid a\alpha^2 + b\alpha + c = 0\}$$

Frage 1) Wie kann man L bestimmen?

Frage 2) Was genau versteht man unter „Zahlen"?

Frage 3) Was verstehen wir unter einer Menge?

Idee: Quadratische Ergänzung:

$$aX^2+bX+c = a\left(X^2+\frac{b}{a}X+\frac{c}{a}\right).$$

Hier muss man ausklammern können und dividieren.

$$a\left(X^2+\frac{b}{a}X+\frac{c}{a}\right) = a\left(X^2+2\frac{b}{2a}X+\left(\frac{b}{2a}\right)^2-\left(\frac{b}{2a}\right)^2+\frac{c}{a}\right)$$

$$= a\left(\left(X+\frac{b}{2a}\right)^2-\frac{b^2-4ac}{4a^2}\right)$$

Wir sehen $aX^2+bX+c=0$, falls

$$\left(X+\frac{b}{2a}\right)^2 = \frac{b^2-4ac}{4a^2}$$

Man nennt $\Delta := b^2-4ac$ die Diskriminante der Gleichung aX^2+bX+c.

Zu Frage 1)

⊗ Wenn wir L bestimmen wollen, müssen wir annehmen, dass $2a \neq 0$. Es gibt tatsächlich „Zahlen", wo $2a=0$.

Dann gilt:

⊛ hat Lösung genau dann, wenn Δ ein Quadrat ist, d.h., wenn eine „Zahl" s existiert mit $s^2 = \Delta$.

Das sieht man wie folgt:

(i) Sei α eine Lösung von ⊛. Dann gilt

$$a\alpha^2 + b\alpha + c = 0.$$

Also folgt

$$\left(\alpha + \frac{b}{2a}\right)^2 = \frac{\Delta}{4a^2} = \frac{\Delta}{(2a)^2}.$$

Mit anderen Worten

$$\Delta = \left(2a\left(\alpha + \frac{b}{2a}\right)\right)^2, \text{ d.h.}$$

mit $s = 2a\left(\alpha + \frac{b}{2a}\right)$ gilt $s^2 = \Delta$.

(ii) Sei umgekehrt Δ ein Quadrat, d.h. es gibt „Zahl" s mit $s^2 = \Delta$, so setzen wir

$x = \frac{s-b}{2a}$ und erhalten:

$$ax^2+bx+c = a\left(\frac{s-b}{2a}\right)^2 + b\left(\frac{s-b}{2a}\right) + c$$
$$= \frac{1}{4a}\left(s^2 + (4ac-b^2)\right) = 0$$

Da nun s und $-s$ die einzigen „Zahlen" sind mit $s^2 = \Delta$ und $(-s)^2 = \Delta$ folgt:

$$L = \left\{ \frac{s-b}{2a} \,;\, \frac{-s-b}{2a} \right\}.$$

Zu Frage 2)

Wir kennen bereits „Zahlen". z.B.:

$\mathbb{N} = \{0, 1, 2, \dots\}$ Menge der natürlichen Zahlen. ($\mathbb{N}_{>0} = \{1, 2, 3, \dots\}$)

$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ Menge der ganzen Zahlen.

$\mathbb{Q} = \left\{ \frac{m}{n} \mid m, n \in \mathbb{Z}, \text{und } n \neq 0 \right\}$ Menge der rationalen Zahlen.

$$\mathbb{R} = \left\{ \sum_{i=-\infty}^{n} z_i \cdot 10^i \mid z_i \in \{0,\dots,9\} \text{ und } n \in \mathbb{Z} \right\}$$

Menge der reellen Zahlen. Werden in Analysis genauer behandelt.

Wir werden später genau erklären, was genau wir unter „Zahlen" verstehen.

Wir verstehen nun wie quadratische Gleichungen

$$aX^2 + bX + c = 0$$

gelöst werden.

In der Algebra-Vorlesung geht es unter anderem darum, wie die Lösungsmenge von Gleichungen der Form

$$a_n X^n + a_{n-1} X^{n-1} + \dots + a_0 = 0 \quad , n \geq 3$$

bestimmt werden kann.

In der algebraischen Geometrie geht es dann darum die Lösungsmenge von

2b:

$$x^2 + y^3 - z = 0$$
$$-yz^2 + 3x^3 + 2xy = 0$$

zu verstehen.

Wir in der <u>linearen Algebra</u> beschäftigen uns zunächst mit <u>linearen Gleichungssystemen</u> (LGS) der Form:

$$\begin{aligned} a_{11}X_1 + a_{12}X_2 + \dots + a_{1n}X_n &= 0 \\ a_{21}X_1 + a_{22}X_2 + \dots + a_{2n}X_n &= 0 \\ &\vdots \\ a_{m1}X_1 + a_{m2}X_2 + \dots + a_{mn}X_n &= 0 \end{aligned} \qquad (*)$$

,

also $m \geq 0$ Gleichungen in $n \geq 0$ Unbestimmten.

Bsp $\quad \begin{aligned} aX + bY &= 0 \\ cX + dY &= 0 \end{aligned} \qquad (**) \qquad m = n = 2.$

1. Fall: $a = b = c = d = 0$, so sind alle $X = \alpha$, $Y = \beta$ „Zahlen"

Lösungen.

2 Fall: $a \neq 0$. Wenn man bei unseren „Zahlen" das $\frac{c}{a}$-fache der 1. Gleichung von der 2. Gleichung subtrahiert erhält man:

$$aX + bY = 0$$

$$\left(\frac{ad-bc}{a}\right)Y = 0$$

Da $a \neq 0$, folgt für $ad - bc \neq 0$ gerade $y = 0$ und somit $X = 0$.

Ist $ad - bc = 0$, so folgt $y = \beta$ beliebige „Zahl" und $X = -\frac{b\beta}{a}$.

Wir sehen also, wie man das LGS

$$aX + bY = 0$$
$$cX + dY = 0$$

lösen könnte. Dafür müsste man in unseren „Zahlen" zum Beispiel folgende

Rechenoperationen durchführen können:

- Dividieren
- subtrahieren, addieren
- multiplizieren
- ausklammern / ausmultiplizieren
- es muss $a(b+c) = ab + ac$ gelten

etc.

In $\mathbb{Q}$ oder $\mathbb{R}$ kann man diese Rechenoperationen durchführen. In $\mathbb{Z}$ nicht, da man nicht immer dividieren kann.

Um zu klären, was genau mit unter „Zahlen" verstanden werden, müssen wir zunächst klären, was $\mathbb{Z}$ und $\mathbb{R}$ genau sind. (Frage 3)).

§2
Mengen und Abbildungen

Wir benutzen Cantors intuitive Sichtweise, um über Mengen zu sprechen. Eine exakte Axiomatisierung der Mengentheorie ist z.B. durch die Zermelo-Fraenkel-Mengenlehre mit Auswahlaxiom gegeben.

Unter einer Menge X verstehen wir eine Zusammenfassung gewisser Dinge a, genannt Elemente der Menge X. Eine Menge X ist in eindeutiger Weise durch ihre Elemente festgelegt.

Ist a ein Element der Menge X, so schreibt man $a \in X$. Falls a kein Element von X ist, so schreibt man $a \notin X$.

Man bezeichnet eine Menge X dadurch, daß man ihre Elemente in geschweiften Klammern $\{ \dots \}$ schreibt.

Bsp 2.1 $X = \{0, \pi, 3\}$ hat 3 Elemente:

$0 \in X$, $\pi \in X$, $3 \in X$, $1 \notin X$.

Elemente die man nicht nennt kann man durch Punkte andeuten:

Bsp 2.2 $\mathbb{N} = \{0, 1, 2, \dots\}$

Ist E eine Eigenschaft, die jedes Element a einer Menge X hat, so bezeichnet

$$\{a \in X \mid a \text{ hat Eigenschaft } E\}$$

die Menge alle Elemente von X mit Eigenschaft E.

Bsp 2.3 $\mathbb{N} = \{a \in \mathbb{Z} \mid a \text{ nicht negativ}\}$

Dies führt zum natürlichen Begriff der Teilmenge.

Def 2.4 Seien X und Y zwei Mengen. Wir schreiben $X \subset Y$ und sagen, daß X eine Teilmenge von Y ist, falls für jedes $a \in X$ auch $a \in Y$ gilt.

Bsp 2.5

$$\{0,1,\pi\} \subset \mathbb{R}, \quad \{0,1\} \subset \mathbb{N} \subset \mathbb{Z}.$$

Die leere Menge $\emptyset = \{\}$ hat kein einziges Element. Für alle a gilt $a \notin \emptyset$. Für alle Mengen X gilt jedoch $\emptyset \subset X$.

Def 2.6 Seien X und Y zwei Mengen. Wir schreiben $X = Y$ und sagen, daß die Mengen X und Y gleich sind, falls

$$X \subset Y \quad \text{und} \quad Y \subset X.$$

Bemerkung 2.7 Bei Mengen kommt es in der Angabe der Elemente nicht auf die Reihenfolge oder Wiederholungen an. Beispielsweise sind

$$X = \{1,0,1\} \quad \text{und} \quad Y = \{1,0\}$$

gleich.

Man kann aus gegebenen Mengen neue Mengen konstruieren.

Def 2.8 Seien X und Y zwei Mengen.
Die Vereinigung von X und Y ist die Menge

$$X \cup Y = \{a \mid a \in X \text{ oder } a \in Y\}$$

Def 2.9 Seien X und Y zwei Mengen.
Der Durchschnitt von X und Y ist die Menge

$$X \cap Y = \{a \mid a \in X \text{ und } a \in Y\}$$

Bsp 2.10 $\mathbb{Z} \cup \mathbb{N} = \mathbb{Z}$ und $\mathbb{Z} \cap \mathbb{N} = \mathbb{N}$.

Man nennt zwei Mengen X und Y disjunkt, wenn $X \cap Y = \emptyset$.

Manchmal wird es nötig sein Vereinigungen und Durchschnitte von mehr als endlich vielen Mengen zu betrachten. Dazu verwendet man eine Menge I, die Indexmenge, und betrachtet die Mengen X_i, $i \in I$.

Dann ist

$$\bigcup_{i \in I} X_i = \{a \mid \text{es gibt ein } i \in I \text{ mit } a \in X_i\}$$

die Vereinigung der Mengen X_i und

$$\bigcap_{i \in I} X_i = \{ a \mid a \in X_i \text{ für alle } i \in I \}$$

der Durchschnitt der Mengen X_i.

Bsp 2.11 $I = \mathbb{N}$ und $X_i = [-i, i] \subset \mathbb{R}$ Intervalle.

Dann gilt

$$\bigcup_{i \in I} X_i = \mathbb{R} \quad \text{und} \quad \bigcap_{i \in I} X_i = \{0\}.$$

Def 2.12 Seien X und Y Mengen. Die Komplementärmenge von X und Y ist die Menge

$$X \setminus Y = \{ a \mid a \in X \text{ und } a \notin Y \}.$$

Def 2.13 Seien $X_1, \dots, X_n$ Mengen. Dann heißt

$$\prod_{i=1}^{n} X_i = X_1 \times X_2 \times \dots \times X_n = \{ (a_1, \dots, a_n) \mid a_i \in X_i \}$$

das kartesische Produkt der Mengen $X_1, \dots, X_n$.

Die Elemente $(a_1, \dots, a_n)$ heißen n-Tupel und es gilt $(a_1, \dots, a_n) = (a_1', \dots, a_n')$ genau dann, wenn $a_i = a_i'$ für $i = 1, \dots, n$.

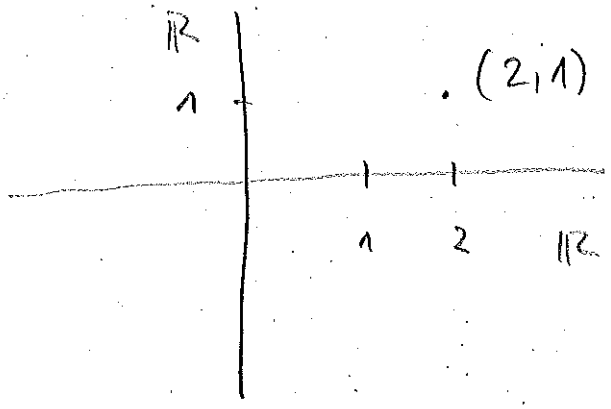
Bsp 2.14 X, Y zwei Mengen. Dann ist

$$X \times Y = \{(a,b) \mid a \in X, b \in Y\}.$$

Hierbei ist $(a,b) = (a',b') \iff a = a'$ und $b = b'$.

(genau dann)

Für $X = Y = \mathbb{R}$ erhält man



das Koordinatensystem mit reellen Koordinaten.

Als nächstes kommen wir zu dem Begriff der Abbildung zwischen Mengen zu sprechen.

Def 2.15 Eine Abbildung $f: X \to Y$ zwischen zwei Mengen X und Y ist eine Vorschrift, welche jedem $a \in X$ genau ein $b \in Y$ zuordnet. Man schreibt $b = f(a)$ und $a \mapsto f(a)$. Dabei heißt X der Definitionsbereich und Y der Wertebereich der Abbildung f.

Zwei Abbildungen $f: X \to Y$ und $g: X \to Y$ heißen gleich und man schreibt $f = g$, wenn $f(a) = g(a)$ für alle $a \in X$.

Bsp 2.16 $f: \mathbb{Z} \to \mathbb{R}$, $a \mapsto a^2$ oder

$$f: \mathbb{N} \to \mathbb{Z}, \; n \mapsto \begin{cases} \frac{n}{2}, & n \text{ gerade} \\ -\frac{n-1}{2}, & n \text{ ungerade} \end{cases}$$

Bei Abbildungen ist es wichtig auch Definitionsbereich und Wertebereich anzugeben.
So sind $f: \mathbb{Q} \to \mathbb{Q}$, $a \mapsto a^3$ und $f: \mathbb{R} \to \mathbb{R}$, $a \mapsto a^3$ verschieden, obwohl beide die gleiche Vorschrift $a \mapsto a^3$ besitzen.

Sei $f: X \to Y$ eine Abbildung und $A \subset X$ eine Teilmenge. Die Menge

$$f(A) = \{ b \in Y \mid \text{es gibt ein } a \in A \text{ mit } f(a) = b \}$$

heißt das Bild von A. Es ist $f(A) \subset Y$.

Ist $B \subset Y$ eine Teilmenge, so heißt die Menge

$$f^{-1}(B) = \{ a \in X \mid f(a) \in B \} \subset X$$

das Urbild von B.

Besonders wichtige Eigenschaften von Abbildungen haben eigene Namen.

Def 2.17 Eine Abbildung $f: X \to Y$ heißt

(i) injektiv, falls aus $a, a' \in X$ und $f(a) = f(a')$ stets $a = a'$ folgt.

(ii) surjektiv, falls es zu jedem $b \in Y$ mindestens ein $a \in X$ gibt mit $f(a) = b$.

(iii) bijektiv, falls f injektiv und surjektiv ist.

Bsp 2.18 Die Abbildung $f: \mathbb{N} \to \mathbb{N}$, $a \mapsto a+1$ ist injektiv, aber nicht surjektiv.

Die Abbildung $f: \mathbb{N} \to \mathbb{N}$, $a \mapsto \begin{cases} a, & a \text{ ungerade} \\ \frac{a}{2}, & a \text{ gerade} \end{cases}$ ist surjektiv, aber nicht injektiv.

Ist $f: X \to Y$ bijektiv, so gibt es zu jedem $b \in Y$ genau ein $a \in X$ mit $f(a) = b$. In diesem Fall existiert also eine Umkehrabbildung

$$f^{-1}: Y \to X, \quad b \mapsto a \quad \text{mit} \quad b = f(a).$$

Man schreibt dann $b \mapsto f^{-1}(b)$.

Bsp 2.19 Die Abbildung $f: \mathbb{R} \to \mathbb{R}$, $a \mapsto a+5$ ist bijektiv und die Umkehrabbildung ist $f^{-1}: \mathbb{R} \to \mathbb{R}$, $a \mapsto a-5$.

Eine Menge X heißt endlich, falls $X = \{a_1, \dots, a_n\}$, d.h. falls sie nur endlich viele Elemente besitzt.

Propo. 2.20 Sind X und Y endliche Mengen mit gleich vielen Elementen n, so sind für eine Abbildung $f: X \to Y$ folgende Aussagen äquivalent:

(i) f ist injektiv

(ii) f ist surjektiv

(iii) f ist bijektiv

Beweis $X = \{a_1, \dots, a_n\}$ mit paarweise verschiedenen a_i;

(i) $\Rightarrow$ (ii): Angenommen f ist nicht surjektiv. Dann besteht $f(X)$ aus $m < n$ Elementen. Also existieren $a_i, a_j \in X$ $i \neq j$, mit $f(a_i) = f(a_j)$. Also nicht injektiv.

(ii) $\Rightarrow$ (i): Angenommen f ist nicht injektiv. Dann existieren $a_i, a_j \in X$, $i \neq j$ mit $f(a_i) = f(a_j)$. Dann kann $f(X)$ höchstens $n-1$ Elemente besitzen. Also ist f nicht surjektiv.

(i) $\Leftrightarrow$ (iii) klar.

Die Aussage von Satz 1 wird falsch, wenn man Mengen mit unendlich vielen verschiedenen Elementen betrachtet.

Bsp 2.21 $X = \mathbb{N}$, $f: \mathbb{N} \to \mathbb{N}$, $a \mapsto a+1$ ist injektiv, aber nicht surjektiv und somit auch nicht bijektiv.

Sind X, Y, Z Mengen und $f: X \to Y$ sowie $g: Y \to Z$ Abbildungen, so heißt die Abbildung

$$g \circ f : X \to Z, \quad x \mapsto g(f(x)) = (g \circ f)(x)$$

die Komposition von f und g.

Die natürlichen Zahlen $\mathbb{N}$ können durch Axiome beschrieben werden (Peano-Axiome). John von Neumann gab eine Möglichkeit die natürlichen Zahlen durch Mengen darzustellen:

$0 := \emptyset$

$1 := \{\emptyset\}$

$2 := \{\emptyset, \{\emptyset\}\}$

$3 := \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$

$\vdots$

$n+1 := n \cup \{n\}$

Wir werden später sehen, wie man aus $\mathbb{N}$ die Menge der ganzen Zahlen $\mathbb{Z}$ und wie man aus diesen schließlich $\mathbb{Q}$ erhält.

Dies geschieht dann mittels Äquivalenzrelationen.

Aussagen über natürliche Zahlen lassen sich mit der Methode der vollständigen Induktion beweisen.

Propo. 2.22 Sei $n \in \mathbb{N}$ und $A(n)$ eine Aussage. Wir nehmen an, daß wir folgendes zeigen können:

(i) Die Aussage $A(0)$ gilt

(ii) Wenn $A(n)$ gilt, so gilt auch $A(n+1)$.

Dann gilt die Aussage $A(n)$ für alle $n \in \mathbb{N}$.

Beweis Sei S die Menge der natürlichen Zahlen für die die Aussage nicht gilt. Nehmen an $S \neq \emptyset$. Dann existiert ein kleinstes Element $n_0 \in S$. Dann ist $n_0 \neq 0$ wegen (i). Dann gilt die Aussage jedoch für $n_0 - 1$. Wegen (ii) gilt dann die Aussage auch für n_0.

Dies ist ein Widerspruch.

Bemerkung 2.23 Das Prinzip der vollständigen Induktion funktioniert auch, wenn man (i) und (ii) ersetzt durch:

(i)' Sei $k \in \mathbb{N}$ fest. Die Aussage $A(k)$ gilt

(ii)" Wenn $A(n)$ für $n \geq k$ gilt, so gilt auch $A(n+1)$.

Bsp 2.24 $$\sum_{i=0}^{n} i = 0+1+2+\dots+n = \frac{n(n+1)}{2}$$

Hier ist die Formel $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$ die Aussage $A(n)$.

(i) Wir müssen zeigen, daß $A(0)$ gilt. Man nennt (i) auch den Induktionsanfang.

Also zu zeigen ist:

$$\sum_{i=0}^{0} i = 0 = \frac{0(0+1)}{2} = 0$$

Dies ist also klar.

(ii) Wir müssen nun zeigen, daß aus $A(n)$ die Aussage $A(n+1)$ folgt. Dies nennt man auch Induktionsschritt. Wir nehmen also an, daß $A(n)$ gilt:

Also $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$

Die Aussage $A(n+1)$ lautet:

$$\sum_{i=0}^{n+1} i = \frac{(n+1)(n+2)}{2}.$$

Diese ist aus $A(n)$ zu folgern:

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

$$\overset{\uparrow}{=} \frac{n(n+1)}{2} + (n+1) = \frac{n(n+1)+2(n+1)}{2}$$

$A(n)$ gilt

$$= \frac{(n+1)(n+2)}{2}$$

Also haben wir aus $A(n)$ die Aussage $A(n+1)$ gefolgert.

Bsp 2.25 Sei $f: \mathbb{N}_{>0} \to \mathbb{N}_{>0}$ eine Abbildung, so daß $f(n+m) = f(n) \cdot f(m)$. Setze $a = f(1)$, so gilt $f(n) = a^n$.

Hier ist die Aussage $A(n)$ die Gleichung $f(n) = a^n$.

Induktionsanfang: $A(1)$:

$f(1) = a^1 = a$. Dies ist trivialerweise erfüllt.

Induktionsschritt: Wir nehmen an, daß $f(n) = a^n$ und müssen zeigen, daß $f(n+1) = a^{n+1}$.

$$f(n+1) = f(n) \cdot f(1) = a^n \cdot a = a^{n+1}.$$

$A(n)$ gilt

§ 3
Gruppen und Ringe

Wir kommen nun zu den Begriffen Gruppe und Ring und nähern uns so der Vorstellung, was wir später unter „Zahlenmengen" verstehen werden.

Unter einer Verknüpfung auf einer Menge G verstehen wir eine Abbildung $f: G \times G \to G$. Sie ordnet jedem Paar $(a,b) \in G \times G$ ein Element $f(a,b) \in G$ zu.

Def 3.1 Eine Menge G mit einer Verknüpfung $*: G \times G \to G$, $(a,b) \mapsto *(a,b) =: a*b$ heißt Gruppe, wenn folgende Eigenschaften erfüllt sind:

(G1) Assoziativität: Für alle $a,b,c \in G$ gilt
$$(a*b)*c = a*(b*c)$$

(G2) Existenz eines neutralen Elements: Es existiert ein Element $e \in G$, so daß $e*a = a*e = a$ für alle $a \in G$. Das Element e heißt neutrales Element

(G3) Inverses Element: Zu jedem $a \in G$ gibt es ein $b \in G$ mit $a * b = b * a = e$. Das Element b heißt Inverses zu a.

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

Propo 3.2 Sei G eine Gruppe und e, e' zwei neutrale Elemente, so gilt $e = e'$

Beweis Nach (G2) gilt $a = a * e$ und $e' * b = b$ für alle $a, b \in G$. Für $a = e'$ und $b = e$ folgt

$$e' = e' * e = e.$$

Propo 3.3 Sei G eine Gruppe und $a \in G$. Seien b und b' zwei Inverse zu a, so gilt $b = b'$

Beweis Übungsblatt.

Bsp 3.4 • Die Menge $\mathbb{Z}$ mit „+" als Verknüpfung ist eine Gruppe. Neutrales Element ist 0 und inverses zu a ist $-a$.

• Die Menge $\mathbb{Q} \setminus \{0\}$ mit „·" als Verknüpfung ist eine Gruppe. Neutrales Element ist 1. Zu einem Element $\frac{n}{m} \in \mathbb{Q} \setminus \{0\}$ ist $\frac{m}{n}$ das inverse.

Beide Gruppen sind kommutativ. Es gibt aber auch Gruppen, welche nicht kommutativ sind.

Bsp 3.5 Sei X eine Menge und

$$G = \{ f : X \to X \mid f \text{ bijektiv} \}.$$

Dann ist G mit der Verknüpfung „Komposition" eine Gruppe.
Das neutrale Element ist die Identitätsabbildung $id_X : X \to X$, $a \mapsto a$ und das Inverse zu f ist die Umkehrabbildung f^{-1}.

Diese Gruppe ist im Allgemeinen nicht kommutativ.
Sei etwa $X = \{1,2,3\}$ und f und g definiert durch die Wertetabelle

	1	2	3
$f(a)$	2	3	1
$g(a)$	1	3	2

Dann ist $f(g(1)) = 2$ und $g(f(1)) = 3$, d.h. $f \circ g \neq g \circ f$.

Notation:
Sei G eine Gruppe und $a \in G$. So bezeichnen wir das Inverse zu a mit a^{-1}.

Propo 3.6 Sei G eine Gruppe. Dann gilt:

(i) $e^{-1} = e$

(ii) $(a^{-1})^{-1} = a$

(iii) $(a * b)^{-1} = b^{-1} * a^{-1}$

Beweis

(i) Es gilt $e * a = a$ für alle $a \in G$.
Insbesondere für $a = e$ gilt $e * e = e$.
Also folgt $e^{-1} = e$.

(ii) $a * a^{-1} = e = a^{-1} * a$. Aus Proposition 3.3 folgt direkt $(a^{-1})^{-1} = a$.

(iii) $$(a*b)*(b^{-1}*a^{-1}) \overset{(G1)}{=} a*(b*(b^{-1}*a^{-1}))$$
$$= a*((b*b^{-1})*a^{-1})$$
$$\overset{(G1)}{=} a*(e*a^{-1})$$
$$\overset{(G2)}{=} a*a^{-1} = e$$

Genau so zeigt man $(b^{-1}*a^{-1})*(a*b) = e$.

Wir kommen nun zu interessanten Beispielen von Gruppen.

Sei $X = \{1, 2, \dots, n\}$ und G die Gruppe

$$G = \{\sigma : X \to X \mid \sigma \text{ bijektiv}\}.$$

Diese Gruppe bezeichnet man als

Symmetrische Gruppe und schreibt $S_n = G$.

Wie wir bereits gesehen haben, ist S_3 nicht kommutativ.

Die Elemente $\sigma \in S_n$ nennt man auch Permutationen. Gilt für eine Permutation σ etwa $\sigma(i) = a_i$ für $i = 1, \dots, n$, so schreibt man

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}.$$

Bsp 3.7 $X = \{1,2,3\}$, $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \in S_3$.

Man sieht sofort, daß S_n aus genau $n!$ vielen Elementen besteht. (Übung)

Die Anzahl der Elemente einer Gruppe G nennt man Ordnung. Man schreibt $\mathrm{ord}(G)$.

Def 3.8 Sei $\sigma \in S_n$, so nennt man

$$\mathrm{sgn}(\sigma) = \prod_{1 \le i < j \le n} \frac{\sigma(j) - \sigma(i)}{j - i} \in \mathbb{Q}$$

das Signum von σ.

Propo 3.9 Sei $\sigma \in S_n$, so gilt $\operatorname{sgn}(\sigma) \in \{\pm 1\}$.

Beweis Eine Permutation $\sigma \in S_n$ bildet die zwei-elementigen Teilmengen von $\{1, \dots, n\}$ bijektiv auf sich selbst ab.

Daher gilt

$$\prod_{i<j} (j-i) = \pm \prod_{i<j} (\sigma(j) - \sigma(i))$$

und somit $\operatorname{sgn}(\sigma) \in \{\pm 1\}$.

Wir benötigen das Signum später für die Determinante.

Propo 3.10 Seien $\sigma, \tau \in S_n$, so gilt

$$\operatorname{sgn}(\sigma \circ \tau) = \operatorname{sgn}(\sigma) \operatorname{sgn}(\tau).$$

Beweis Übungsblatt.

Ist $\operatorname{sgn}(\sigma) = 1$, nennt man σ gerade, andernfalls ungerade.

Bsp 3.11 $n = 2$, $\operatorname{ord}(S_2) = 2$. Elemente sind

$$\sigma = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \quad \text{und} \quad \tau = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}.$$

Nun ist $\operatorname{sgn}(\sigma) = \prod_{1<2} \frac{\sigma(2)-\sigma(1)}{2-1} = \frac{2-1}{2-1} = 1$

gerade und $\operatorname{sgn}(\tau) = \prod_{1<2} \frac{\tau(2)-\tau(1)}{2-1} = \frac{1-2}{2-1} = -1$

ungerade.

Als nächstes wollen wir außer den Gruppen $(\mathbb{Z},+)$ oder S_n weitere Beispiele für Gruppen kennenlernen. Dafür sei $m \in \mathbb{Z}$ und $n \in \mathbb{N}_{>0}$. Wir teilen m durch n und erhalten ein $q \in \mathbb{Z}$ und einen Rest r, so daß

$$m = q \cdot n + r, \quad 0 \le r < n$$

gilt. Hier sind q und r eindeutig bestimmt.

Bsp 3.12 $m = 37$ und $n = 5$. Dann gilt

$$37 = 7 \cdot 5 + 2$$ und 2 ist der Rest.

Wir definieren nun folgende Menge

$$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}$$

und fassen zunächst $[a]$, $0 \le a \le n-1$ als formale Symbole auf. Wir setzen

$$a = 0 \cdot n + a, \text{ also Rest von } a =: [a].$$

Wir definieren auf der Menge $\mathbb{Z}/n\mathbb{Z}$ eine Verknüpfung „+" durch

$$[a] + [b] = \text{Rest von } a+b$$

Dadurch wird $(\mathbb{Z}/n\mathbb{Z}, +)$ zu einer Gruppe.

Propo 3.13 Für jedes $n \geq 1$ ist $(\mathbb{Z}/n\mathbb{Z}, +)$ eine kommutative Gruppe.

Beweis

(G2): $[0]$ ist neutrales Element. Klar, da $[a] + [0] = \text{Rest von } a = [a]$ und $[0] + [a] = \text{Rest von } a = [a]$.

(G3): Sei $[0] \neq [a] \in \mathbb{Z}/n\mathbb{Z}$. Dann ist $[n-a] \in \mathbb{Z}/n\mathbb{Z}$ das Inverse zu $[a]$.

$[a] + [n-a] = \text{Rest von } n = 0 = [0]$

$[n-a] + [a] = \text{Rest von } n = 0 = [0]$

Falls $[a] = [0]$, so ist $[0]$ das Inverse.

(G1): Dies ist ein wenig schwieriger.

Wir müssen zeigen, daß

$([a]+[b])+[c] = [a]+([b]+[c])$. Nun ist

$a+b = q'n + r'$, $0 \le r' \le n-1$. und

$r'+c = qn + r$, $0 \le r \le n-1$.

Dann gilt:

$r = r'+c-qn = a+b-q'n+c-qn$

$= a+b+c-(q+q')n$, d.h.

$a+b+c = (q+q')n + r$, $0 \le r \le n-1$.

Die rechte Seite ergibt sich durch:

$b+c = p'n+s'$, $0 \le s' \le n-1$ und

$a+s' = pn+s$, $0 \le s \le n-1$. Wie oben

folgt: $a+b+c = (p+p')n+s$. Aufgrund

der Eindeutigkeit bei der Division mit Rest,

folgt $p+p' = q+q'$ und $r=s$. Also gilt

$([a]+[b])+[c] = [a]+([b]+[c])$.

Kommutativität ist klar, da

$[a]+[b]$ = Rest von $a+b$ = Rest von $b+a$ =

$[b]+[a]$.

Das Element $[a] \in \mathbb{Z}/n\mathbb{Z}$ nennt man Kongruenzklasse mod n. Wir werden später sehen wieso.

Wir bemerken, daß $\operatorname{ord}(\mathbb{Z}/n\mathbb{Z}) = n$.

Nun kennen wir schon folgende Gruppen:

$(\mathbb{Z}, +)$, $(\mathbb{Q}\setminus\{0\}, \cdot)$, $(\mathbb{Q}, +)$, S_n und $\mathbb{Z}/n\mathbb{Z}$.

(mit dem Begriff „Gruppe" lassen sich nun „Zahlenmengen" abstrahieren.

Def 3.14 Ein assoziativer Ring, kurz Ring, ist Menge R, mit zwei Verknüpfungen

$$+ : R \times R \to R \quad \text{und} \quad \cdot : R \times R \to R,$$

so daß folgendes erfüllt ist:

(

(R1) $(R, +)$ ist kommutative Gruppe.

(R2) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ für alle $a, b, c \in R$

(R3) es gibt ein Element $1 \in R$ mit $1 \cdot a = a \cdot 1 = a$ für alle $a \in R$.

(R4) Für alle $a, b, c \in R$ gelt

$$a(b+c) = a \cdot b + a \cdot c$$

$$(b+c) \cdot a = b \cdot a + c \cdot a.$$

Man nennt (R4) das Distributivgesetz und 1 das neutrale Element bezüglich der Multiplikation „·"

Das neutrale Element bezüglich der Addition „+" schreiben wir als 0 und nennen es das Nullelement. Die 1 heißt Einselement.

Das Inverse zu $a \in R$ bezüglich der Addition „+" schreibt man $-a \in R$ und nennt es das Negative von a.

Wir machen nun einige Beobachtungen.

Propo 3.15 Sei R ein Ring. Dann gilt für alle $a \in R$

$$0 \cdot a = 0 = a \cdot 0$$

Beweis Es gilt

$$0 \cdot a = (0+0) \cdot a \overset{(R4)}{=} 0 \cdot a + 0 \cdot a.$$

Da $(R,+)$ kommutative Gruppe ist können wir auf beide Seiten

$-(0 \cdot a)$ addieren.

Das ergibt

$$0 = 0 \cdot a - 0 \cdot a = 0 \cdot a.$$

↯

Propo 3.16 Sei R ein Ring. Dann gilt für alle $a \in R$

$$(-1) \cdot a = -a = a \cdot (-1)$$

Beweis Übungsaufgabe.

Propo 3.17 Sei R ein Ring. Dann ist R der Nullring genau dann, wenn $0 = 1$.

Beweis Falls R Nullring, so gilt $0 = 1$.
Nehmen wir also an, $0 = 1 \in R$.
Wir müssen also jetzt zeigen, daß $R = \{0\}$.
Sei hierfür $a \in R$ beliebig.
Es gilt

$$a \cdot 1 = a \overset{3.15}{=} a \cdot 0 = 0$$

Also $a = 0$, d.h. $R = \{0\}$.

Wie bei Gruppen zeigt man:

Propo 3.18 Sei R ein Ring und $1'$ und 1 neutrale Elemente bezüglich der Multiplikation, so gilt $1' = 1$.

Beweis Nach (R3) gilt $a \cdot 1 = a = 1 \cdot a$ und $1' \cdot b = b = b \cdot 1'$ für alle $a, b \in R$. Insbesondere gilt für $a = 1'$ und $b = 1$: $1' \cdot 1 = 1' = 1$. □

Ein Ring $(R, +, \cdot)$ in dem $a \cdot b = b \cdot a$ für $a, b \in R$ heißt kommutativer Ring.

Bsp 3.19 Offenbar sind $R = \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ mit Verknüpfungen „+" und „·" Ringe. Da $a \cdot b = b \cdot a$ für $a, b \in R$ sind diese Ringe auch kommutativ.

Wir erinnern an die kommutative Gruppe $(\mathbb{Z}/n\mathbb{Z}, +)$. Diese Gruppe können wir durch weitere Verknüpfung

$[a] \cdot [b]$ = Rest von $a \cdot b$

zu einem Ring $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ machen.

Da $(\mathbb{Z}/n\mathbb{Z}, +)$ bereits kommutative Gruppe ist, müssen wir nun noch (R2), (R3) und (R4) nachprüfen.

Zu (R3): Für $[1] \in \mathbb{Z}/n\mathbb{Z}$ gilt:

$[a] \cdot [1]$ = Rest von a = $[a]$

$[1] \cdot [a]$ = Rest von a = $[a]$

Wegen Propo. 3.18 gilt

$\underline{1} = [1]$.

Analog zeigt man (R2) und (R4).

Der Ring $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ ist kommutativ. Es gilt nämlich

$[a][b]$ = Rest $a \cdot b$ = Rest $b \cdot a$ = $[b][a]$.

Wir werden später Ringe kennenlernen, die nicht kommutativ sind.

*

§ 4
Körper

In den Ringen $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ existiert für jedes Element $a \neq 0$ ein Inverses bezüglich „$\cdot$". In dem Ring $(\mathbb{Z}, +, \cdot)$ hingegen nicht.

(Um lineare Gleichungssysteme zu lösen, reicht es nicht Ringe als Zahlenmengen zu betrachten. Zum Beispiel ist die Gleichung

$$3x - 7 = 0$$

im Ring $(\mathbb{Z}, +, \cdot)$ nicht lösbar. In $\mathbb{Q}$ oder $\mathbb{R}$ allerdings schon. Bei Gleichungen der Form $aX + b = 0$, $a \neq 0$ müssten wir Folgende Umformung machen können:

$$aX + b = 0 \text{ , also } aX = -b.$$

Wenn in der Zahlenmenge das Inverse zu a bezüglich „$\cdot$" existiert, schreibt man

$$x = -b \cdot a^{-1} = -\frac{b}{a}$$

als Lösung. Dies führt auf den Begriff „Körper".

Def 4.1 Sei K ein kommutativer Ring. Man nennt K einen Körper, wenn gilt:

(i) $1 \neq 0$

(ii) jedes Element $a \neq 0$ besitzt ein Inverses bezüglich „$\cdot$".

Bsp. 4.2 offenbar sind $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ Körper.

Propo 4.3 Sei K ein Körper und $a, a', b \in K$ mit $b \neq 0$. Wenn $ab = a'b$, dann $a = a'$

Beweis Multiplizieren $ab = a'b$ auf beiden Seiten mit b^{-1}. □

Propo 4.4 Sei K ein Körper und $a, b \in K$. mit $ab = 0$. Dann ist $a = 0$ oder $b = 0$.

Beweis $ab = 0$, $a \neq 0$. Dann $a^{-1}ab = b = 0$. (15)

Wir wollen anhand $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ weitere Beispiele von Körpern angeben.

Wir führen nun den Körper der komplexen Zahlen $\mathbb{C}$ ein.

Wir setzen

$$\mathbb{C} := \mathbb{R} \times \mathbb{R} = \{(a, a') \mid a, a' \in \mathbb{R}\}$$

und definieren Addition und Multiplikation durch

$$(a, a') + (b, b') = (a + b, a' + b')$$

$$(a, a') \cdot (b, b') = (ab - a'b', ab' + a'b)$$

Man prüft leicht nach, dass $(\mathbb{C}, +)$ eine kommutative Gruppe ist. Das neutrale Element ist $0 = (0, 0)$ und das Negative von (a, a') ist $(-a, -a')$.

Außerdem prüft man leicht nach, daß $(\mathbb{C}, +, \cdot)$ ein kommutatives Ring ist:

Das Einselement ist $1 = (1,0)$ und

$$0 = (0,0) \neq (1,0) = 1.$$

Das entscheidende noch zu zeigende ist:

Propo 4.5 Das Inverse zu $(0,0) \neq (a,a') \in \mathbb{C}$ ist

$$(a,a')^{-1} = \left(\frac{a}{a^2+a'^2} , \frac{-a'}{a^2+a'^2} \right)$$

Beweis Nachrechnen.

Wir sehen, $(\mathbb{C}, +, \cdot)$ ist Körper. Nullelement ist $0 = (0,0)$ und Einselement ist $1 = (1,0)$.

Das Element $(0,1) \in \mathbb{C}$ heißt imaginäre Zahl und wird mit i bezeichnet.

Es gilt

$$i^2 = (0,1) \cdot (0,1) = (-1,0) = -1$$

Dafür schreibt man auch $i = \sqrt{-1}$.

Da -1 in $\mathbb{R}$ kein Quadrat ist, heißt i „imaginär".

Es gilt jetzt:

$$(a,a') = (a,0) + (0,1)\cdot(a',0) = a\cdot 1 + a'\cdot 1\cdot i$$
$$= a + i\cdot a'$$

Wir schreiben komplexe Zahlen $z = (a,a') \in \mathbb{C}$ daher auch als $z = a + ia'$.

Def 4.6 Sei $z = a + ia' \in \mathbb{C}$ eine komplexe Zahl, so heißt a der Realteil und a' der Imaginärteil der Zahl z. Das komplex Konjugierte von $z = a + ia'$ ist $\overline{z} = a - ia'$.
Der Betrag von z ist $|z| = \sqrt{a^2 + a'^2}$.

Mit $i^2 = -1$ ergeben die Verknüpfungen

$$(a + ia') + (b + ib') = (a+a') + i(b+b')$$

$$(a + ia')\cdot(b + ib') = (aa' - bb') + i(ab' + ba')$$

Betrachten wir die Gleichung

$$\text{(*)} \qquad x^2 + 1 = 0 \,,$$

so sehen wir $\Delta = 0 - 4 = -4$. Die Zahl -4 ist kein Quadrat in $\mathbb{R}$. Daher hat (*) in $\mathbb{R}$ keine Lösung. In $\mathbb{C}$ jedoch gilt

$$(2i)^2 = -4 .$$

Also hat (*) in $\mathbb{C}$ die Lösungen $\pm i$.

Dies kann man verallgemeinern zu

Theorem 4.7 (Fundamentalsatz der Algebra)

Jede Gleichung

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 = 0$$

mit $n \geq 1$ und $a_0, \dots, a_n \in \mathbb{C}$, $a_n \neq 0$ hat eine Lösung in $\mathbb{C}$.

Beweis wird in Analysis IV geführt.

Wir haben gesehen, daß $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ ein kommutativer Ring ist.

Für $n = 2$ gilt

$+$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

$\cdot$	$[0]$	$[1]$
$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$

Offenbar hat $[1]$ ein Inverses. Also ist $\mathbb{Z}/2\mathbb{Z}$ ein Körper.

Man kann auch $n = 3$ betrachten:

$\cdot$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$
$[2]$	$[0]$	$[2]$	$[1]$

Wir sehen, daß $[1]$ und $[2]$ ein Inverses besitzen. Also ist auch $\mathbb{Z}/3\mathbb{Z}$ ein Körper.

Für $n = 4$ allerdings gilt:

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

Mit Proposition 4.4 folgt dann aber, daß $\mathbb{Z}/4\mathbb{Z}$ kein Körper ist.
Es stellt sich die Frage, für welche $n \geq 1$ der Ring $\mathbb{Z}/n\mathbb{Z}$ ein Körper ist.
Wir müssen schauen, für welche $n \geq 1$ die Elemente $[a] \neq [0] \in \mathbb{Z}/n\mathbb{Z}$ ein Inverses besitzen.

Propo 4.8 Sei $[0] \neq [a] \in \mathbb{Z}/n\mathbb{Z}$. Dann besitzt $[a]$ ein Inverses genau dann, wenn ein $b \in \mathbb{Z}$ existiert mit der Eigenschaft, daß n die Zahl $ab-1$ teilt.

Beweis Sei $[b]$ das Inverse zu $[a]$. Dann gilt

$[a] \cdot [b] =$ Rest von $a \cdot b = [1]$.

Also $a \cdot b = q \cdot n + 1$, oder $a \cdot b - 1 = q \cdot n$. Also existiert ein $b \in \mathbb{Z}$, so daß n die Zahl $ab-1$ teilt.

Sei nun $b \in \mathbb{Z}$, so daß n die Zahl $a \cdot b - 1$ teilt. Es gilt also

$$a \cdot b - 1 = q' \cdot n, \quad \text{oder}$$

$a \cdot b = q' \cdot n + 1$. Sei nun $b = s \cdot n + r$, $0 \le r \le n-1$. Division mit Rest. Dann gilt $[a] \cdot [r] =$ Rest von $a \cdot r$. Es ist aber

$$a \cdot b = a(s \cdot n + r) = a \cdot s \cdot n + a \cdot r = q' \cdot n + 1.$$

Also gilt: $a \cdot r = (q' - a \cdot s) \cdot n + 1$.

Wegen Eindeutigkeit des Rests und der Zahl $(q' - as)$ folgt $[a][r] =$ Rest von $a \cdot r = [1]$.

Also hat $[a]$ ein Inverses. ☐

Man kann leicht entscheiden, ob so ein $b \in \mathbb{Z}$ existiert. Dies beruht auf dem euklidischen Algorithmus:

Sei $a, b > 0$ aus $\mathbb{Z}$. Wir setzen $x_0 = a$ und $x_1 = b$. Wir führen sukzessive Division mit Rest durch:

$$x_0 = q_1 x_1 + x_2 \quad , \quad 0 < x_2 < x_1$$
$$x_1 = q_2 x_2 + x_3 \quad , \quad 0 < x_3 < x_2$$
$$\vdots \qquad\qquad \vdots$$
$$x_{m-2} = q_{m-1} x_{m-1} + x_m \quad , \quad 0 < x_m < x_{m-1}$$
$$x_{m-1} = q_m x_m + 0$$

Da $x_1 > x_2 > x_3 > \dots \geq 0$ endet dieses Verfahren nach endlich vielen Schritten.

Man definiert $x_m = ggT(a,b)$ und nennt diese Zahl den <u>größten gemeinsamen Teiler</u> von a und b.

Nachdem man $x_m = ggT(a,b)$ gefunden hat, kann man das Verfahren „umdrehen".

$$ggT(a,b) = x_m = x_{m-2} - q_{m-1} x_{m-1}$$

$$x_{m-1} = x_{m-3} - q_{m-2} x_{m-2}$$

$$\vdots$$

$$x_2 = \underset{\parallel}{x_0} - q_1 \underset{\parallel}{x_1}$$
$$\quad\; a \qquad\; b$$

Durch sukzessives Einsetzen erhält man

$x_m = ggT(a,b) = ra + sb$, für geeignete $a, b \in \mathbb{Z}$.

Bsp 4.9 $\quad a = 107$, $b = 7$

$$x_0 = a = 107 = 15 \cdot 7 + 2$$
$$7 = 3 \cdot 2 + 1$$
$$2 = 2 \cdot 1 + 0$$

Also $ggT(107,7) = 1$. Weiter gilt:

$$1 = ggT(107,7) = 7 - 3 \cdot 2 \quad \text{und}$$
$$2 = 107 - 15 \cdot 7$$

Setzen wir ein, so erhalten wir

$$1 = 7 - 3 \cdot (107 - 15 \cdot 7) = 7 - 3 \cdot 107 + 7 \cdot 3 \cdot 15$$

$$= -3 \cdot 107 + 7(3 \cdot 15 + 1)$$

$$= -3 \cdot 107 + (46 \cdot 7$$

$$\begin{array}{cccc} \| & \| & & \| \\ r & a & & b \end{array}$$

Notation Seien $r, s \in \mathbb{Z}$. Man sagt r teilt s und schreibt $r \mid s$, wenn es ein $t \in \mathbb{Z}$ gibt mit $r \cdot t = s$.

Propo 4.10 Sind $a, b > 0$ aus $\mathbb{Z}$ und $g = ggT(a,b)$. Dann gilt:

(i) $g \mid a$ und $g \mid b$

(ii) Für jedes $d \in \mathbb{Z}$ mit $d \mid a$ und $d \mid b$ gilt $d \mid g$.

Beweis (i) Aus euklidischen Algorithmus folgt $g \mid x_m$ und $g \mid x_{m-1}$. Also auch $g \mid x_{m-2}$. Induktiv folgt $g \mid x_i$, $0 \le i \le m$. Insbesondere $g \mid x_0$ und $g \mid x_1$. Da $a = x_0$ und $b = x_1$ folgt Behauptung.

(ii) $d \mid a$ und $d \mid b$. Aus
euklidischem Algorithmus folgt induktiv
$d \mid x_i$, $0 \le i \le m$. Insbesondere teilt
d die Zahl $x_m = g$.

Aus Proposition 4.8 folgt sofort:

Propo. 4.11 Ein Element $[a] \neq [0] \in \mathbb{Z}/n\mathbb{Z}$
besitzt ein Inverses genau
dann, wenn $ggT(a,n) = 1$.

Eine ganze Zahl $p > 0$ heißt Primzahl,
wenn $p \neq 1$ und die einzigen Teiler d von
p nur $d = 1$ und $d = p$ sind. Beispielsweise
sind die ersten Primzahlen

$$p = 2, 3, 5, 7, 11, 13, \ldots$$

Propo 4.12 Sei $n > 0$. Der Ring $\mathbb{Z}/n\mathbb{Z}$ ist
Körper genau dann, wenn
n eine Primzahl ist.

Beweis „⇒" Sei $\mathbb{Z}/n\mathbb{Z}$ ein Körper und $d > 0$ ein Teiler von n. Wir müssen zeigen, daß $d = 1$ oder $d = n$.

Da $d > 0$ Teiler von n, gilt $0 < d \leq n$. Wenn $d = n$ brauchen wir nichts zu zeigen. Also $d < n$.

Dann hat $[d]$ ein Inverses.

Aus Proposition 4.11 folgt $ggT(d, n) = 1$. Wir schreiben $1 = r \cdot d + s \cdot n$. Da $d \mid n$ und $d \mid d$, folgt $d \mid 1$, d.h. $d = 1$.

„⇐" Sei $n > 0$ Primzahl und $[0] \neq [a] \in \mathbb{Z}/n\mathbb{Z}$. Wir müssen zeigen, daß $[a]$ Inverses besitzt.

D.h. wir müssen zeigen, daß $ggT(a, n) = 1$ gemäß Prop. 4.11.

Wäre $g = ggT(a, n) > 1$, so folgt aus $g \mid n$ und $g \mid a$, daß $g = n$, da n Primzahl.

Folglich $u \mid a$, was nicht gelten kann, da $a < u$. ☒

Man nennt die Körper $\mathbb{Z}/p\mathbb{Z}$ mit p Primzahl endliche Primkörper und schreibt $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Wir haben folgende Körper kennengelernt:

$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ und $\mathbb{F}_p$, p Primzahl.

§ 5
Vektorräume

Sei K ein Körper, z.B. $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p$.
Wir haben in der Einführung lineare Gleichungssysteme

$$\begin{aligned} a_{11}X_1 + a_{12}X_2 + \dots + a_{1n}X_n &= 0 \\ a_{21}X_1 + a_{22}X_2 + \dots + a_{2n}X_n &= 0 \\ \vdots \qquad\quad \vdots \qquad\quad & \qquad\quad \vdots \\ a_{m1}X_1 + a_{m2}X_2 + \dots + a_{mn}X_n &= 0 \end{aligned} \qquad (*)$$

betrachtet. Wir haben folgende Kurzschreibweise

$$\sum_{j=1}^{n} a_{ij}X_j = 0, \quad 1 \le i \le m.$$

Eine Lösung von $(*)$ ist ein n-Tupel $(\alpha_1, \dots, \alpha_n) \in K^n$ mit

$$\sum_{j=1}^{n} a_{ij}\alpha_j = 0, \quad 1 \le i \le m$$

Die Lösungsmenge ist gegeben durch

$$L = \{ (\alpha_1, \dots, \alpha_n) \in K^n \mid \sum_{j=1}^{n} a_{ij}\alpha_j = 0, \ 1 \le i \le m \}.$$

Diese Menge L hat folgende Eigenschaft: Sind $(\alpha_1, \dots, \alpha_n)$ und $(\alpha_1', \dots, \alpha_n')$ Lösungen und $\lambda \in K$, so ist

$$(\alpha_1 + \lambda\alpha_1', \dots, \alpha_n + \lambda\alpha_n')$$

ebenfalls eine Lösung. Außerdem ist $(0, \dots, 0) \in K^n$ auch eine Lösung. Dies kann man abstrahieren zum Begriff des

Vektorraums.

Def 5.1 Sei K ein Körper. Ein K-Vektorraum ist eine kommutative Gruppe V, versehen mit einer Verknüpfung

$$K \times V \longrightarrow V, \ (\lambda, a) \mapsto \lambda \cdot a,$$

so daß

folgende Axiome gelten:

(V1) $(\lambda+\mu)\cdot a = \lambda a + \mu \cdot a$, für $a \in V$ und $\lambda, \mu \in K$.

(V2) $(\lambda \cdot \mu)\cdot a = \lambda(\mu \cdot a)$, für $a \in V$ und $\lambda, \mu \in K$.

(V3) $\lambda(a+b) = \lambda a + \lambda b$, für $a, b \in V$ und $\lambda \in K$.

(V4) $1 \cdot a = a$ für Einselement $1 \in K$.

Die Elemente $a \in V$ heißen Vektoren und die $\lambda \in K$ werden Skalare genannt.

Die Gruppen-Verknüpfung

$$V \times V \to V, \quad (a,b) \mapsto a+b$$

heißt Vektoraddition. Die Verknüpfung

$$K \times V \to V, \quad (\lambda, a) \mapsto \lambda \cdot a$$

heißt Skalarmultiplikation.

Bsp 5.2 Standardvektorraum

$V = K^n$, $n \geq 0$.

Vektoraddition ist gegeben durch

$$(\alpha_1, \dots, \alpha_n) + (\alpha_1', \dots, \alpha_n') = (\alpha_1 + \alpha_1', \dots, \alpha_n + \alpha_n'),$$

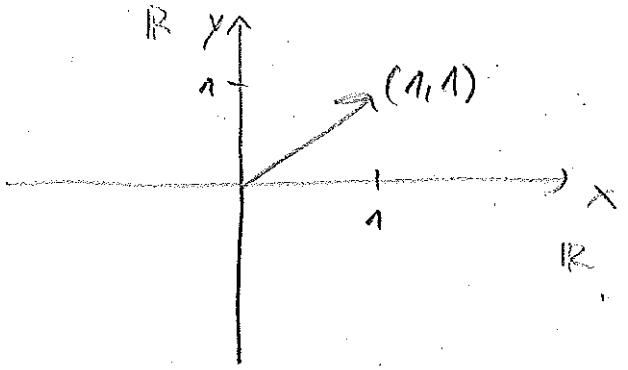
Skalarmultiplikation durch

$$\lambda \cdot (\alpha_1, \dots, \alpha_n) = (\lambda \alpha_1, \dots, \lambda \alpha_n).$$

Bsp 5.3 Die Lösungsmenge $L \subset K^4$ eines LGS $\sum_{j=1}^{n} a_{ij} x_j = 0$, $1 \leq i \leq m$.

Vektoraddition und Skalarmultiplikation ist gegeben wie in Bsp. 5.2.

Bsp 5.4 $K = \mathbb{R}$. Dann ist $V = \mathbb{R}^2$ das bekannte Koordinatensystem



Bemerkung. Im Standardvektorraum $V = K^n$ schreibt man die Vektoren

$a = (\alpha_1, \ldots, \alpha_n)$ auch so:

$$a = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$$

Bsp 5.5 Sei K ein Körper

Ein Polynom über K ist ein formaler Ausdruck der Gestalt $p(T) = a_0 + a_1 T + \cdots + a_n T^n$, wobei $a_0, a_1, \ldots, a_n \in K$. Man bezeichnet die Menge aller solcher Polynome mit $K[T]$. Auf dieser Menge hat man Addition: Sei ohne Einschränkung $m \geq n$ und

$$p(T) = a_0 + a_1 T + \cdots + a_n T^n \quad \text{und}$$

$$q(T) = b_0 + b_1 T + \cdots + b_n T^n + b_{n+1} T^{n+1} + \cdots + b_m T^m.$$

Dann ist

$$p(T) + q(T) = (a_0 + b_0) + (a_1 + b_1) T + \cdots + (a_n + b_n) T^n + b_{n+1} T^{n+1} + \cdots + b_m T^m.$$

Mit dieser Addition wird $(K[T], +)$ zu einer kommutativen Gruppe. Neutrales Element ist das Nullpolynom $p(T) = 0$.

Sei $\lambda \in K$ und $p(T) = a_0 + a_1 T + \dots + a_n T^n$ ein Polynom. Dann definiert

$$\lambda \cdot p(T) = \lambda a_0 + \lambda a_1 T + \dots + \lambda a_n T^n$$

eine Skalarmultiplikation. Man prüft leicht nach, daß $K[T]$ mit obiger Addition und Skalarmultiplikation ein K-Vektorraum wird.

Zur besseren Unterscheidung schreiben wir $0_V \in V$ für den Nullvektor und $0_K \in K$ für das Nullelement des Körpers.

Propo 5.6 In jedem K-Vektorraum V gilt:

(i) $0_K \cdot a = 0_V$

(ii) $\lambda \cdot 0_V = 0_V$

(iii) $(-1) \cdot a = -a$

für alle $a \in V$.

Beweis zu (i):

$$0_K \cdot a + a = 0_K \cdot a + 1 \cdot a$$
$$= (0_K + 1) \cdot a = 1 \cdot a = a$$

Auf beiden Seiten $-a$ addieren ergibt

$$0_K \cdot a = 0.$$

zu (ii):

$$\lambda \cdot 0_V = \lambda \cdot 0_V + \lambda \cdot 0_V - (\lambda \cdot 0_V)$$
$$= \lambda \cdot (0_V + 0_V) - (\lambda \cdot 0_V) = \lambda \cdot 0_V - \lambda \cdot 0_V$$
$$= 0_V$$

zu (iii)

$$a + (-1) \cdot a = 1 \cdot a + (-1) \cdot a = (1 + (-1)) \cdot a$$
$$= 0_K \cdot a = 0_V$$
$$\text{(i)}$$

Also $-a = (-1) \cdot a$.

□

Propo 5.7 Sei V ein K-Vektorraum und $\lambda \in K$ und $a \in V$. Wenn $\lambda \cdot a = 0_V$, so muss $\lambda = 0_K$ oder $a = 0_V$.

Def 5.8 Es sei V ein K-Vektorraum. Eine Teilmenge $U \subset V$ heißt Untervektorraum, wenn gilt:

(i) $0_V \in U$

(ii) Sind $a, b \in U$, so auch $a+b \in U$.

(iii) Sind $\lambda \in K$ und $a \in U$, so ist $\lambda \cdot a \in U$.

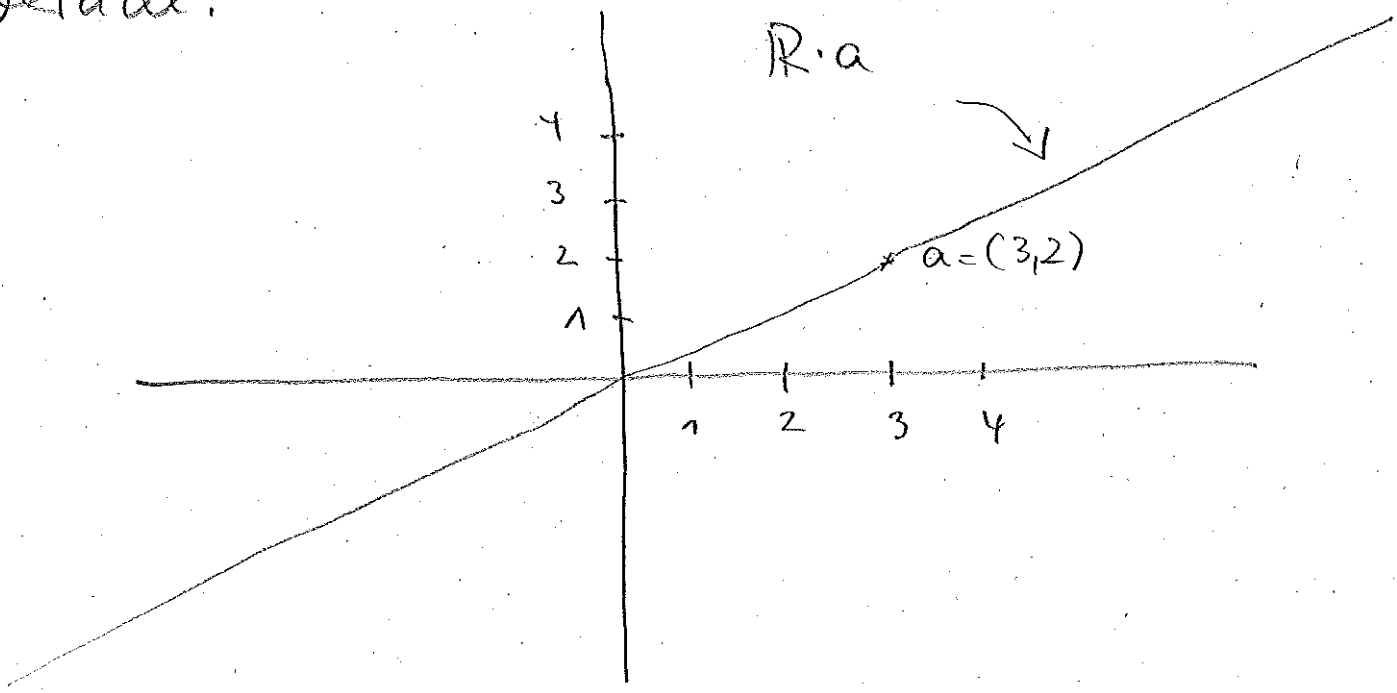
Bsp 5.9 (Geraden).

Für einen Vektor $a \in V$ ist die Menge

$$K \cdot a := \{ \lambda \cdot a \mid \lambda \in K \}$$

ein Untervektorraum von V. Im Falle $a \neq 0$ nennt man $K \cdot a$ eine Gerade.

Ist $V = \mathbb{R}^2$ und $a = (3,2) \in V$, so ist $\mathbb{R} \cdot a = \{(\lambda 3, \lambda 2) \mid \lambda \in \mathbb{R}\}$ folgende Gerade:



Lemma 5.10 Sei V ein K-Vektorraum. Eine nicht-leere Teilmenge $U \subset V$ ist ein Untervektorraum genau dann, wenn für alle $a, b \in U$ und $\lambda \in K$ auch $a + \lambda \cdot b \in U$.

Beweis Wenn U ein Untervektorraum ist, so gilt für alle $a, b \in U$ und $\lambda \in K$ trivialerweise $a + \lambda b \in U$.

Seien $a, b \in U$ und $\lambda \in K$ mit $a + \lambda b \in U$.
Wir müssen die Bedingungen (i), (ii) und (iii) an die Definition nachprüfen.

Zu (i): Da $U \neq 0$ gibt es ein $b \in U$.
Für $a = b$ und $\lambda = -1$ gilt
$a + \lambda \cdot b = b + (-1) \cdot b = 0_V \in U$.

Zu (ii): Seien $a, b \in U$ und $\lambda = 1$.
Dann gilt $a + 1 \cdot b = a + b \in U$.

Zu (iii): Da nach (i) $0_V \in U$ folgt mit
$a = 0_V$, $b \in U$, $\lambda \in K$ gerade
$a + \lambda \cdot b = \lambda \cdot b \in U$.

Weitere Beispiele von Untervektorräumen:

Bsp. 5.11 Sei $V = \{ f : \mathbb{R} \to \mathbb{R} \}$ der $\mathbb{R}$-Vektorraum aller Abbildungen auf $\mathbb{R}$.
Vektoraddition ist gegeben durch
$(f + g)(x) = f(x) + g(x)$.
Skalarmultiplikation

ist gegeben durch

$$(\lambda f)(x) = \lambda \cdot f(x).$$

Sei $U = \{ f : \mathbb{R} \to \mathbb{R} \mid f(x) \leq 0 \}$. Dann ist $U \subset V$ ein Untervektorraum.

Bsp. 5.12 Sei L ein Körper. Eine Teilmenge $K \subset L$ heißt Unterkörper, falls:

(i) $\lambda, \mu \in K$, so auch $\lambda + \mu, \lambda \cdot \mu \in K$

(ii) $\lambda \in K$, so auch $-\lambda \in K$

(iii) $\lambda \in K$, $\lambda \neq 0$, so auch $\lambda^{-1} \in K$

(iv) $0, 1 \in K$.

Dann ist L ein K-Vektorraum und $K \subset L$ ein Untervektorraum.

Bsp. 5.13 Sei $V = K[T]$. Mit Skalarmultiplikation

$$\lambda \cdot p(T) = \lambda \cdot (a_0 + a_1 T + \cdots + a_n T^n)$$
$$= \lambda a_0 + \lambda a_1 T + \cdots + \lambda a_n T^n$$

wird $K[T]$ zu einem K-Vektorraum.

Sei $p(T) = a_0 + a_1 T + \cdots + a_n T^n$ und $a_n \neq 0$, so nennt man n den Grad von $p(T)$ und schreibt $\deg(p) = n$.

Für das Nullpolynom $p(T) = 0$ setzt man $\deg(p) = -\infty$. Sei nun $d > 0$ fest und

$$U = \{ p \in K[T] \mid \deg(p) \leq d \}.$$

Dann ist $U \subset V$ ein Untervektorraum.

(

Propo. 5.14 Sei V ein Vektorraum, $U_i \subset V$, $i \in I$ Untervektorräume. Dann ist

$$U = \bigcap_{i \in I} U_i \subset V$$

ein Untervektorraum.

Beweis: Wir müssen zeigen, daß für $a, b \in U$, $\lambda \in K$ auch $a + \lambda b \in U$.

Für $b \in U$ gilt $b \in U_i$ für alle $i \in I$. Da U_i Untervektorraum, folgt $\lambda b \in U_i$ für alle $i \in I$. Da $a \in U$, folgt $a \in U_i$ für alle $i \in I$. Also sind $a, \lambda b \in U_i$ für alle $i \in I$.

Aus Lemma 5.10 folgt

$$a + \lambda b \in U_i \text{ für alle } i \in I.$$

Insgesamt gilt also

$$a + \lambda b \in U.$$

□

§ 6
Linearkombinationen und Basen

Sei K ein Körper und V ein K-Vektorraum. Sind $a_1, \dots, a_r \in V$ und $\lambda_1, \dots, \lambda_r \in K$, so nennt man

$$\lambda_1 a_1 + \dots + \lambda_r a_r = \sum_{i=1}^{r} \lambda_i a_i \in V$$

eine Linearkombination der Vektoren $a_1, \dots, a_r \in V$.

Def 6.1 Ein System von Vektoren $a_1, \dots, a_n$ eines K-Vektorraums V heißt linear unabhängig, wenn aus einer Gleichung

$$\sum_{i=1}^{n} \lambda_i a_i = 0 \quad , \quad \lambda_i \in K$$

notwendig $\lambda_1 = \lambda_2 = \dots = \lambda_n = 0$ folgt.

In obige Definition ist lineare Unabhängigkeit für endliche Systeme von Vektoren formuliert. Der Begriff überträgt sich auch auf beliebige Systeme.

Sei nun $a_i \in V$, $i \in I$ beliebige Familie von Vektoren und $\lambda_i \in K$, $i \in I$ Skalare.

Eine Linearkombination der a_i ist Ausdruck der Form

$$\sum_{i \in I} \lambda_i a_i \quad , \quad \lambda_i \in K$$

wobei die $\lambda_i \in K$ für fast alle $i \in I$ verschwinden.

Man bezeichnet dann ein System a_i, $i \in I$ von Vektoren aus V als linear unabhängig, wenn aus dem Verschwinden einer Linear-kombination der a_i, also einer Gleichung

der Form $\sum_{i \in I} \lambda_i a_i = 0$ notwendig

$\lambda_i = 0$ für alle $i \in I$ folgt.

Bsp 6.2 Sei $V = K[T]$ der K-Vektorraum der Polynome und $a_i = T^i$, $i \in \mathbb{N}$.
Dann ist das System der Vektoren $a_i \in V$, $i \in \mathbb{N}$ linear unabhängig.

Bsp 6.3 $\mathbb{R}$ ist ein Unterkörper von $\mathbb{C}$.
Dann ist $\mathbb{C}$ ein $\mathbb{R}$-Vektorraum.
Die Vektoren $a_1 = 1$ und $a_2 = i$ sind linear unabhängig.

Bemerkung 6.4 Ist ein System $a_i \in V$, $i \in I$ nicht linear unabhängig, so sagt man $a_i \in V$ sind linear abhängig.

Def 6.5 Sei V ein K-Vektorraum und $A \subset V$ eine Teilmenge.

Dann ist

$$\langle A \rangle = \left\{ \sum_{i=1}^{r} \lambda_i a_i \;\middle|\; r \in \mathbb{N}, \lambda_i \in K, a_i \in A \right\}$$

ein Untervektorraum von V.

Man nennt $\langle A \rangle$ den von A erzeugten Untervektorraum in V.

Falls $\langle A \rangle = V$, so sagt man A erzeugt den Vektorraum V.

Prop 6.6 Sei V ein K-Vektorraum und $A \subset V$ eine Teilmenge. Dann gilt

$$\bigcap_{A \subset U} U = \langle A \rangle$$

Folgerung ist $\langle A \rangle$ der kleinste Untervektorraum der A enthält.

Beweis

„$\subset$": Der Untervektorraum $\langle A \rangle$ enthält die Menge A. Also gilt

$$\bigcap_{A \subset U} U \subset \langle A \rangle.$$

„$\supset$": Sei $\sum_{i=1}^{r} \lambda_i a_i \in \langle A \rangle$.

Da $a_i \in A \subset U$ und U Untervektorraum sind gilt

$$\sum_{i=1}^{r} \lambda_i a_i \in U. \text{ Also}$$

$$\sum_{i=1}^{r} \lambda_i a_i \in \bigcap_{A \subset U} U.$$

□

Es gelten folgende elementare Eigenschaften:

(i) $\langle \emptyset \rangle = 0$

(ii) $A \subset \langle A \rangle$ für jede Teilmenge $A \subset V$

(iii) $\langle U \rangle = U$ für einen Untervektorraum $U \subset V$.

(iv) $A \subset B$, dann $\langle A \rangle \subset \langle B \rangle$.

Def 6.7 Sei V ein K-Vektorraum und $a_i \in V$, $i \in I$ Vektoren. Dann nennt man $a_i \in V$ eine Basis von V, falls

(i) $\langle \{ a_i \mid i \in I \} \rangle = V$

(ii) Die Familie $a_i \in V$, $i \in I$ ist linear unabhängig.

Bsp. 6.8 Sei $V = K^n$ und $e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$, $e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \dots, e_n = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$

die Einheitsvektoren.

Dann ist $e_1, \dots, e_n \in V$ eine Basis von V.

Das sieht man folgendermaßen:

(i) Da jeder Vektor $a = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \in K^n$

geschrieben werden kann als

$$\sum_{i=1}^{n} a_i e_i = a$$

folgt $\langle \{ e_i \mid i = 1, \ldots, n \} \rangle = V$.

(ii) Man rechnet leicht nach, daß $e_1, \ldots, e_n$ linear unabhängig sind.

Für $n = 1$ oder $n = 2$ ist es oft leicht nachzurechnen, ob $a_1, \ldots, a_n \in V$ linear unabhängig sind.

Lemma 6.9 Sei $a \in V$ ein Vektor. Dann gilt:

$a \in V$ ist linear unabhängig genau dann, wenn $a \neq 0$.

Beweis „$\Leftarrow$" Sei $n \cdot a = 0$. Nach Prop. 5.7 gilt $n = 0$ oder $a = 0$. Da $a \neq 0$ nach Voraussetzung folgt $n = 0$.

„⇒" Angenommen $a = 0$. Nehme $\lambda = 1$. Dann gilt $\lambda \cdot a = 0$. Dies ist ein Widerspruch zur linearen Unabhängigkeit.

□

Wir haben eben definiert, was eine Basis eines Vektorraums V ist. Wir haben in Beispielen gesehen, daß Basen existieren. Es stellt sich allerdings die Frage, ob jeder Vektorraum eine Basis besitzt. Um das zu beweisen, benötigen wir folgendes

Lemma 6.10 Seien $a_1, \dots, a_n \in V$ linear unabhängig und $b \in V$ ein beliebiger Vektor. Dann gilt:

$a_1, \dots, a_n, b \in V$ sind linear unabhängig genau dann, wenn

$b \notin \langle \{a_1, \dots, a_n\} \rangle$.

Beweis

„⇒" Angenommen $b \in \langle \{a_1, \dots, a_n\} \rangle$.

Dann ist

$$b = \lambda_1 a_1 + \dots + \lambda_n a_n \quad , \text{ also}$$

$$1 \cdot b + (-\lambda_1) a_1 + \dots + (-\lambda_n) a_n = 0 .$$

Sind $a_1, \dots, a_n, b \in V$ linear unabhängig, so folgt $1 = 0$ in K. Dies ist ein Widerspruch.

„⇐" Sei $\lambda_1 a_1 + \lambda_2 a_2 + \dots + \lambda_n a_n + \lambda_{n+1} \cdot b = 0$.

Angenommen $\lambda_{n+1} \neq 0$. Dann ist

$$b = \left(-\frac{\lambda_1}{\lambda_{n+1}}\right) a_1 + \dots + \left(-\frac{\lambda_n}{\lambda_{n+1}}\right) a_n .$$

Dies ist Widerspruch zur Voraussetzung $b \notin \langle \{a_1, \dots, a_n\} \rangle$. Also folgt $\lambda_{n+1} = 0$.

Dann ist aber

$$\lambda_1 a_1 + \dots + \lambda_n a_n = 0 .$$

Da $a_1, \dots, a_n \in V$ linear unabhängig, folgt $\lambda_1 = \lambda_2 = \dots = \lambda_n = \lambda_{n+1} = 0$.

Außerdem benötigen wir folgende

Propo. 6.11 Ist $a_i \in V$, $i \in I$ ein Erzeugendensystem, so gibt es eine Teilmenge $J \subset I$, so daß $a_j \in V$, $j \in J$ eine Basis bilden.

Beweis: Einfachheitshalber nehmen wir an, daß $I = \mathbb{N}$.

Nun bilden wir die Teilmenge

$$J = \{ j \in I \mid a_j \notin \langle a_0, \dots, a_{j-1} \rangle \}.$$

Wir werden zeigen, daß a_j, $j \in J$ eine Basis bilden.

Sei $U = \langle \{ a_j \mid j \in J \} \rangle$. Wir zeigen zunächst $U = V$. Dafür müssen wir beweisen, daß $a_i \in U$, $i \in I$.

Betrachten wir nun die Menge

$$L = \{ i \in I \mid a_i \notin U \}.$$

Sei $m \in L$ das kleinste Element. Dann gilt $a_0, \dots, a_{m-1} \in U$ aber $a_m \notin U$.

Dann gilt

$$\langle a_0, \dots, a_{m-1} \rangle \subset U \quad \text{aber}$$

$a_m \notin \langle a_0, \dots, a_{m-1} \rangle$. Also ist $m \in J$.

Dann gilt aber $a_m \in U$. Dies ist ein Widerspruch, also $L = \emptyset$.

Wir zeigen nun, daß a_j, $j \in J$ linear unabhängig sind. Wir betrachten

$$\sum_{j \in M} \lambda_j a_j = 0$$

und $M = \{ j \in J \mid \lambda_j \neq 0 \}$

Nach Definition von Linearkombination sind diese Mengen M endlich.

Da $J \subset I = \mathbb{N}$ und M endlich, existiert ein größtes Element $n \in M$. Dann gilt

$$a_n = -\frac{1}{\lambda_n} \cdot \sum_{\substack{j \in M \\ j \neq n}} \lambda_j a_j \in \langle a_0, \ldots, a_{n-1} \rangle$$

Also ist $n \notin J$ und somit $n \notin M$.
Dies bedeutet $M = \emptyset$.

□

Theorem 6.12 Jeder Vektorraum besitzt eine Basis.

Beweis Sei V ein K-Vektorraum. Dann existiert immer ein Erzeugendensystem. $a_i \in V$, $i \in I$. Man kann dafür die Familie aller Vektoren aus V nehmen.

Die Aussage folgt jetzt aus Proposition 6.11

□

Bemerkung 6.13

Der Beweis von Proposition 6.11 und somit von Theorem 6.12 basiert auf der Annahme $I = \mathbb{N}$. Einen Beweis kann man auch für beliebige Indexmengen I durchführen. Man muss auf I eine Wohlordnung wählen. Das stellt sicher, dass jede nicht-leere Teilmenge $J \subset I$ ein kleinstes Element besitzt. Ein Axiom aus der Mengentheorie stellt die Existenz solcher Wohlordnungen sicher.

Bemerkung 6.14

Theorem 6.12 ist eine Existenzaussage. Es gibt uns keine Möglichkeit an die Hand, Basen einfach hinzuschreiben. Beispielsweise kann man keine Basis von $\mathbb{R}$ als $\mathbb{Q}$-VR hinschreiben.

§7

Endlich-dimensionale Vektorräume

Wir haben gesehen, daß jeder Vektorraum eine Basis besitzt. In der LAI beschäftigen wir uns hauptsächlich mit endlich-dimensionalen.

Def 7.1 Ein K-Vektorraum V heißt endlich-dimensional, wenn

$$\langle a_1, \dots, a_m \rangle = V.$$

Man schreibt $\dim_K(V) < \infty$.

Bsp 7.2 Der Vektorraum $V = K^4$ ist endlich-dimensional, da

$$\langle e_1, \dots, e_n \rangle = V.$$

Bsp. 7.3 Der $\mathbb{R}$-Vektorraum $\mathbb{C}$ ist endlich-dimensional. Es ist

$$\langle 1, i \rangle = \mathbb{C}.$$

Ist V endlich-dimensional, so ist

$$\langle a_1, \dots, a_m \rangle = V.$$

Proposition 6.10 zeigt, daß man durch Weglassen von Vektoren aus der Menge $\{a_1, \dots, a_m\}$ eine Basis erhält. Es stellt sich die Frage, wie viele Vektoren dann eine Basis bilden.

Um diese Frage zu beantworten benötigen wir folgendes Lemma.

Lemma 7.4 (Austauschsatz von Steinitz)

Sei $a_1, \dots, a_n \in V$ eine Basis und $b = \sum_{i=1}^{n} \eta_i a_i$ ein Vektor. Für jedes $1 \leq j \leq n$ mit $\eta_j \neq 0$ ist

$$a_1, a_2, \dots, a_{j-1}, b, a_{j+1}, \dots, a_n \in V$$

ebenfalls Basis.

Beweis Wir zeigen

$a_j \in \langle a_1, a_2, \dots, a_{j-1}, b, a_{j+1}, \dots, a_n \rangle$ ⊛

Dann folgt $\langle a_1, \dots, a_{j-1}, b, a_{j+1}, \dots, a_n \rangle = V$

Es gilt

$$b - \sum_{i \neq j} \eta_i a_i = \eta_j a_j .$$

Da $\eta_j \neq 0$ erhalten wir

$$a_j = \frac{1}{\eta_j} b - \sum_{i \neq j} \frac{\eta_i}{\eta_j} a_i \text{ , also gilt } ⊛.$$

Wir zeigen nun, daß

$a_1, \dots, a_{j-1}, b, a_{j+1}, \dots, a_n$ linear unabhängig sind. Sei

$$\mu_j b + \sum_{i \neq j} \mu_i a_i = 0 ,$$

dann müssen wir $\mu_1 = \mu_2 = \dots = \mu_n = 0$ zeigen. Da $b = \sum_{i=1}^{n} \eta_i a_i$ erhalten wir

$$0 = \mu_j \Big(\sum_{i=1}^{n} \lambda_i a_i \Big) + \sum_{i \neq j} \mu_i a_i$$

$$= \mu_j \lambda_j a_j + \sum_{i \neq j} (\mu_j \lambda_i + \mu_i) a_i$$

Da $a_1, \dots, a_n$ linear unabhängig folgt

$$\mu_j \lambda_j = 0 \quad \text{und} \quad \mu_j \lambda_i + \mu_i = 0$$

Da $\lambda_j \neq 0$ nach Voraussetzung, folgt

$\mu_j = 0$ und schließlich $\mu_i = 0$. ☐

Bemerkung 7.5 Ist $a_1, \dots, a_n \in V$ eine Basis, dann gibt es zu jedem $v \in V$ genau ein $(\lambda_1, \dots, \lambda_n) \in K^n$, so daß

$$v = \lambda_1 a_1 + \dots + \lambda_n a_n.$$

Das sieht man folgendermaßen:

Da $\langle a_1, \ldots, a_n \rangle = V$ kann man jedes $v \in V$ schreiben als

$$v = \eta_1 a_1 + \eta_2 a_2 + \ldots + \eta_n a_n .$$

Angenommen

$v = \mu_1 a_1 + \mu_2 a_2 + \ldots + \mu_n a_n$, so folgt

$$\eta_1 a_1 + \ldots + \eta_n a_n = \mu_1 a_1 + \ldots + \mu_n a_n .$$

Also $(\eta_1 - \mu_1) a_1 + \ldots + (\eta_n - \mu_n) a_n = 0$.

Da $a_1, \ldots, a_n$ linear unabhängig, folgt $\eta_i = \mu_i$ für alle $1 \leq i \leq n$.

Korollar 7.6 Sind $a_1, \ldots, a_n$ und $b_1, \ldots, b_m$ Basen von V, so gibt es an jedem a_i ein b_j, so daß aus $a_1, \ldots, a_n$ wieder eine Basis entsteht, wenn a_i durch b_j ersetzt wird.

Beweis Folgt aus Lemma 7.4

Theorem 7.7 Sind $a_1, \ldots, a_n$ und $b_1, \ldots, b_m$ Basen von V, so ist $n = m$.

Beweis Angenommen $n \neq m$, $n < m$.
Dann könnten durch wiederholtes Anwenden von Korollar 7.6 alle Vektoren $b_1, \ldots, b_m$ gegen Vektoren $a_1, \ldots, a_n$ ausgetauscht werden. Man erhielte so eine Basis, in der mindestens ein Vektor doppelt vorkommt. Dies widerspricht jedoch der linearen Unabhängigkeit der neuen Basis.

□

Das Theorem rechtfertigt folgende Definition.

Def 7.8 Sei V ein endlich-dimensionaler K-Vektorraum. Die Dimension

$$\dim_K(V) \in \mathbb{N}$$

ist die Anzahl der Basisvektoren einer Basis $a_1, \ldots, a_n \in V$.

Bsp 7.9 Sei $V = K^n$, so gilt

$$\dim_K(V) = n.$$

Bsp. 7.10 Sei $V = \mathbb{C}$ aufgefasst als $\mathbb{R}$-Vektorraum, so gilt

$$\dim_{\mathbb{R}}(\mathbb{C}) = 2.$$

Propo. 7.11 Seien $a_1, \ldots, a_n \in V$ eine Basis und $b_1, \ldots, b_m$ beliebige Vektoren. Ist $m > n$, so sind $b_1, \ldots, b_m$ linear abhängig.

Beweis: 1. Fall: es existieren $i,j \in \{1,\dots,m\}$ $i \neq j$, so daß $b_i = b_j$. Dann sind $b_1,\dots,b_m$ offensichtlich linear abhängig.

2 Fall: es existiert ein $i \in \{1,\dots,m\}$, so daß $b_i = 0$. Dann sind die $b_1,\dots,b_m$ linear abhängig.

3 Fall: $b_1,\dots,b_m$ sind alle verschieden und $b_i \neq 0$ für alle $1 \leq i \leq m$.
Durch wiederholtes Anwenden von Lemma 7.4 kann man alle Vektoren der Basis $a_1,\dots,a_n \in V$ gegen die Vektoren $b_1,\dots,b_m$ austauschen. Da $m > n$ bleiben also n der Vektoren aus der Menge

$\{b_1, \dots, b_m\}$ eine Basis. Ohne Einschränkung seien also $b_1, \dots, b_n$. Dann kann b_{n+1} aus $b_1, \dots, b_n$ linearkombiniert werden. ☒

Korollar 7.12 Sei V ein K-Vektorraum. Dann gilt:

$\dim_K(V) = \infty$ genau dann, wenn es eine Folge von Vektoren $a_0, a_1, a_2, \dots \in V$ gibt, welche linear unabhängig sind.

Beweis „$\Rightarrow$" Sei $\dim_K(V) = \infty$. OBdA konstruieren wir eine Folge rekursiv. Sei $n \geq 0$ und die Folge $a_0, \dots, a_n$ bereits festgelegt. Da $\dim_K(V) = \infty$, folgt

$$\langle a_0, \dots, a_n \rangle \subsetneq V.$$

Wähle Vektor $a_{n+1} \notin \langle a_0, .., a_n \rangle$.
Aus Lemma 6.10 folgt, daß
$a_0, .., a_n, a_{n+1}$ linear unabhängig sind.

„⇐" Folgt direkt aus Proposition 7.11.

□

Bsp 7.13 Sei $V = K[T]$. Dann haben wir in Beispiel 6.2 gesehen, daß $a_i = T^i$, $i \in \mathbb{N}$ eine Folge linear unabhängiger Vektoren ist. Korollar 7.12 zeigt $\dim_K(V) = \infty$.

Propo 7.14 Sei V endlich-dimensional. Dann ist jeder Untervektorraum $U \subset V$ auch endlich-dimensional und es gilt $\dim_K(U) \leq \dim_K(V)$.

Beweis Sei $\dim_K(V) = n$ und $a_1, \ldots, a_n \in V$ eine Basis.

Angenommen $\dim_K(U) > n$.

Dann gibt es Vektoren $b_1, \ldots, b_{n+1} \in U$, welche linear unabhängig sind. Falls $\dim_K(U) < \infty$ ist das offensichtlich. Falls $\dim_K(U) = \infty$, folgt das aus Korollar 7.12.

Aus Proposition 7.11 jedoch folgt, daß $b_1, \ldots, b_{n+1}$ linear unabhängig sein müssen.

Dies ist ein Widerspruch zu $\dim_K(V) = n$, also $\dim_K(U) \leq n$.

□

Bsp 7.15 Sei $V = \mathbb{R}^3$ und $U \subset V$ ein Untervektorraum. Dann gilt

$\dim_K(U) \in \{0, 1, 2, 3\}$

Die Geraden $U = \langle a \rangle$, $a \neq 0$ haben $\dim_K(U) = 1$.

Wie sehen die Untervektorräume U aus, für die $\dim_K(U) = 0$ oder $\dim_K(U) = 3$?

Propo 7.16 Sei V endlich - dimensional und $U \subset V$ Untervektorraum. Dann gilt:

$U = V \iff \dim(U) = \dim(V)$

Beweis „⇒" klar.

„⇐" Sei $n = \dim(U) = \dim(V)$.

Wähle Basis $b_1, \dots, b_n \in U$.

Wir zeigen, daß $\langle b_1, \dots, b_n \rangle = V$.

Angenommen nicht, so existiert $b_{n+1} \in V$ mit $b_{n+1} \notin \langle b_1 \dots, b_n \rangle$.

Nach Lemma 6.10 sind

$b_1, \dots, b_n, b_{n+1}$ linear unabhängig.

Dies ist ein Widerspruch, da

$\dim(V) = n$.

□

Korollar 7.17 Für jeden Vektorraum V gilt

$$V = \{0\} \iff \dim(V) = 0.$$

Bsp 7.18 Sei $V = \mathbb{R}^3$ und $U \subset V$. Ist $\dim(U) = 0$, so $U = \{0\}$. Ist $\dim(U) = 3$, so folgt $U = \mathbb{R}^3$.

Bsp 7.19 Sei $V = \mathbb{R}^3$ und $a = (1,1,1)$. Dann ist $\dim(U) = 1$ für $U = \langle a \rangle$. Wir sehen

$$a = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \quad e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \quad e_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

sind Basis von $\mathbb{R}^3$.

Dies lässt sich verallgemeinern.

(Basisergänzungssatz)

Propo 7.20 Sei $a_1, \dots, a_n \in V$ eine Basis und $b_1, \dots, b_m$ linear unabhängig. Dann gilt $m \leq n$ und die $b_1, \dots, b_m$ können durch $n-m$ Vektoren aus der Menge $\{a_1, \dots, a_n\}$ zu einer Basis ergänzt werden.

Beweis: Beweis per Induktion nach m.

$m = 0$ klar.

Sei nun $m \geq 1$.

Nehmen an, die Behauptung gelt für $m-1$. Wir können also die linear unabhängigen Vektoren

$$b_1, \dots, b_{m-1} \in V$$

durch $n-(m-1)$ Vektoren aus der Menge $\{a_1, \dots, a_n\}$ zu einer Basis ergänzen.

Ohne Einschränkung seien dies $a_m, a_{m+1}, \dots, a_n$.

Also bilden die Vektoren

$$b_1, \dots, b_{m-1}, a_m, a_{m+1}, \dots, a_n$$

eine Basis von V. Wir schreiben jetzt

$$b_m = \sum_{i=1}^{m-1} \eta_i b_i + \sum_{i=m}^{n} \eta_i a_i$$

Da $b_1, \dots, b_{m-1}, b_m$ linear unabhängig ist $\eta_m = \dots = \eta_n = 0$ unmöglich. Daher ist mindestens eins der η_i, $m \le i \le n$ nicht Null. Wenden wir nun Lemma 7.4 an,

und nehmen wir ohne Einschränkung $j = m$ an, so folgt, daß

$$b_1, \dots, b_{m-1}, b_m, a_{m+1}, \dots, a_n \in V$$

eine Basis ist. □

Sei nun V ein Vektorraum und $U, U' \subset V$ Untervektorräume. Dann ist auch $U \cap U' \subset V$ ein Untervektorraum.

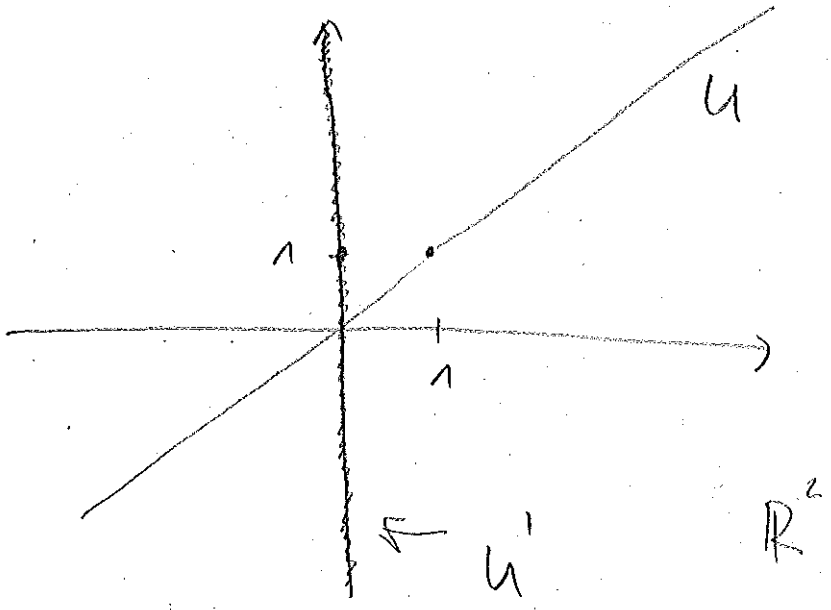
Def 7.21 Sind $U, U' \subset V$ Untervektorräume von V, so heißt

$$U + U' = \{ a + b \mid a \in U, b \in U' \}$$

die Summe von U und U'.

Bsp. 7.22 Sei $V = \mathbb{R}^2$ und $U = \langle a \rangle$ und $U' = \langle b \rangle$ mit $a = (1,1)$ und $b = (0,1)$. Dann gilt

$$U + U' = \mathbb{R}^2.$$

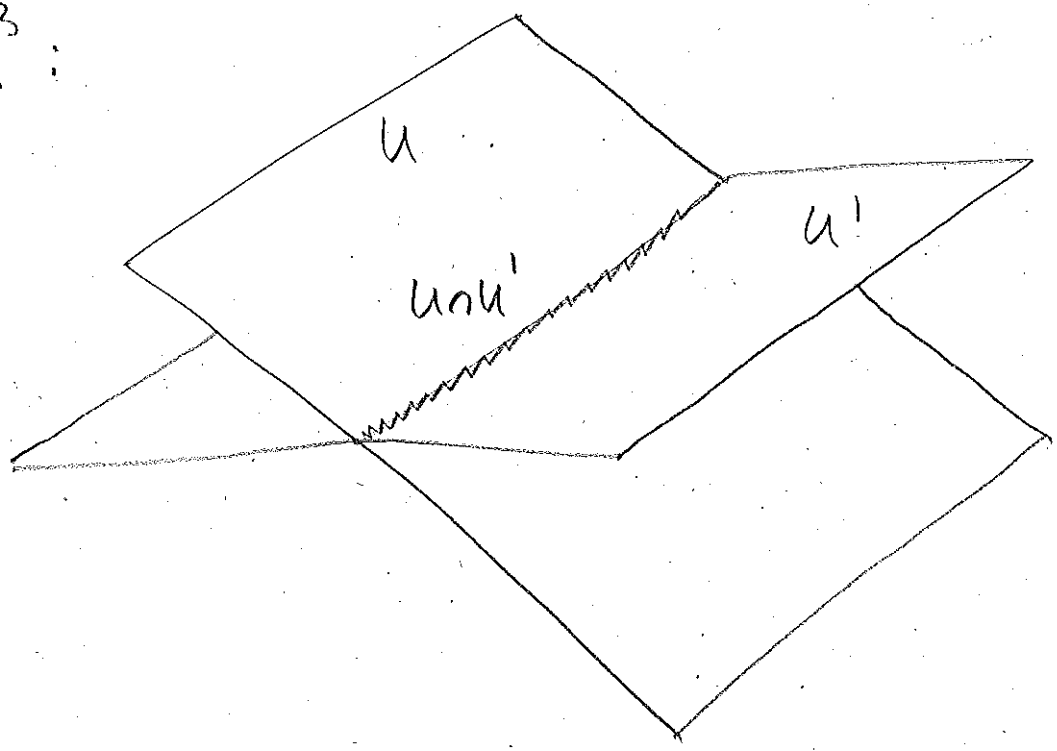


Wir sehen $U \cap U' = \{0\}$. Außerdem ist

$\dim(U) = \dim(U') = 1$ und $\dim(U) + \dim(U') = 2$.

Dies ist jedoch nicht immer der Fall:

$\mathbb{R}^3$:



Hier gilt $\dim(U) = \dim(U') = 2$ und

$\dim(U) + \dim(U') = 4$, obwohl $\dim(\mathbb{R}^3) = 3$.

Anpreaden ist $\dim(U \cap U') = 1$.
Wie können wir diese Verhalten von Untervektorräumen genau verstehen?

Theorem 7.23 Ist V endlich-dimensional, so gilt für Untervektorräume $U, U' \subset V$:

$$\dim(U) + \dim(U') = \dim(U+U') + \dim(U \cap U')$$

Diese Formel heißt Dimensionsformel.

Beweis Nach Propo. 7.14 gilt, $U \cap U'$, U und U' sind endlich-dimensional.
Wir wählen Basis:

$a_1, \dots, a_r \in U \cap U'$, $r = \dim(U \cap U')$
Nach Basisergänzungssatz ergänzen wir zu Basen

$$a_1, \dots, a_r, b_1, \dots, b_s \in U, \quad r+s = \dim(U)$$

$$a_1, \dots, a_r, c_1, \dots, c_t \in U', \quad r+t = \dim(U').$$

Es gilt

$$a_1, \dots, a_r, b_1, \dots, b_s, c_1, \dots, c_t \in U+U'.$$

Wir zeigen nun, daß dies eine Basis von $U+U'$ ist. Dann gilt nämlich:

$$\begin{aligned}\dim(U)+\dim(U') &= (r+s)+(r+t)\\ &= 2r+s+t\\ &= (r+s+t)+r\\ &= \dim(U+U')+\dim(U\cap U').\end{aligned}$$

Dann $\langle a_1,\dots,a_r,b_1,\dots,b_s,c_1,\dots,c_t\rangle = U+U'$ ist klar, da $y\in U$ und $y'\in U'$ jeweils Linearkombination der Vektoren

$$a_1,\dots,a_r,b_1,\dots,b_s,c_1,\dots,c_t \qquad (*)$$

sind. Also auch $y+y'$.

Es bleibt zu zeigen, daß $(*)$ linear unabhängig ist. Sei also für

$$\sum_{i=1}^{r}\lambda_i a_i + \sum_{j=1}^{s}\mu_j b_j + \sum_{\ell=1}^{t}\nu_\ell c_\ell = 0$$

Dann gilt

$$\sum_{i=1}^{r}\lambda_i a_i + \sum_{j=1}^{s}\mu_j b_j = -\sum_{\ell=1}^{t}\nu_\ell c_\ell$$

Wir setzen $x = -\sum_{e=1}^{t} \mu_e c_e$ und sehen

$$\sum_{i=1}^{r} \lambda_i a_i + \sum_{j=1}^{s} \mu_j b_j \in U \quad \text{und}$$

$$-\sum_{e=1}^{t} \mu_e c_e \in U'. \quad \text{Also } x \in U \cap U'. \quad \text{Da}$$

also $x \in U \cap U'$, insbesondere $x \in U$, schreiben wir $x = \sum_{i=1}^{r} \tilde{\lambda}_i a_i$.

Da $a_1, \dots, a_r, b_1, \dots, b_s \in U$ linear unabhängig, gilt $\tilde{\lambda}_i = \lambda_i$ für alle $1 \le i \le r$ und

$\mu_j = 0$ für $1 \le j \le s$. Vertauscht man Rolle von U und U' folgt $\mu_e = 0$ für alle $1 \le e \le t$. Schließlich folgt $\sum_{i=1}^{r} \lambda_i a_i = 0$

und da $a_1, \dots, a_r$ linear unabhängig, ergibt sich $\lambda_i = 0$ für alle $1 \le i \le r$.

□

Korollar 7.24 Sei V ein Vektorraum und $U, U' \subset V$ Untervektorräume. Ist $\dim(U) + \dim(U') = \dim(V)$, dann

$$U + U' = V \iff U \cap U' = \{0\}$$

Beweis Nach Dimensionsformel gilt

$$\dim(V) = \dim(U + U') + \dim(U \cap U').$$

„$\Rightarrow$" Ist $U + U' = V$, so folgt $\dim(U \cap U') = 0$. Korollar 7.17 zeigt $U \cap U' = \{0\}$.

„$\Leftarrow$" Ist $U \cap U' = \{0\}$, so zeigt Korollar 7.17 $\dim(U \cap U') = 0$. Also $\dim(V) = \dim(U + U')$. Propo. 7.16 zeigt $V = U + U'$.

□

Def 7.25 Sei $U = U_1 + U_2$ eine Summe von Untervektorräumen $U_1, U_2 \subset V$. Dann heißt U <u>direkte Summe</u> von U_1 und U_2 falls $U_1 \cap U_2 = \{0\}$. Man schreibt dann $U = U_1 \oplus U_2$.

Bemerkung 7.26 Sei $U = U_1 \oplus U_2 \subset V$. Dann gilt $\dim(U_1 \oplus U_2) = \dim(U_1) + \dim(U_2)$.

Es ist auch möglich direkte Summen von mehr als zwei Untervektorräumen zu bilden.

Propo. 7.27 Eine Summe $U_1 + U_2 \subset V$ ist direkt, genau dann, wenn sich jeder Vektor $v \in U_1 + U_2$ eindeutig als $v = a + b$, $a \in U_1$, $b \in U_2$ schreiben lässt.

Beweis „$\Rightarrow$" $U_1 \oplus U_2 \subset V$. Dann gilt $U_1 \cap U_2 = \{0\}$. Sei $v = a + b$ und $v = a' + b'$ mit $a, a' \in U_1$ und $b, b' \in U_2$. Dann gilt

$a+b = a'+b'$, also $a-a' = b'-b$.

Da $a-a' \in U$ und $b'-b \in U'$, folgt

$a-a' \in U \cap U'$, d.h. $a = a'$. Folgerich $b = b'$.

Also ist $v = a+b$ eindeutig mit $a \in U$, $b \in U'$.

„$\Leftarrow$". Sei $v = a+b$ mit eindeutigen $a \in U$, $b \in U'$.

Sei $x \in U \cap U'$. Dann gilt

$$v = (a+b) + (x-x) = (a+x) + (b-x).$$

Da $a+x \in U$ und $b-x \in U'$ und

$v = a+b$ mit eindeutigen $a \in U$, $b \in U'$,

folgt $a = a+x$ und $b = b-x$. Also

$x = 0$, d.h. $U \cap U' = \{0\}$.

□

<u>Def 7.28</u> Eine Summe

$$\sum_{i=1}^{n} U_i := \{ b_1 + \dots + b_n \mid b_i \in U_i \}$$ von

Untervektorräumen $U_i \subset V$ heißt

<u>direkt</u>, falls sich jedes $b \in \sum_{i=1}^{n} U_i$

eindeutig als $b = b_1 + \dots + b_n$ schreiben

lässt.

Bsp 7.29 $V = K^n = \underbrace{K \oplus K \oplus \cdots \oplus K}_{n\text{-mal}}$.

§ 8
Lineare Abbildungen und Matrizen

Def 8.1 Eine Abbildung $f: V \to W$ zwischen zwei K-Vektorräumen V und W heißt <u>linear</u>, wenn gilt

(i) $f(a+b) = f(a) + f(b)$

(ii) $f(\lambda \cdot a) = \lambda \cdot f(a)$

für alle $a, b \in V$ und $\lambda \in K$.

Bsp 8.2 Sei
$$\begin{aligned} aX + bY &= 0 \\ cX + dY &= 0 \end{aligned}$$
ein LGS über dem Körper K, d.h. $a,b,c,d \in K$. Wir sahen in Bsp 5.3., daß der Lösungsraum $L \subset K^2$ ein Untervektorraum ist.

Betrachten wir die Abb.

$$f: L \to K^2, \quad (\lambda, \mu) \mapsto \begin{pmatrix} a\lambda + b\mu \\ c\lambda + d\mu \end{pmatrix}.$$

Dann gilt für $v=(\lambda,\mu)$, $w=(\lambda',\mu')$ und $r \in K$:

$$f(v+w) = \begin{pmatrix} a(\lambda+\lambda') + b(\mu+\mu') \\ c(\lambda+\lambda') + d(\mu+\mu') \end{pmatrix} = 0$$

$$= \begin{pmatrix} a\lambda + a\lambda' + b\mu + b\mu' \\ c\lambda + c\lambda' + d\mu + d\mu' \end{pmatrix} = 0$$

$$= f(v) + f(w)$$

$$f(r \cdot v) = \begin{pmatrix} a(r\lambda) + b(r\mu) \\ c(r\lambda) + d(r\mu) \end{pmatrix} = 0$$

$$= r \cdot f(v)$$

Bsp 8.3 Nullabbildung $V \to W$, $a \mapsto 0$ ist linear.

Die Identität $id_V : V \to V$, $a \mapsto a$ ist linear.

Die Inklusionsabb $i: U \to V$, $a \mapsto a$ für Unterverktorraum $U \subset V$ ist linear.

Bsp 8.4 $f: \mathbb{R} \to \mathbb{R}$, $a \mapsto a+3$ ist nicht linear. Es gilt:

$f(1+2) = f(3) = 6$, aber

$f(1) = 4$ und $f(2) = 5$, also

$f(1+2) \neq f(1) + f(2)$.

Propo 8.5 Sei $\alpha \in K$. Dann ist

$f: K \to K$, $a \mapsto \alpha a$

linear. Umgekehrt ist jede lineare Abb $g: K \to K$ von der Form $a \mapsto \alpha a$ mit $\alpha = g(1)$.

Beweis Es gilt $f(a+b) = \alpha(a+b) = \alpha a + \alpha b$

$= f(a) + f(b)$

und $f(\lambda \cdot a) = \alpha \cdot (\lambda \cdot a) = \alpha \cdot \lambda \cdot a$

$= \lambda \cdot \alpha \cdot a$

$= \lambda \cdot f(a)$

Sei nun $g: K \to K$ linear. Dann ist $g(a) = g(a \cdot 1) = a \cdot g(1) = \alpha \cdot a$

Lineare Abb. haben folgende Eigenschaften:

Propo 8.6 Es sei $f: V \to W$ eine lineare Abb. Dann gilt:

(i) $f(0) = 0$

(ii) $f(-a) = -f(a)$

(iii) $f\left(\sum_{i \in I} \lambda_i a_i\right) = \sum_{i \in I} \lambda_i f(a_i)$

Beweis

(i) Es gilt $f(0_V) = f(0_K \cdot 0_V) = 0_K \cdot f(0_V)$
$= 0_W$

(ii) Sei $\lambda = -1$. Dann gilt
$f(-a) = f(\lambda \cdot a) = \lambda \cdot f(a) = -1 \cdot f(a)$
$= -f(a)$

(iii) In Linearkombinationen $\sum_{i \in I} \lambda_i a_i$
verschwinden fast alle λ_i. Man hat also nur endlich viele λ_i, $i \in I$, die ungleich Null sind. Ohne Einschränkg

sei $I = \{1, \dots, n\}$. Dann folgt die Behauptung per Induktion nach $n \geq 0$. ⊡

Def 8.7 Seien V und W, K-Vektorräume. Dann nennt man den K-Vektorraum

$$\mathrm{Hom}_K(V,W) = \{f : V \to W \mid f \text{ linear}\}$$

den Hom-Raum. Die Verknüpfungen sind gegeben durch

$$(f+g)(a) = f(a) + g(a)$$
$$(\lambda \cdot f)(a) = \lambda \cdot f(a).$$

Propo 8.8 Ist $f : V \to W$ eine bijektive Abb. Dann ist $f^{-1} : W \to V$ ebenfalls linear.

Beweis Wir müssen zeigen:

$$f^{-1}(a+b) = f^{-1}(a) + f^{-1}(b)$$

$f^{-1}(\lambda \cdot a) = \lambda \cdot f^{-1}(a)$.

Es gilt:

$f(f^{-1}(a+b)) = a+b$ und

$f(f^{-1}(a) + f^{-1}(b)) = a+b$.

Da f bijektiv, folgt $f^{-1}(a+b) = f^{-1}(a) + f^{-1}(b)$.

Analog zeigt man $f^{-1}(\lambda \cdot a) = \lambda \cdot f^{-1}(a)$. ⊡

Bemerkung 8.9 Bijektive lineare Abb $f: V \to W$ heißen Isomorphismen.

In diesem Fall sind V und W strukturell „gleich", obwohl V und W sehr unterschiedliche Vektorräume sein können.

Existiert ein Isomorphismus $f: V \to W$, so nennt man V und W isomorph.

Lineare Abb. können auf besonders einfache Weise hingeschrieben werden.

Propo 8.10 Seien V und W zwei K-Vektorräume und $a_i \in V$, $i \in I$ eine Basis. Zu jeder Familie $b_i \in W$, $i \in I$ gibt es genau eine lineare Abb $f: V \to W$ mit $f(a_i) = b_i$ für alle $i \in I$.

Beweis Seien $f, g: V \to W$ zwei solche linearen Abb. Schreiben wir $x = \sum_{i \in I} \lambda_i a_i \in V$ als Linear-kombination, so gilt mit Propo. 8.6

$$f(x) = \sum_{i \in I} \lambda_i f(a_i) = \sum_{i \in I} \lambda_i b_i$$

$$= \sum_{i \in I} \lambda_i g(a_i)$$

$$= g(x).$$

Also sind f und g gleich.

Wenn man also zwei solche linearen Abb hat, so sind sie gleich. Wir zeigen nun, daß es eine solche Abb. gibt.

Wir definieren zunächst eine Abb:

$$f: V \to W, \quad x \mapsto \sum_{i \in I} \lambda_i b_i$$

wobei $x = \sum_{i \in I} \lambda_i a_i$.

Wir zeigen, daß f linear ist. Für $x = a_i$ gilt dann $f(a_i) = b_i$.

Also, seien $x, x' \in V$ mit

$$x = \sum_{i \in I} \lambda_i a_i \quad \text{und} \quad x' = \sum_{i \in I} \lambda_i' a_i .$$

Dann gilt

$$f(x+x') = f\Big(\sum_{i \in I} (\lambda_i + \lambda_i') a_i\Big) = \sum_{i \in I} (\lambda_i + \lambda_i') b_i$$

$$= \sum_{i \in I} \lambda_i b_i + \sum_{i \in I} \lambda_i' b_i$$

$$= f(x) + f(x').$$

Analog zeigt man $f(\lambda x) = \lambda f(x)$.

Bemerkung 8.11 Proposition 8.10 zeigt, daß eine lineare Abb $f: V \to W$ schon dadurch festgelegt ist, wohin man die Basisvektoren $a_i \in V$, $i \in I$ abbildet.

Wir betrachten nun folgende Situation:
Seien $a_1, \dots, a_n \in V$ und $b_1, \dots, b_m \in W$ Basen und $f: V \to W$ eine lineare Abb. Schreiben wir

$$f(a_j) = \sum_{i=1}^{m} \alpha_{ij} b_i \quad , \quad 1 \le j \le n \, ,$$

so sind die Koeffizienten α_{ij} eindeutig bestimmt. Wir schreiben α_{ij}, $1 \le i \le m$, $1 \le j \le n$ als rechteckiges Schema

$$\begin{pmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ \alpha_{21} & \cdots & \cdots & \alpha_{2n} \\ \vdots & & & \\ \alpha_{m1} & \cdots & \cdots & \alpha_{mn} \end{pmatrix}$$

oder (α_{ij}) $1 \leq i \leq m$, $1 \leq j \leq n$ als Kurzschreibweise. Man nennt (α_{ij}) die Matrix der Abb. f bezüglich der Basen a_i und b_j.

Def 8.12 Eine $(m \times n)$-Matrix mit Einträgen in einem Körper K ist eine Abb

$$\alpha : \{1, \ldots, m\} \times \{1, \ldots, n\} \longrightarrow K .$$

Man notiert

$$\alpha = (\alpha_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} = \begin{pmatrix} \alpha_{11} & \cdots & \alpha_{1n} \\ \vdots & & \\ \alpha_{m1} & \cdots & \alpha_{mn} \end{pmatrix}$$

Bsp 8.13 Sei $V = W = K^2$ und $f : K^2 \to K^2$ folgende lineare Abb. $(a,b) \mapsto (3a, a+b)$.

Wählen wir $e_1, e_2 \in K^2$ als Basis, so erhalten wir:

$$f(e_1) = f(1,0) = (3,1) = 3 \cdot e_1 + 1 \cdot e_2$$

$$f(e_2) = f(0,1) = (0,1) = 0 \cdot e_1 + 1 \cdot e_2$$

Dann ist $A = \begin{pmatrix} 3 & 0 \\ 1 & 1 \end{pmatrix}$.

Wir machen nun folgende Beobachtung:

Lemma 8.14 Sei $f: V \to W$ eine lineare Abb. und $a_1, \dots, a_n \in V$, deren Bilder $f(a_1), \dots, f(a_n)$ linear unabhängig sind. Dann sind auch $a_1, \dots, a_n \in V$ linear unabhängig.

Beweis Wir zeigen, daß $a_1, \dots, a_n \in V$ linear unabhängig sind.
Angenommen $a_1, \dots, a_n \in V$ sind linear abhängig. Dann existiert ein $\lambda_i \in K$, $i \in \{1, \dots, n\}$, so daß

$\lambda_i \neq 0$ und $\lambda_1 a_1 + \dots + \lambda_{i-1} a_{i-1} + \lambda_i a_i + \dots + \lambda_n a_n = 0$

Dann gilt:

$$f(\lambda_1 a_1 + \dots + \lambda_{i-1} a_i + \lambda_i a_i + \lambda_{i+1} a_{i+1} + \dots + \lambda_n a_n) =$$

$$f(0) = 0$$

$$= \lambda_1 f(a_1) + \dots + \lambda_i f(a_i) + \dots + \lambda_n f(a_n)$$

Da jedoch $f(a_1), \dots, f(a_n)$ linear unabhängig, folgt $\lambda_i = 0$ für alle $i \in \{1, \dots, n\}$.

Dies ist ein Widerspruch. ☒

Frage: Wann gilt die Umkehrung von Lemma 8.14?

Def. 8.15 Sei $f: V \to W$ eine lineare Abb.

Man nennt

$$\ker(f) = f^{-1}(\{0\}) = \{a \in V \mid f(a) = 0\}$$

den Kern von f und

$$\operatorname{Im}(f) = f(V) = \{f(a) \mid a \in V\}$$

das Bild von f.

Man rechnet leicht nach, daß

$\ker(f) \subset V$ und $\operatorname{Im}(f) \subset W$

Untervektorräume sind.

Lemma 8.16 Eine lineare Abb. $f: V \to W$ ist injektiv genau dann, wenn $\ker(f) = \{0\}$.

Beweis „$\Rightarrow$" klar, folgt aus Propo. 8.6 (i) und Definition der Injektivität.

„$\Leftarrow$" Sei $\ker(f) = \{0\}$. Nehmen wir $a, a' \in V$ mit $f(a) = f(a')$, so folgt $f(a) - f(a') = 0$.

Nun ist $f(a) - f(a') = f(a - a') = 0$

und da $\ker f = \{0\}$, erhalten wir $a - a' = 0$. Also $a = a'$.

□

Wir können nun obige Frage beantworten.

Propo 8.17 Sei $f: V \to W$ linear injektiv und $a_1, \dots, a_n \in V$. Dann sind $a_1, \dots, a_n \in V$ linear unabhängig genau dann, wenn $f(a_1), \dots, f(a_n)$ linear unabhängig.

Beweis „$\Leftarrow$" Ist gerade Lemma 8.14.

„$\Rightarrow$" Zu zeigen ist, $f(a_1), \dots, f(a_n)$ sind linear unabhängig.

Sei dazu

$$\lambda_1 f(a_1) + \dots + \lambda_n f(a_n) = 0.$$

Wegen Linearität gilt

$$f(\lambda_1 a_1 + \dots + \lambda_n a_n) = 0.$$

Da $\ker(f) = \{0\}$, gilt

$$\lambda_1 a_1 + \dots + \lambda_n a_n = 0.$$

Da $a_1, \dots, a_n$ linear unabhängig, erhalten wir $\lambda_i = 0$ für alle

$1 \in I \in \mathcal{U}$.

Propo 8.18 Seien V und W zwei K-Vektorräume. Es gilt

(i) Sei $f: V \to W$ ein Isomorphismus, so folgt $\dim(V) = \dim(W)$

(ii) Falls $\dim(V) = \dim(W) < \infty$, so existiert ein Isomorphismus $f: V \to W$.

Beweis

(i) Ist $\dim(V) = \infty$, so folgt mit Korollar 7.12, daß es eine Folge $a_1, a_2, \ldots, \in V$ linear unabhängige Vektoren gibt. Aus Propo. 8.17 folgt, daß $f(a_1), f(a_2), \ldots, \in W$ eine Folge linear unabhängiger Vektoren aus W. Also $\dim(W) = \infty$.

Sei nun $\dim(V) = n < \infty$ und $a_1, \dots, a_n \in V$ Basis. Dann sind $f(a_1), \dots, f(a_n)$ linear unabhängig nach Propo. 8.17. Also $\dim(W) \geq n$.

Sei $y \in W$ und x das Urbild, d.h. $f(x) = y$ (existiert, da f surjektiv).

Schreibe $x = \lambda_1 a_1 + \dots + \lambda_n a_n$ als Linearkombination. Dann gilt $f(x) = y = \lambda_1 f(a_1) + \dots + \lambda_n f(a_n)$. Also gilt

$$\langle f(a_1), \dots, f(a_n) \rangle = W.$$

Folgerich $\dim(W) = n$.

(ii) Sei nun $\dim(V) = \dim(W) = n < \infty$.
Wählen Basen $a_1, \dots, a_n \in V$ und $b_1, \dots, b_n \in W$.
Laut Propo 8.10 ex. lineare Abb.
$f: V \to W$ mit $f(a_i) = b_i$.
Zu zeigen bleibt, f ist bijektiv.

Injektivität: Sei $x \in \ker(f)$.

Schreibe $x = \lambda_1 a_1 + \dots + \lambda_n a_n$. Dann gilt

$$f(x) = \lambda_1 f(a_1) + \dots + \lambda_n f(a_n) =$$

$$= \lambda_1 b_1 + \dots + \lambda_n b_n = 0$$

Da $b_1, \dots, b_n$ Basis, folgt $\lambda_i = 0$ für alle $1 \le i \le n$. Also $x = 0$, d.h. $\ker(f) = \{0\}$.

Surjektivität folgt man wie in (i). □

Korollar 8.19 Ist V ein K-Vektorraum mit $\dim(V) = n < \infty$. Dann existiert ein Isomorphismus $f: V \to K^n$

Bemerkung 8.20 Korollar 8.19 bedeutet, daß es bis auf Isomorphie als endlich-dimensionale K-VR nur die K^n gibt.

Zwischen Kern und Bild einer linearen Abb $f: V \to W$ besteht ein wichtiger Zusammenhang.

Theorem 8.21 Sei $f: V \to W$ lineare Abb. zwischen endlich-dimensionalen Vektorräumen. Dann gilt

$$\dim(V) = \dim \ker(f) + \dim \operatorname{Im}(f).$$

Beweis Sei $s = \dim \ker(f)$ und $r = \dim \operatorname{Im}(f)$. Wählen Basen $a_1, \dots, a_s \in \ker(f)$ und $b_1, \dots, b_r \in \operatorname{Im}(f)$. Seien $a_{s+i} \in V$ die Urbilder von b_i, $1 \le i \le r$. Wir zeigen nun, daß

$$a_1, \dots, a_s, a_{s+1}, \dots, a_{s+r} \in V$$

eine Basis bilden.

Wir zeigen zunächst

$$\langle a_1, \dots, a_s, a_{s+1}, \dots, a_{s+r} \rangle = V.$$

Sei $x \in V$ und schreibe

$f(x) = \sum_{i=1}^{r} \mu_i b_i$. Wir bilden

$x' = \sum_{i=1}^{r} \mu_i a_{s+i} \in V$. Dann gilt

$$f(x') = \sum_{i=1}^{r} \mu_i f(a_{s+i}) = \sum_{i=1}^{r} \mu_i b_i = f(x).$$

Also folgt $x - x' \in \ker(f)$. Dann gilt

$$x - x' = \eta_1 a_1 + \dots + \eta_s a_s.$$

Dann folgt

$$x = (x - x') + x' = \sum_{j=1}^{s} \eta_j a_j + \sum_{i=1}^{r} \mu_i a_{s+i}.$$

Also $\langle a_1, \dots, a_s, a_{s+1}, \dots, a_{s+r} \rangle = V$.

Nun zeigen wir, daß die Vektoren

$a_1, \dots, a_s, a_{s+1}, \dots, a_{s+r}$ linear unabhängig

sind. Sei dann

$$\lambda_1 a_1 + \dots + \lambda_s a_s + \lambda_{s+1} a_{s+1} + \dots + \lambda_{s+r} a_{s+r} = 0.$$

Anwendung von f ergibt

$$0 = \lambda_1 f(a_1) + \dots + \lambda_s f(a_s) + \lambda_{s+1} f(a_{s+1}) + \dots + \lambda_{s+r} f(a_{s+r}).$$

$$= \lambda_{s+1} f(a_{s+1}) + \dots + \lambda_{s+r} f(a_{s+r})$$

$$= \lambda_{s+1} b_1 + \dots + \lambda_{s+r} b_r.$$

Da $b_1, \dots, b_r \in \operatorname{Im}(f)$ linear unabhängig, folgt $\lambda_{s+1} = \dots = \lambda_{s+r} = 0$. Also gilt

$0 = \lambda_1 a_1 + \dots + \lambda_s a_s$ und da $a_1, \dots, a_s \in \ker(f)$ linear unabhängig folgt $\lambda_1 = \lambda_2 = \dots = \lambda_s = 0$.

□

Wir schreiben

$$\mathrm{Mat}_{m\times n}(K) = \left\{ (\alpha_{ij})_{\substack{1\le i\le m \\ 1\le j\le n}} \mid \alpha_{ij} \in K \right\}$$

als die Menge aller $(m\times n)$-Matrizen.

Man nennt i den Zeilenindex und j den Spaltenindex der Matrix (α_{ij}).

Für eine Matrix (α_{ij}) schreibt man kurz $A \in \mathrm{Mat}_{m\times n}(K)$. Es sei nun $f: V \to W$ eine lineare Abb und $a_1, \dots, a_n \in V$ und $b_1, \dots, b_m \in W$ Basen und $A = (\alpha_{ij})$ die Matrix der Abb. f. Dann erhalten wir Abb.

$$(*) \qquad \mathrm{Hom}(V,W) \longrightarrow \mathrm{Mat}_{m\times n}(K),$$
$$f \longmapsto (\alpha_{ij}) = A.$$

Propo 8.22 Die obige Abb. (*) ist ein Isomorphismus von Vektorräumen.

Beweis Die Abb.

$$\mathrm{Hom}(V,W) \longrightarrow \mathrm{Mat}_{m\times n}(K)$$
$$f \longmapsto (\alpha_{ij}) = A$$

ist injektiv nach Propo. 8.10 und Definition von Basis.

Sei nun $(\beta_{ij}) = B \in \mathrm{Mat}_{m\times n}(K)$.

Definiere

$$f(a_j) = \sum_{i=1}^{m} \beta_{ij} \cdot b_i \quad , \quad 1 \le j \le n.$$

Nach Propo. 8.10 erhält man so eine Abb. $f: V \to W$.

Zu klären ist noch die Vektorraumstruktur auf $\mathrm{Mat}_{m\times n}(K)$.

Durch

$$(\alpha_{ij}) + (\beta_{ij}) = (\alpha_{ij} + \beta_{ij}) \quad \text{und}$$

$$\lambda \cdot (\alpha_{ij}) = (\lambda \cdot \alpha_{ij}) \quad \text{wird}$$

$\mathrm{Mat}_{m\times n}(K)$ ist ein K-Vektorraum.

Die Abb $f \mapsto (\alpha_{ij})$ ist linear, da

$$(f+f')(a_j) = f(a_j) + f'(a_j) =$$

$$= \left(\sum \alpha_{ij} b_i\right) + \left(\sum \alpha'_{ij} b_i\right)$$

$$= \sum (\alpha_{ij} + \alpha'_{ij})\, b_i$$

$$(\lambda \cdot f)(a_j) = \lambda \cdot f(a_j) = \lambda \left(\sum \alpha_{ij} b_i\right)$$

$$= \sum (\lambda \cdot \alpha_{ij})\, b_i$$

□

Sei nun $V = K^n$ und $W = K^m$. Dann hat man eine kanonische Wahl für Basen $a_j = e_j \in K^n$, $1 \le j \le n$ und $b_i = e_i \in K^m$, $1 \le i \le m$. Erhalten so

$$\mathrm{Hom}(K^n, K^m) = \mathrm{Mat}_{m\times n}(K),$$

da die linearen Abb $f: K^n \to K^m$

„sind" die Matrizen. Das schreiben wir genauer.

Sei $x = \lambda_1 a_1 + \dots + \lambda_n a_n = (\lambda_1, \dots, \lambda_n) \in K^n$.

Dann gilt

$$\begin{aligned} f(x) &= \lambda_1 f(a_1) + \dots + \lambda_n f(a_n) \\ &= \sum_{j=1}^{n} \lambda_j \left(\sum_{i=1}^{m} \alpha_{ij} b_i \right) \\ &= \sum_{i=1}^{m} \left(\sum_{j=1}^{n} \alpha_{ij} \lambda_j \right) b_i \\ &= \left(\dots, \sum_{j=1}^{n} \alpha_{ij} \lambda_j, \dots \right) \end{aligned}$$

$\uparrow$ i-te Stelle

Nehmen wir jetzt $(\alpha_{ij}) = A \in \mathrm{Mat}_{m \times n}(K)$, dann kann man folgendes definieren

$$\begin{pmatrix} \alpha_{11} & \dots & \alpha_{1n} \\ \vdots & & \vdots \\ \alpha_{i1} & \dots & \alpha_{in} \\ \vdots & & \vdots \\ \alpha_{m1} & \dots & \alpha_{mn} \end{pmatrix} \cdot \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = \begin{pmatrix} \vdots \\ \sum_{j=1}^{n} \alpha_{ij} \lambda_j \\ \vdots \end{pmatrix} = f(x)$$

Auf diese Art und Weise ist

$f(x) = A \cdot x$ und $A : K^n \to K^m$ linear.

Bsp. 8.22 Sei $\sum_{j=1}^{n} \alpha_{ij} x_j = 0$, $1 \le i \le m$

ein LGS.

Wir können das Gleichungssystem jetzt schreiben als

$$\begin{pmatrix} \alpha_{11} & \cdots & \alpha_{1n} \\ \vdots & & \vdots \\ \alpha_{m1} & \cdots & \alpha_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Mit $(\alpha_{ij}) = A$ und $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$

ist $A \cdot X = 0$.

Der Lösungsraum L ist also der Kern der linearen Abb $A : K^n \to K^m$. Also $L = \ker(A)$.

Wir betrachten jetzt folgende Situation:

Seien $g: U \to V$ und $f: V \to W$ lineare Abb. und $a_1, \dots, a_r \in U$, $b_1, \dots, b_n \in V$ und $c_1, \dots, c_m \in W$ Basen.

Durch $g(a_k) = \sum_{j=1}^{n} \mu_{jk} b_j$ und $f(b_j) = \sum_{i=1}^{m} \lambda_{ij} c_i$ erhalten wir Matrizen

$$A = (\lambda_{ij})_{\substack{1 \le i \le m \\ 1 \le j \le n}} \quad \text{und} \quad B = (\mu_{jk})_{\substack{1 \le j \le n \\ 1 \le k \le r}}$$

Nun berechnen wir die Matrix von $f \circ g$:

$$f(g(a_k)) = \sum_{j=1}^{n} \mu_{jk} f(b_j) = \sum_{j=1}^{n} \sum_{i=1}^{m} \mu_{jk} \lambda_{ij} c_i .$$

An jeder i ist der Koeffizient bei c_i also

$$\sum_{j=1}^{n} \lambda_{ij} \mu_{jk} \in K$$

Wir erhalten für $f \circ g$ also die Matrix

$$\left(\sum_{j=1}^{u} a_{ij} b_{jk} \right)_{\substack{1 \le i \le m \\ 1 \le k \le r}}$$

Auf diese Weise definieren wir die Matrixmultiplikation:

$$\underset{m \times u}{\mathrm{Mat}}(K) \times \underset{u \times r}{\mathrm{Mat}}(K) \longrightarrow \underset{m \times r}{\mathrm{Mat}}(K)$$

gleich

$$(a_{ij}) \cdot (b_{jk}) = \left(\sum_{j=1}^{u} a_{ij} b_{jk} \right)$$

Bsp 8.23 $m = u = r = 2$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}$$

oder für $m = 1$, $u = 3$, $r = 2$

$$(a, b, c) \begin{pmatrix} u & v \\ w & x \\ y & z \end{pmatrix} = \begin{pmatrix} au+bw+cy \\ av+bx+cz \end{pmatrix}$$

Propo 8.24 Für $A \in \mathrm{Mat}_{m \times u}(K)$, $B \in \mathrm{Mat}_{u \times r}(K)$ und $C \in \mathrm{Mat}_{r \times s}(K)$ gilt

$$(A \cdot B) \cdot C = A \cdot (B \cdot C) \in \mathrm{Mat}_{m \times s}(K)$$

Beweis Kann man direkt nachrechnen.

Alternativ:

Seien $f: K^u \to K^m$, $g: K^r \to K^u$ und $h: K^s \to K^r$ die linearen Abb zu A, B und C. Dann gilt offenbar

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

□

Propo 8.25 Der Vektorraum $\mathrm{Mat}_n(K)$ wird mit Matrixmultiplikation zu einem assoziativen Ring.

Beweis Man rechnet nach, daß

$$A(B+B') = A \cdot B + A \cdot B' \quad \text{und}$$

$$(A+A') \cdot B = AB + A'B'.$$

Nullelement ist die Nullmatrix

$$0 = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix} \quad \text{und Einselement}$$

$$E = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix} \quad \text{ist die}$$

Einheitsmatrix.

Betrachten wir die Matrizen

$$B_{rs} = \left(\begin{array}{ccc} & \vdots & \\ \cdots & 1 & \cdots \\ & \vdots & \end{array} \right) \leftarrow r\text{-te Zeile} \in \mathrm{Mat}_{m\times n}(K)$$

$\uparrow$ s-te Spalte

so bilden die B_{rs}, $1 \le r \le m$, $1 \le s \le n$ eine Basis des Vektorraums $\mathrm{Mat}_{m\times n}(K)$.

Es gilt also $\dim\left(\mathrm{Mat}_{m\times n}(K)\right) = m \cdot n$.

Propo 8.26 Es seien V und W zwei K-Vektorräume mit $\dim(V) = n$ und $\dim(W) = m$. Dann gilt $\dim\left(\mathrm{Hom}(V,W)\right) = m \cdot n$.

Beweis Folgt aus Propo. 8.21, Propo. 8.17 und aus $\dim\left(\mathrm{Mat}_{m\times n}(K)\right) = m \cdot n$

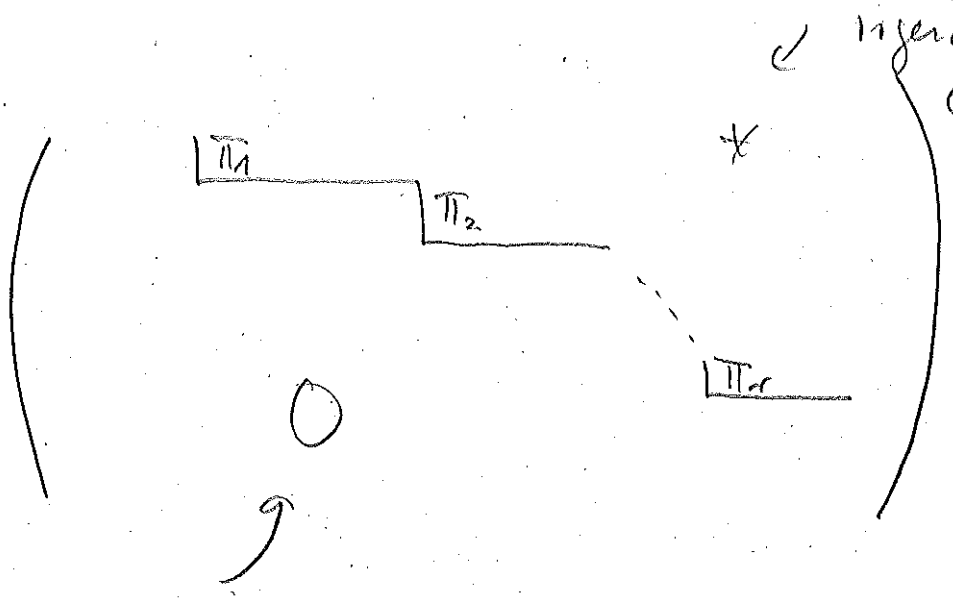
§ 9
Rangs-Algorithmus

Def 9.1 Sei $f: V \to W$ eine lineare Abb. Man definiert den Rang von f als $\operatorname{rank}(f) = \dim \operatorname{Im}(f)$.

Für eine Matrix $A = (a_{ij}) \in \operatorname{Mat}_{m\times n}(K)$ als lineare Abb $A: K^n \to K^m$, $x \mapsto A \cdot x$ schreiben wir $\operatorname{rank}(A)$.

Der Rangs-Algorithmus wandelt eine Matrix A in eine Matrix B um, so daß $\operatorname{rank}(A) = \operatorname{rank}(B)$ und $\operatorname{Ke}(A) = \operatorname{Ke}(B)$.

Def 9.2 Sei K ein Körper. Eine Matrix $B = (b_{ij}) \in \operatorname{Mat}_{m\times n}(K)$ hat Zeilenstufenform (ZSF), wenn sie folgende Gestalt hat



Hierbei sind $\Pi_1, \dots, \Pi_r \in K \setminus \{0\}$ und

$0 \leq r \leq \min\{m, n\}$.

Bsp 9.3 In Zeilenstufenform sind

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} 0 & 1 & 2 \\ 0 & 0 & 3 \\ 0 & 0 & 0 \end{pmatrix}$$

nicht jedoch

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

Die $\pi_1, \dots, \pi_r \in K \setminus \{0\}$ nennt man Pivotelemente und die entsprechenden Spalten Pivotspalten. Schreibt man $\pi_i = \beta_{i,j_i}$ mit $1 \le i \le r$, so nennt man $j_1, \dots, j_r$ die Pivotindizes.

Sei nun $A = (\alpha_{ij}) \in \mathrm{Mat}_{m \times n}(K)$ und fassen wir A vermöge $A: K^n \to K^m$, $x \mapsto A \cdot x$ als lineare Abb. auf, so wird $\mathrm{Im}(A) \subset K^m$ von den Bildern der Vektoren $e_j = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \in K^n$, $1 \le j \le n$ erzeugt. Diese sind

$$A e_j = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} \alpha_{1j} \\ \vdots \\ \alpha_{mj} \end{pmatrix},$$

also die j-te Spalte von A.

Sind also $b_1, \dots, b_n \in K^4$ die Spalten der Matrix A, so gilt

$$\operatorname{rank}(A) = \dim_K \langle b_1, \dots, b_n \rangle .$$

Propo 9.4 Sei $B = (\beta_{ij}) \in \operatorname{Mat}_{m \times n}(K)$ in Zeilenstufenform mit Spalten $b_1, \dots, b_n$ und mit Pivotelementen

$$\pi_1 = \beta_{1,j_1}, \ \pi_2 = \beta_{2,j_2}, \dots, \ \pi_r = \beta_{r,j_r}.$$

Sei $P = \{j_1, \dots, j_r\}$ die Menge der Pivotindizes und $J = \{1, \dots, n\}$.

Dann gilt $\operatorname{rank}(B) = r$.

Beweis Es ist $\operatorname{Im}(B) = \langle b_1, \dots, b_n \rangle$.

Sei

$$P' = \{ 1 \le s \le n \mid b_s \notin \langle b_1, \dots, b_{s-1} \rangle \}$$

Dann bilden nach Lemma 6.10 die b_s, $s \in P'$ eine Basis von $\operatorname{Im}(B)$.

Wir zeigen $P = P'$.

Zunächst zeigen wir $P \subset P'$.

Sei $b_s \in K^m$ eine Pivotspalte mit Pivotelement $\pi_s \neq 0$, d.h.

$$B = \begin{pmatrix} & & & | & * \\ & & & | & \\ 0 & \cdots & 0 & \pi_s & \\ & & & | & \ddots \\ & & & | & \end{pmatrix}$$

$b_1 \; \cdots \; b_{s-1}$

offensichtlich gelt $b_s \notin \langle b_1, \ldots, b_{s-1} \rangle$. Also $s \in P'$.

Nun zeigen wir $P' \subset P$.

Sei dann $b_j \in K^m$ keine Pivotspalte, d.h.

$$B = \begin{pmatrix} \pi_1 & & & h_1 & \\ & \ddots & & | & \\ & & \pi_{s'} & h_s & \\ & & & 0 & \\ & & & | & \\ & & & 0 & \end{pmatrix}$$

Spalte b_j

Schreiben

$$b_j = \begin{pmatrix} * \\ \vdots \\ * \\ 0 \\ \vdots \\ 0 \end{pmatrix} \in K^s \times 0^{n-s} \subset K^n$$

Links neben b_j stehen genau s Pivotspalten. Diese sind linear unabhängig wegen $P \subset P'$, und erzeugen deshalb einen s-dimensionalen Untervektorraum $U \subset K^s \times 0^{n-s}$. Da $\dim(K^s \times 0^{n-s}) = s$, folgt $U = K^s \times 0^{n-s}$.

Insbesondere $b_j \in \langle b_{j_1}, \dots, b_{j_s} \rangle$, wobei $j_1, \dots, j_s$ die Pivotindizes $\leq j$. □

Korollar 9.5 Alles wie in Propo. 9.4. Dann gilt

$$\dim \ker(B) = n - r,$$

die Anzahl der Nicht-Pivotspalten.

Ist eine Matrix $B = (b_{ij})$ in ZSF, kann man leicht $\ker(B)$ bestimmen.

Betrachten wir also LGS

$$\begin{aligned} \pi_1 x_{j_1} + \dots &= 0 \\ \pi_2 x_{j_2} + \dots &= 0 \\ &\ddots \\ \pi_r x_{j_r} + \dots &= 0 \end{aligned} \qquad (*)$$

Offenbar kann man die Nicht-Pivot-variablen x_j, $j \in J \setminus P$ beliebig wählen, die Pivotvariablen $x_{j_1}, \dots, x_{j_r}$ sind dann eindeutig festgelegt durch:

$$x_{j_r} = -\frac{1}{\pi_r} \sum_{j > j_r} \beta_{rj} x_j$$

$$\vdots$$

$$x_{j_1} = -\frac{1}{\pi_1} \sum_{j > j_1} \beta_{1j} x_j \qquad (**)$$

Das zeigt:

Propo 3.6 Sei $B = (\beta_{ij}) \in \mathrm{Mat}_{m \times n}(K)$ in ZSF wie in Propo. 3.4.

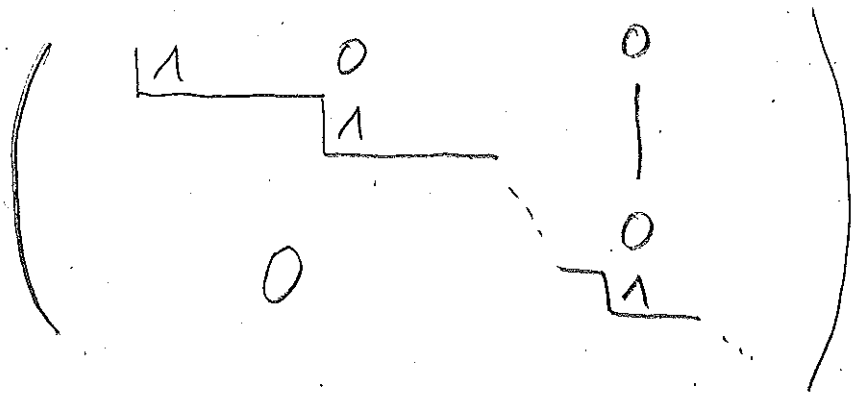
Dann gilt:

$$\mathrm{Ke}(B) = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in K^n \;\middle|\; \begin{array}{l} x_j \in K \text{ bel. für } j \in J \setminus P, \\ x_{j_i} = -\frac{1}{\pi_i} \sum_{j > j_i} \beta_{ij} x_j, \; i = r, \ldots, 1 \end{array} \right\}$$

Man kann mit Hilfe von Propo. 3.6 eine Basis von $\mathrm{Ke}(B)$ leicht angeben.

Besonders einfach wird es, wenn

$B = (\beta_{ij})$ in reduzierter ZSF ist.



da die Pivotelemente $\pi_1 = \dots = \pi_r = 1$ und die Einträge oberhalb der Pivotelemente verschwinden. Dann gilt:

$$x_{j_r} = - \sum_{\substack{j > j_r \\ j \notin P}} \beta_{rj} x_j$$

$$\vdots$$

$$x_{j_1} = - \sum_{\substack{j > j_1 \\ j \notin P}} \beta_{1j} x_j$$

Bsp 9.7 Sei $B = \begin{pmatrix} 1 & 2 & 0 & 3 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 \end{pmatrix}$, dann

$\pi_1 = 1$, $\pi_2 = 1$. Wir schauen uns

$B \cdot x = 0$, mit $x = \begin{pmatrix} x_1 \\ \vdots \\ x_4 \end{pmatrix}$ an.

Dann gilt:

$$\begin{aligned} x_1 + 2x_2 \quad + 3x_4 &= 0 \\ x_3 + 2x_4 &= 0 \end{aligned}$$

Pivotvariablen sind x_3 und x_1.

Proposition 9.6 zeigt

$$\mathrm{Ker}(B) = \left\{ \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \lambda_3 \\ \lambda_4 \end{pmatrix} \in K^4 \;\middle|\; \begin{array}{l} \lambda_4, \lambda_2 \text{ beliebig,} \\ \lambda_3 = -2\lambda_4 \text{ und} \\ \lambda_1 = -2\lambda_2 - 3\lambda_4 \end{array} \right\}$$

$$= \left\{ \begin{pmatrix} -2\lambda_2 - 3\lambda_4 \\ \lambda_2 \\ -2\lambda_4 \\ \lambda_4 \end{pmatrix} \;\middle|\; \lambda_2, \lambda_4 \in K \text{ bel.} \right\}$$

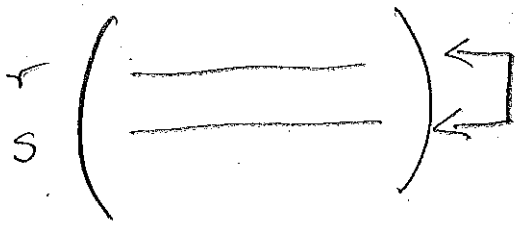
$$= \left\{ \lambda_2 \begin{pmatrix} -2 \\ 1 \\ 0 \\ 0 \end{pmatrix} + \lambda_4 \begin{pmatrix} -3 \\ 0 \\ -2 \\ 1 \end{pmatrix} \;\middle|\; \lambda_2, \lambda_4 \in K \right\}$$

$$= \left\langle \begin{pmatrix} -2 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} -3 \\ 0 \\ -2 \\ 1 \end{pmatrix} \right\rangle.$$

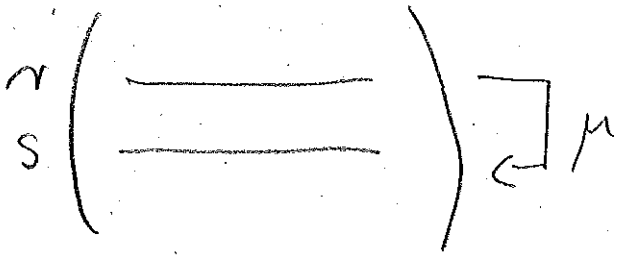
Sei nun $A = (\alpha_{ij}) \in \mathrm{Mat}_{m \times n}(K)$ beliebig.

Wollen nun A durch einen Algorithmus in ZSF bringen, ohne dabei $\mathrm{Ke}(A)$ zu ändern. Das geschieht durch Zeilenoperationen:

Typ I: Vertausche r-te und s-te Zeile für gewisse $r \neq s$. Notation:



Typ II: Addiere μ-fache der r-ten Zeile zur s-ten Zeile für gewisse $\mu \in K$, $r \neq s$. Notation:



Typ III: Multipliziere r-te Zeile mit einem $\varepsilon \in K \setminus \{0\}$. Notation:

$\left(\quad\quad\quad\right) \leftarrow \varepsilon$

Bsp. 9.8 Sei $A = \begin{pmatrix} 0 & 1 & 4 & 2 \\ 3 & 4 & 5 & 3 \\ 9 & 8 & 7 & 6 \end{pmatrix}$

$$\begin{pmatrix} 0 & 1 & 4 & 2 \\ 3 & 4 & 5 & 3 \\ 9 & 8 & 7 & 6 \end{pmatrix} \leftarrow \leftarrow$$

$$\begin{pmatrix} 3 & 4 & 5 & 3 \\ 0 & 1 & 4 & 2 \\ 9 & 8 & 7 & 6 \end{pmatrix} \rfloor -3$$

$$\begin{pmatrix} 3 & 4 & 5 & 3 \\ 0 & 1 & 4 & 2 \\ 0 & -4 & -8 & -3 \end{pmatrix} \rfloor 4$$

$$\begin{pmatrix} \boxed{3} & 4 & 5 & 3 \\ 0 & \boxed{1} & 4 & 2 \\ 0 & 0 & \boxed{8} & 5 \end{pmatrix} \qquad \pi_1 = 3,\ \pi_2 = 1,\ \pi_3 = 8.$$

↖ in ZSF.

Dieses Beispiel lässt sich formalisieren

Sei $A = (\alpha_{ij}) \in \mathrm{Mat}_{m\times n}(K)$.
Der folgende Durchlauf bringt A auf die Form:

$$\left(\begin{array}{c|c} 0 & \\ | & A' \\ 0 & \end{array}\right) \quad \text{oder} \quad \left(\begin{array}{c|c} \pi & * \\ \hline 0 & \\ | & A' \\ 0 & \end{array}\right)$$

wobei A' $(n+1)$ Spalten hat und $\pi \in K \setminus \{0\}$.

Falls in A die erste Spalte verschwindet ist nichts zu tun. Andernfalls machen wir folgende Schritte:

1. Schritt (Pivotsuche)

Wähle $1 \le r \le m$ mit $\alpha_{r1} \neq 0$.

2. Schritt (Zeilenoperation Typ I)

Vertausche r-te und 1-te Zeile.
Damach ist also $\pi = \alpha_{11} \neq 0$

3. Schritt (Zeilenoperation Typ II)

Für $i = 2, \dots, m$ setze $\mu = -\frac{a_{i1}}{\pi}$ und addiere μ-fache der 1.-ten Zeile zur i-ten Zeile. Danach ist also

$$a_{21} = \dots = a_{m1} = 0.$$

Dann ist die Matrix A in die Form

$$\left(\begin{array}{c|c} \pi & * \\ \hline 0 & \\ \vdots & A' \\ 0 & \end{array}\right)$$ gebracht worden.

Gauß-Algorithmus: Sei $A \in Mat_{m\times n}(K)$.

Man bringt A durch die Schritte 1. – 3. auf die Form

$$\left(\begin{array}{c|c} 0 & \\ \vdots & A' \\ 0 & \end{array}\right) \text{ mit } A' \in Mat_{m\times(n-1)}(K)$$

oder $$\left(\begin{array}{c|c} \pi & * \\ \hline 0 & \\ \vdots & A' \\ 0 & \end{array}\right) \text{ mit } A' \in Mat_{(m-1)\times(n-1)}(K)$$

Danach wendet man die Schritte 1. – 3. auf A' an. Nach endlich vielen Durchläufen erhält man eine Matrix $B \in \mathrm{Mat}_{m\times n}(K)$ in ZSF:

$$B = \begin{pmatrix} \Pi_1 & & & * \\ & \Pi_2 & & \\ & & \ddots & \\ 0 & & & \Pi_r \end{pmatrix}.$$

Bemerkung 3.9 Mit Zeilenoperationen vom Typ III erreicht man, $\Pi_1 = \dots = \Pi_r = 1$. Mit weiteren Zeilenoperationen vom Typ II erreicht man reduzierte ZSF.

Theorem 3.10 Der Gauß-Algorithmus bringt jedes $A \in \mathrm{Mat}_{m\times n}(K)$ durch endlich viele

Zeilenoperationen vom Typ I und Typ II auf ZSF

$$B = \begin{pmatrix} \text{II}_1 & & * \\ & \text{II}_2 & \\ & & \ddots \\ 0 & & \text{II}_1 \end{pmatrix}$$

Durch endlich viele weitere Zeilenoperationen vom Typ II und Typ III erreicht man reduzierte ZSF

$$\begin{pmatrix} 1 & 0 & 0 \\ & 1 & \vdots \\ & & 0 \\ 0 & & 1 \end{pmatrix}$$

Bemerkung 3.11 Wegen der Pivotsuche ist der Gauß-Algorithmus nicht-deterministisch. Entsprechend ist ZSF nicht eindeutig. Die reduzierte ZSF jedoch ist eindeutig. Beweis in Übung!

Propo 3.12 Sei $A \in Mat_{m\times n}(K)$ und B die Matrix, welche aus A durch Gauß-Algorithmus auf ZSF gebracht wurde. Dann gilt

$Ke(A) = Ke(B)$ und

$rank(A) = rank(B)$.

Beweis Um $Ke(A) = Ke(B)$ zu zeigen reicht es, Gleichheit bei Zeilenoperationen zu prüfen. Für Operationen vom Typ I und III ist das trivial. Wir müssen drucken, ob dies auch für Operationen von Typ II gilt. Sei $A = (a_{ij})$ und

$A \cdot X = 0$ für $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$. Das LGS

$A \cdot X = 0$ sieht folgendermaßen aus:

$$\sum_{j=1}^{n} \alpha_{ij} x_j = 0 \,, \quad 1 \le i \le m.$$

Sei B die Matrix, welche aus A durch Zeilenoperation vom Typ II entsteht.

$$A = \begin{pmatrix} \\ \\ \end{pmatrix} \begin{matrix} r \\ s \end{matrix} \Big] \mu$$

Dann ist das LGS für B gegeben durch

$$\sum_{j=1}^{n} \alpha_{ij} x_j = 0 \,, \quad 1 \le i \le m \,, \; i \neq s.$$

$$\sum_{j=1}^{n} (\mu \alpha_{rj} + \alpha_{sj}) x_j = 0.$$

Offensichtlich gilt $\mathrm{Ke}(A) \subset \mathrm{Ke}(B)$.

Sei nun $(\eta_1, \dots, \eta_n) \in \mathrm{Ke}(B)$.

Da $\sum_{j=1}^{n} \alpha_{rj} \eta_j = 0$ und

$\sum_{j=1}^{n} (\mu a_{rj} + a_{sj}) \lambda_j = 0$, folgt

$\sum_{j=1}^{n} a_{sj} \lambda_j = 0$, d.h. $\ker(B) \subset \ker(A)$.

Da nun $\operatorname{rank}(A) = \dim \operatorname{Im}(A)$ folgt aus Theorem 8.21 gerade $\operatorname{rank}(A) = \operatorname{rank}(B)$. □

Mit dem Gauß-Algorithmus lassen sich einige Probleme der linearen Algebra lösen.

Sei $A = (a_{ij}) \in \mathrm{Mat}_{m \times n}(K)$.

Problem 1 (Berechne von $\operatorname{rank}(A)$ und $\dim(\ker(A))$)

Bringe A mit Gauß-Algo. auf ZSF.
Dann $\operatorname{rank}(A)$ = Anzahl der Pivotspalten.
und $\dim(\ker(A))$ = Anzahl der <u>Nicht</u>-Pivotspalten.

Problem 2 (Berechnung einer Basis von $\ker(A)$)

Bringe A mit Gauß-Alg. auf Zeilenstufenform $B = (\beta_{ij})$. Dann benutze Proposition 3.6 (Bsp. 3.7 zeigt wie's geht)

Propo 3.13 Sei $A = (\alpha_{ij}) \in \mathrm{Mat}_{m\times n}(K)$ und $A: K^n \to K^m$ die lineare Abb.

Sei $\tilde{A}$ folgende Matrix

$$\tilde{A} = \begin{pmatrix} \alpha_{11} & \cdots & \alpha_{1n} & y_1 \\ \vdots & & \vdots & \vdots \\ \alpha_{m1} & \cdots & \alpha_{mn} & y_m \end{pmatrix} \in \mathrm{Mat}_{m\times(n+1)}(K)$$

mit $y = (y_1, \dots, y_m) \in K^m$ beliebig.

Dann gilt:

$$y \in \mathrm{Im}(A) \iff \mathrm{rank}(A) = \mathrm{rank}(\tilde{A}).$$

Beweis Seien

$A: K^n \to K^m$ und $\tilde{A}: K^{n+1} \to K^m$

die entsprechenden linearen Abb. Mit

$U = \mathrm{Im}(A)$ und $\tilde{U} = \mathrm{Im}(\tilde{A})$ gilt

$\tilde{U} = \langle U, y \rangle$.

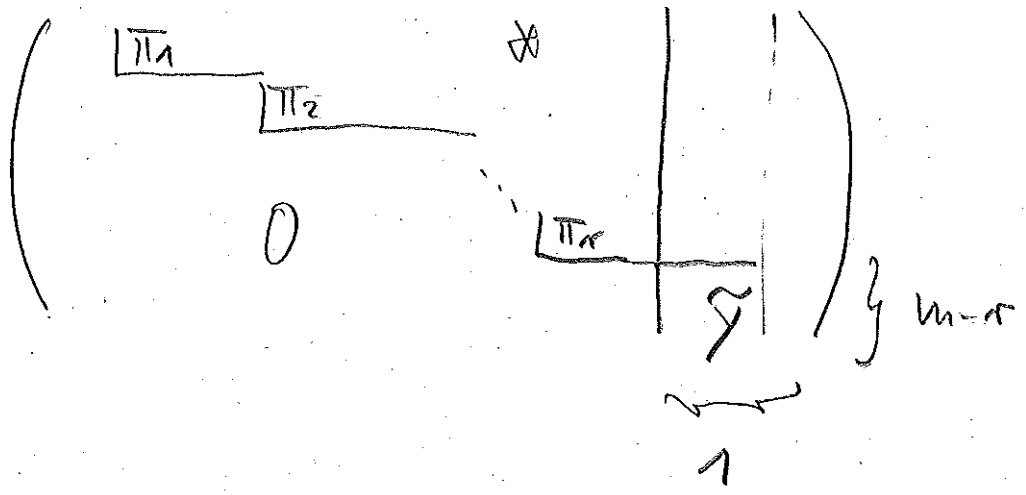
„$\Rightarrow$" Sei $y \in U$, dann $\tilde{U} = U$ also

$\mathrm{rank}(\tilde{A}) = \dim \tilde{U} = \dim U = \mathrm{rank}(A)$.

„$\Leftarrow$" Sei $\mathrm{rank}(A) = \mathrm{rank}(\tilde{A})$. Da $U \subset \tilde{U}$ und $\dim U = \dim \tilde{U}$ folgt aus Propo 7.16 $U = \tilde{U}$.

Problem 3 (Entscheiden, ob $y \in \mathrm{Im}(A)$ für $y \in K^m$)

Betrachte erweiterte Matrix $\tilde{A}$ aus Propo. 3.13 und bringe $\tilde{A}$ mit Gauß-Algo. auf ZSF. $\tilde{B}$:

$\tilde{B} =$ 

Es gilt nach Propo. 3.13: $y \in \mathrm{Im}(A)$ genau dann, wenn die Einträge im $\tilde{y}$-Block verschwinden.

Problem 4 (Basis für $\mathrm{Im}(A) \subset K^m$ angeben)

Bringe A mit Gauß-Algo. auf ZSF B.

Sei $P = \{j_1, \dots, j_r\}$ die Menge der Pivotspaltenindizes und $a_1, \dots, a_n \in K^m$ die Spalten von A. Dann ist

$$a_j \in \mathrm{Im}(A), \quad j \in P$$

eine Basis von $\mathrm{Im}(A)$.

Dies folgt aus der Tatsache, daß
$a_j \in K^m$, $j \in P$ einer maximalen linear unabhängigen Menge ist
aus Propo. 3.4.

Propo 3.14 Sei $A = (a_{ij}) \in \mathrm{Mat}_{m \times n}(K)$
und $a_1, \dots, a_n \in K^m$ die Spalten
von A. Äquivalent sind

(i) $a_1, \dots, a_n \in K^m$ sind ein Erzeugendensystem von K^m.

(ii) $A : K^n \to K^m$ ist surjektiv

(iii) $\mathrm{rank}(A) = m$

Beweis Seien $e_1, \dots, e_n \in K^n$ die Standard-
basisvektoren. Dann gilt
$a_j = A e_j$ und somit

$$\mathrm{Im}(A) = \langle a_1, \dots, a_n \rangle \subset K^m.$$

Offensichtlich gilt (i) $\Leftrightarrow$ (ii).
Das (i) $\Leftrightarrow$ (iii) folgt aus Propo 7.16

□

Propo 9.15 Sei $A = (\alpha_{ij}) \in \mathrm{Mat}_{m\times n}(K)$ und $a_1, \dots, a_n \in K^m$ die Spalten von A. Äquivalent sind

(i) $a_1, \dots, a_n \in K^m$ sind linear unabhängig

(ii) $\mathrm{Ke}(A) = 0$

(iii) $A : K^n \to K^m$ ist injektiv

(iv) $\mathrm{rank}(A) = n$.

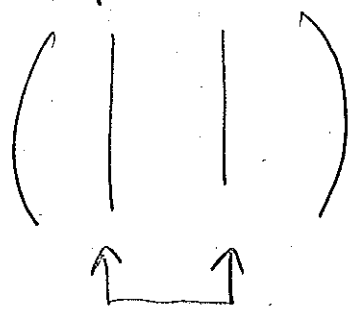
Beweis Für $x_1, \dots, x_n \in K$ gilt

$x_1 a_1 + \dots + x_n a_n = A \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$. Offensichtlich gilt (i) $\Leftrightarrow$ (ii). Aus Lemma 8.16 folgt (ii) $\Leftrightarrow$ (iii). Proposition 7.16 zeigt (i) $\Leftrightarrow$ (iv). ☐

Neben Zeilenoperationen gibt es auch Spaltenoperationen. Sei $A \in \mathrm{Mat}_{m\times n}(K)$.

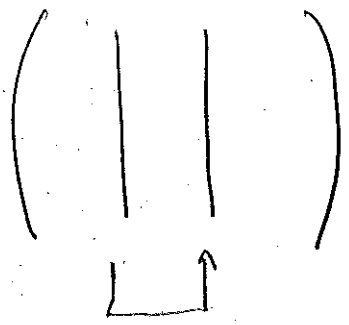
Spaltenoperationen:

Typ I



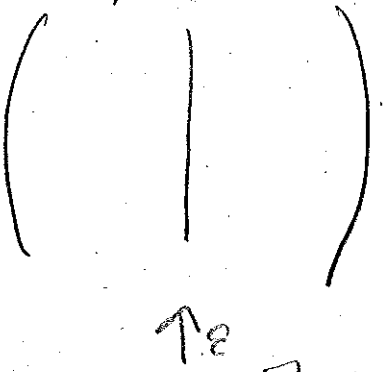
r-te und s-te Spalte vertauschen

Typ II



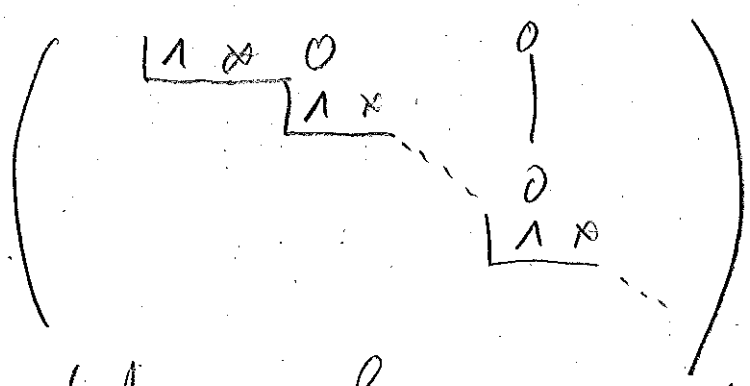
μ-faches der r-ten Spalte zur s-ten Spalte addieren

Typ III



Spalte mit $\varepsilon \in K \setminus \{0\}$ multiplizieren

Das Bild der Matrix A ändert sich nicht bei Spaltenoperationen vom Typ I und Typ III. Der Austauschsatz von Steinitz sagt, daß Typ II - Operationen das Bild ebenfalls nicht ändern. Hat man eine Matrix $A \in \mathrm{Mat}_{m \times n}(K)$ mit Zeilenoperationen auf reduzierte ZSF



gebracht, so kann man mit Spalten-

operationen die Matrix auf die Form

$$(*) \qquad \left(\begin{array}{c|c} \begin{matrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{matrix} & 0 \\ \hline 0 & 0 \end{array}\right) \begin{matrix} \} r \\ \} m-r \end{matrix}$$

$\underbrace{\qquad}_{r} \quad \underbrace{\qquad}_{n-r}$

bringen.

Man kann also jede Matrix $A \in Mat_{m\times n}(K)$ durch Zeilen- und Spaltenoperationen auf die Form $(*)$ bringen. Hierbei ist $r = \operatorname{rank}(A)$.

Seien $U \subset K^m$ und $V \subset K^n$ die von den Spalten bzw. Zeilen von A erzeugten UVR. Man definiert

$$\text{Spaltenrang} = \dim(U)$$
$$\text{Zeilenrang} = \dim(V)$$

Wir sehen, daß Spaltenrang und Zeilenrang bei $(*)$ übereinstimmen.

Prop. 3.16 Für jede Matrix $A \in Mat_{m\times n}(K)$ gilt Zeilenrang = Spaltenrang.

Damit ist Rang wohldefiniert.

Frage: Wie löst man LGS der Form $A \cdot x = b$, $b \in K^m$. Für $b = 0$ haben wir schon gesehen wie das geht.

Korollar 3.17 Sei $A \in \mathrm{Mat}_{m \times n}(K)$, $y = (y_1, \ldots, y_m) \in K^m$ beliebig. Sei

$$\tilde{A} = \left(A \,\middle|\, \begin{matrix} y_1 \\ \vdots \\ y_m \end{matrix} \right).$$

(i) $A \cdot x = y$ ist genau dann lösbar, wenn $\mathrm{rank}(A) = \mathrm{rank}(\tilde{A})$.

(ii) $A \cdot x = y$ besitzt für jedes $y \in K^m$ mindestens eine Lösung, wenn $\mathrm{rank}(A) = m$.

Beweis (i) ist Propo. 3.13.

(ii) folgt aus Propo. 3.14.

Propo. 3.18 Für $A \in Mat_{m\times n}(K)$ und $y \in K^m$ habe man eine Lösung v_y von $A \cdot x = y$. Bezeichnen wir mit L_y die Lösungsmenge des LGS $Ax = y$ und mit L_0 die Lösungsmenge von $A \cdot x = 0$, so gilt

$$L_y = v_y + L_0.$$

Beweis Wir müssen zeigen, daß

$L_y \subset v_y + L_0$ und

$v_y + L_0 \subset L_y$.

Also sei $b \in v_y + L_0$, d.h.

$b = v_y + r$, $r \in L_0$. Dann gilt

$$A \cdot b = A(v_y + r) = Av_y + Ar$$
$$= Av_y = y.$$

Also $b \in L_y$.

Sei nun $c \in L_y$. Dann gilt

für $c - v_y$ gilt $A(c - v_y) =$

$Ac - Av_y = y - y = 0$. Also $c - v_y \in L_0$,

d.h. $c \in v_y + L_0$. ∎

Bsp. 3.19 $A = \begin{pmatrix} 0 & 0 & 1 & 2 \\ 1 & 2 & 1 & 3 \\ 1 & 2 & 2 & 5 \end{pmatrix} \in \mathrm{Mat}_{3\times 4}(\mathbb{R})$

und $y_1 = \begin{pmatrix} 1 \\ 1 \\ 3 \end{pmatrix}$, $y_2 = \begin{pmatrix} 1 \\ 1 \\ 2 \end{pmatrix}$.

$$(A|y_1) = \left(\begin{array}{cccc|c} 0 & 0 & 1 & 2 & 1 \\ 1 & 2 & 1 & 3 & 1 \\ 1 & 2 & 2 & 5 & 3 \end{array}\right) \leftarrow \quad \left(\begin{array}{cccc|c} 1 & 2 & 1 & 3 & 1 \\ 0 & 0 & 1 & 2 & 1 \\ 1 & 2 & 2 & 5 & 3 \end{array}\right) \leftarrow -1$$

$$\left(\begin{array}{cccc|c} 1 & 2 & 1 & 3 & 1 \\ 0 & 0 & 1 & 2 & 1 \\ 0 & 0 & 1 & 2 & 2 \end{array}\right) \leftarrow -1 \quad \left(\begin{array}{cccc|c} 1 & 2 & 0 & 1 & 0 \\ 0 & 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{array}\right)$$

$\mathrm{rank}(A) = 2 \neq \mathrm{rank}((A|y_1)) = 3$. Daher

besitzt $Ax = y_1$ keine Lösung, d.h. $L_{y_1} = \emptyset$.

$$(A|y_2) = \left(\begin{array}{cccc|c} 0 & 0 & 1 & 2 & 1 \\ 1 & 2 & 1 & 3 & 1 \\ 1 & 2 & 2 & 5 & 2 \end{array}\right) \leftarrow \quad \left(\begin{array}{cccc|c} 1 & 2 & 1 & 3 & 1 \\ 0 & 0 & 1 & 2 & 1 \\ 1 & 2 & 2 & 5 & 2 \end{array}\right) \leftarrow -1$$

$$\left(\begin{array}{cccc|c} 1 & 2 & 1 & 3 & 1 \\ 0 & 0 & 1 & 2 & 1 \\ 0 & 0 & 1 & 2 & 1 \end{array}\right) \rightarrow \left(\begin{array}{cccc|c} 1 & 2 & 1 & 3 & 1 \\ 0 & 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

Wir bestimmen die Lösungsmenge wie folgt:

$$\begin{aligned} x_1 + 2x_2 + x_3 + 3x_4 - 1 &= 0 \\ x_3 + 2x_4 - 1 &= 0 \end{aligned}$$

ZTS von A ist $\left(\begin{array}{cccc} 1 & 2 & 1 & 3 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 \end{array}\right)$, also

$$L_{y_2} = \left\{ \begin{pmatrix} 1 - 3\lambda_4 - (1 - 2\lambda_4) - 2\lambda_2 \\ \lambda_2 \\ 1 - 2\lambda_4 \\ \lambda_4 \end{pmatrix} \mid \lambda_2, \lambda_4 \in \mathbb{R} \right\}$$

$$= \left\{ \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \lambda_2 \begin{pmatrix} -2 \\ 1 \\ 0 \\ 0 \end{pmatrix} + \lambda_4 \begin{pmatrix} -1 \\ 0 \\ -2 \\ 1 \end{pmatrix} \mid \lambda_2, \lambda_4 \in \mathbb{R} \right\}$$

$$= \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \left\langle \begin{pmatrix} -2 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \\ -2 \\ 1 \end{pmatrix} \right\rangle$$

Wir erinnern an den assoziativen Ring $\mathrm{Mat}_n(K)$. Das Einselement ist die Einheitsmatrix

$$E = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$$

Hat eine Matrix $A \in \mathrm{Mat}_n(K)$ ein Inverses bezüglich der Matrixmultiplikation, so heißt A invertierbar, Notation: A^{-1}.

Folgende Matrizen sind invertierbar: $\lambda \in K \setminus \{0\}$

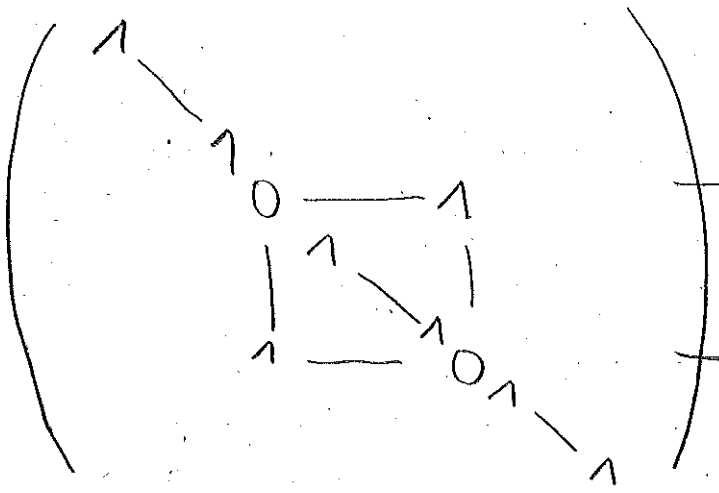
$$E_r(\lambda) = \begin{pmatrix} 1 & & & & 0 \\ & \ddots & & & \\ & & \lambda & & \\ & & & \ddots & \\ 0 & & & & 1 \end{pmatrix} \leftarrow r\text{-te Zeile}$$

$\uparrow$ r-te Spalte

$$E_r(\lambda)^{-1} = \begin{pmatrix} 1 & & & & 0 \\ & \ddots & & & \\ & & \lambda^{-1} & & \\ & & & \ddots & \\ 0 & & & & 1 \end{pmatrix} \leftarrow r\text{-te Zeile}$$

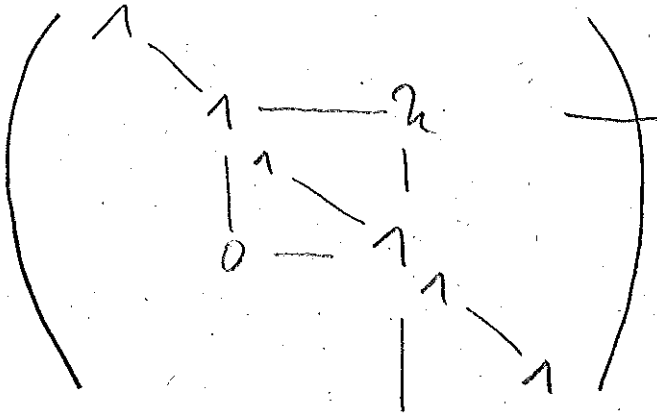
$\uparrow$ r-te Spalte

$E_r^s =$



$(E_r^s)^{-1} = E_r^s$ (nachrechnen)

$E_r^s(\lambda) =$



r-te Spalte

$(E_r^s(\lambda))^{-1} = E_r^s(-\lambda)$ (nachrechnen)

Die Matrizen $E_r(\lambda)$, E_r^s, $E_r^s(\lambda)$ heißen Elementarmatrizen. Es gilt

Propo. 9.20 Sei $A \in Mat_{m\times n}(K)$.

Dann entspricht $E_r(\lambda) \cdot A$ der Matrix, welche aus A durch Zeilenoperation

vom Typ III entsteht. $E^s_r \cdot A$ entspricht Zeilenop. vom Typ I und $E^s_r(\eta) \cdot A$ Zeilenop. vom Typ II.

Beweis Nachrechnen!

Frage: Wie können wir entscheiden, ob ein $A \in Mat_m(K)$ invertierbar ist, und wie können wir gegebenenfalls A^{-1} berechnen?

Propo 5.21 $A \in Mat_m(K)$ ist invertierbar genau dann, wenn $\operatorname{rank}(A) = m$.

Beweis Sei $A: K^m \to K^m$ lineare Abb und B das Inverse. Dann ist $B: K^m \to K^m$ und $A \cdot B = B \cdot A = E$. Also ist $A: K^m \to K^m$ bijektiv.

Propo 3.14 und 3.15 ergeben
rank(A) = n. Sei umgekehrt rank(A) = n.
Dann folgt aus Propo. 3.14 und 3.15,
daß $A: K^n \to K^n$ bijektiv ist. Das
bedeutet, es gibt $B: K^n \to K^n$ mit
$A \cdot B = B \cdot A = E$. ∎

Verfahren zur Bestimmung von A^{-1}:

Zunächst

Lemma 3.22 Sei $A \in Mat_n(K)$ invertierbar
und $B_1, \dots, B_n$ Elementar-
matrizen, so daß
$B_1 \cdots B_n \cdot A = E$. Dann
gilt $A^{-1} = B_1 \cdots B_n$.

Beweis Setze $B = B_1 \cdots B_n$. Dann
$B \cdot A = E$.

Da A invertierbar, existiert $B' \in \mathrm{Mat}_n(K)$ mit $A \cdot B' = E$. Nun ist

$$B \cdot A \cdot B' = B = E \cdot B' = B'.$$

Also ist $B = A^{-1}$. ☐

Da Multiplikation mit Elementar-matrizen den Zeilenoperationen vom Typ I, II und III entsprechen kann man folgendes machen:

	A	E
1)	$B_1 A$	$B_1 E$
2)	$B_2 B_1 A$	$B_2 B_1 E$
	⋮	⋮
4)	$\underbrace{B_k \cdots B_1 \cdot A}_{= E}$	$B_k \cdots B_1 \cdot E$

Dann steht auf der rechten Seite

A^{-1}.

Bsp 9.23 $A = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 2 & 1 \\ 0 & -1 & 0 & 1 \\ 1 & 0 & 0 & 2 \end{pmatrix} \in \mathrm{Mat}_4(\mathbb{R})$.

Zunächst schaut man, ob A invertierbar ist.
Man rechnet nach, dass $\mathrm{rank}(A) = 4$.

$$\begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 2 & 1 \\ 0 & -1 & 0 & 1 \\ 1 & 0 & 0 & 2 \end{pmatrix} \quad \left| \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \right.$$

$(-1)\cdot$ (1. Zeile) $+$ (2. Zeile) $\cdot(-1)$

$$\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & -1 & 0 & 1 \\ 0 & 0 & -1 & 1 \end{pmatrix} \quad \left| \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix} \right.$$

$1\cdot$ (2. Zeile) $+$ (3. Zeile) $\cdot(-1)$

$$\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & -1 & 1 \end{pmatrix} \quad \left| \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ -1 & 1 & 1 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix} \right.$$

$(-1)\cdot$ (1. Zeile) $+$ (4. Zeile) $\cdot(-1)$

$(-1)\cdot$ (2. Zeile) $+$ (3. Zeile) $\cdot(-1)$

$1\cdot$ (3. Zeile) $+$ (4. Zeile) $\cdot(-1)$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 2 \end{pmatrix} \quad \left| \quad \begin{pmatrix} 2 & -1 & -1 & 0 \\ 0 & 0 & -1 & 0 \\ -1 & 1 & 1 & 0 \\ -2 & 1 & 1 & 1 \end{pmatrix} \right.$$

$\frac{1}{2} \rightarrow$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \left| \quad \begin{pmatrix} 2 & -1 & -1 & 0 \\ 0 & 0 & -1 & 0 \\ -1 & 1 & 1 & 0 \\ -1 & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{pmatrix} \right.$$

$1 \rightarrow$, $-1 \rightarrow$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \left| \quad \begin{pmatrix} 2 & -1 & -1 & 0 \\ -1 & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \\ 0 & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ -1 & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{pmatrix} \right.$$

$\leftarrow A^{-1}$

Man rechnet nach: $A A^{-1} = E$.

§ 10
Äquivalenzrelationen und Basiswechsel

Sei V ein K-VR und $A = \{a_1, \dots, a_n\}$ und $A' = \{a_1', \dots, a_n'\}$ zwei Basen.

Sei nun $a_j = \beta_{1j} a_1' + \dots + \beta_{nj} a_n'$,

dann nennt man

$$T_{A'}^{A} = \begin{pmatrix} \beta_{11} & \dots & \beta_{1n} \\ \vdots & & \vdots \\ \beta_{n1} & \dots & \beta_{nn} \end{pmatrix}$$

die Basiswechselmatrix. Wir sehen $T_{A'}^{A} \in \mathrm{Mat}_n(K)$ und da $T_{A'}^{A}$ einer linearen Abb entspricht, welche die Basis A auf die Basis A' abbildet, ist $T_{A'}^{A}$ bijektiv, als Matrix also invertierbar. Offensichtlich gilt $\left(T_{A'}^{A}\right)^{-1} = T_{A}^{A'}$.

Ein Vektor $v \in V$ habe bezüglich der Basis $a_1, \dots, a_n$ die Koordinaten $(\lambda_1, \dots, \lambda_n) \in K^n$, d.h. $v = \lambda_1 a_1 + \dots + \lambda_n a_n$.

Dies beruht auf der Tatsache, daß wir einen kanonischen Isomorphismus $\mathrm{can} : V \to K^n$, $a_i \mapsto e_i$ haben.

Sei nun $a_1', \dots, a_n'$ eine zweite Basis von V und bezeichne $T_{A'}^{A}$ die Basiswechselmatrix, wobei $A = \{a_1, \dots, a_n\}$ und $A' = \{a_1', \dots, a_n'\}$. Sind nun $(\lambda_1, \dots, \lambda_n)$ und $(\lambda_1', \dots, \lambda_n')$ die Koordinaten für $v \in V$, so sieht man leicht

$$\begin{pmatrix} \lambda_1' \\ \vdots \\ \lambda_n' \end{pmatrix} = T_{A'}^{A} \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}.$$

Beispielsweise sei $V \simeq K^2$ gegeben mit Basen $A = \{b_1, b_2\}$, $A' = \{b_1', b_2'\}$ gemäß:

$$T_{A'}^{A} = \begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix},$$ wenn

$$b_1 = \alpha_{11} b_1' + \alpha_{21} b_2', \quad b_2 = \alpha_{12} b_1' + \alpha_{22} b_2'.$$

Für $v = x_1 b_1 + x_2 b_2 = x_1' b_1' + x_2' b_2'$ gelte dann:

$$v = (x_1 \alpha_{11} + x_2 \alpha_{21}) b_1' + (x_1 \alpha_{12} + x_2 \alpha_{22}) b_2'$$

Also $x_1' = x_1 \alpha_{11} + x_2 \alpha_{21}$, $x_2' = x_1 \alpha_{12} + x_2 \alpha_{22}$.

Wir sehen

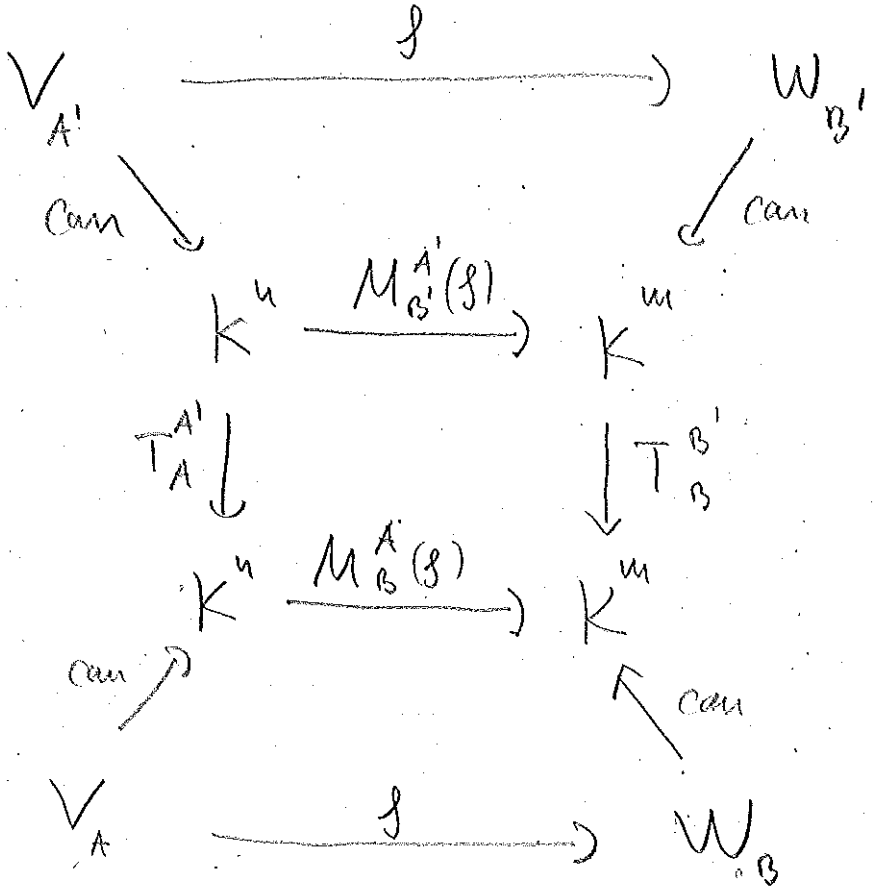
$$\begin{pmatrix} x_1' \\ x_2' \end{pmatrix} = \begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}.$$

Seien nun V und W K-VR und $f: V \to W$ lineare Abb. Es seien $A = \{a_1, \dots, a_n\}$, $A' = \{a_1', \dots, a_n'\}$ Basen von V und $B = \{b_1, \dots, b_m\}$, $B' = \{b_1', \dots, b_m'\}$ Basen von W gegeben.

Seien $M_B^A(f)$ und $M_{B'}^{A'}(f)$ die Abb.-matrizen von f bezüglich der Basen A, B bzw A', B'. Dann gilt

$$M_{B'}^{A'}(f) = T_{B'}^{B}\, M_B^A(f)\, T_A^{A'}$$

Das folgt aus folgendem Diagramm:



Ein wichtiger Spezialfall ist, wenn $f: V \to V$ und wenn wir $A = \{a_1, \dots, a_n\}$ und $A' = \{a_1', \dots, a_n'\}$ als Basen benutzen. Dann gilt

$$M_{A'}^{A'}(f) = T_{A'}^{A} \, M_{A}^{A}(f) \, T_{A}^{A'}$$

mit $T = T_{A}^{A'}$ folgt $M_{A'}^{A'}(f) = T^{-1} M_{A}^{A}(f) T$.

Def 10.1 Zwei Matrizen $A, B \in \mathrm{Mat}_n(K)$ heißen ähnlich, wenn es eine invertierbare Matrix $T \in \mathrm{Mat}_n(K)$ gibt mit

$$B = T^{-1} A T.$$

Diagramm dazu ist:

$$\begin{array}{ccc} K^n & \xrightarrow{B} & K^n \\ T \downarrow & & \downarrow T \\ K^n & \xrightarrow{A} & K^n \end{array} \qquad T^{-1}$$

Beobachtung: Sei $A \in Mat_n(K)$.

Dann ist A ähnlich zu A.

Diagramm:

$$\begin{array}{ccc} K^n & \xrightarrow{A} & K^n \\ E \downarrow & & \downarrow E \\ K^n & \xrightarrow{A} & K^n \end{array}$$

Da $E^{-1} = E$ gilt offensichtlich

$$A = E^{-1} A E = E A E = E \cdot A = A.$$

Seien $A, B \in Mat_n(K)$ ähnlich, dann gilt:

$B = T^{-1} A T$ und somit

$$A = T B T^{-1} = (T^{-1})^{-1} B T^{-1}.$$

Sind $A, B \in Mat_n(K)$ und $B, C \in Mat_n(K)$ ähnlich, so auch $A, C \in Mat_n(K)$.

Das sieht man so:

$B = T^{-1}AT$ und $C = R^{-1}BR$ ... Einsetzen ergibt:

$$C = R^{-1}(T^{-1}AT)R = (TR)^{-1}A(TR).$$

Also sind A, C ähnlich.

Diese Beobachtung verallgemeinert sich zur Definition der Äquivalenzrelation.

Def 10.2 Sei X eine Menge und $R \subset X \times X$ eine Teilmenge. Wir schreiben $a \sim b$ für $(a,b) \in R \subset X \times X$. Man nennt R eine Äquivalenzrelation auf X, wenn gilt

(i) $a \sim a$ für alle $a \in X$ (reflexiv)

(ii) gilt $a \sim b$, so auch $b \sim a$ (symmetrisch)

(iii) aus $a \sim b$ und $b \sim c$ folgt $a \sim c$. (transitiv)

Bsp 10.3 $X = Mat_n(\mathbb{K})$. $A, B \in X$ und

$A \sim B \iff B = T^{-1} A T$.

Haben gesehen, daß Ähnlichkeit von Matrizen eine Äquivalenzrelation ist.

Bsp 10.4 Sei $n \geq 0$ und $X = \mathbb{Z}$.

$a, b \in \mathbb{Z}$, dann definiert

$a \sim b \iff b - a = s \cdot n$ für ein $s \in \mathbb{Z}$

eine Äquivalenzrelation auf $\mathbb{Z}$.

Zu (i): mit $s = 0$ folgt $a - a = 0 \cdot n$, also $a \sim a$.

Zu (ii): aus $b - a = s \cdot n$ folgt $a - b = (-s) \cdot n$.

Zu (iii): Seien $b - a = sn$ und $c - b = tn$, so folgt

$c - b + b - a = sn + tn = (s+t)n$,

also $a \sim c$.

Sei R eine Äquivalenzrelation auf X.
Zu jedem $a \in X$ bilden wir die
Äquivalenzklassen

$$[a] = \{x \in X \mid x \sim a\}.$$

Dann ist $[a] \subset X$ eine Teilmenge.
Da $a \sim a$ folgt $[a] \neq \emptyset$.

Propo 10.5 Sei R eine Äquivalenzrelation auf X. Für alle $a, b \in X$ gilt:

$[a] = [b]$ oder $[a] \cap [b] = \emptyset$.

Beweis Sei $[a] \cap [b] \neq \emptyset$. Zu zeigen ist $[a] = [b]$.
Wähle $c \in [a] \cap [b]$. Dann gilt $c \sim a$ und $c \sim b$.
Sei $x \in [a]$, also $x \sim a$.
Da $a \sim x$ und $c \sim a$ folgt $c \sim x$. Da $b \sim c$ folgt

$b \sim x$, d.h. $x \sim b$ also $x \in [b]$.
Wir haben gezeigt, daß $[a] \subset [b]$. Analog zeigt man $[b] \subset [a]$, also $[a] = [b]$. ∎

Wir wollen nun $[a] \subset X$ als Element $[a] \in X/R$ auffassen, Unsere neue Menge ist also

$$X/R := \{ [a] \mid a \in X \}.$$

Mit dieser Notation erhalten wir:

Propo 10.6 Sei R eine Äquivalenzrelation auf X. Dann ist die Vereinigung

$$X = \bigcup_{[a] \in X/R} [a]$$

disjunkt.

Beweis: Jedes $a \in X$ taucht in der Vereinigung auf, da $a \in [a]$. Nach Propo. 10.5 ist die Vereinigung disjunkt. ☐

Anwendungen von Äquivalenzrelationen:

Die Ringe $\mathbb{Z}/n\mathbb{Z}$ können nun auf rigorose definiert werden.

Sei $n \neq 0$. Auf $\mathbb{Z}$ haben wir Äquivalenzrelation $a \sim b \Leftrightarrow b - a = s \cdot n$ für ein $s \in \mathbb{Z}$

(siehe Bsp 10.4). Das bedeutet $n \mid b-a$.

Die Äquivalenzklassen

$$[a] = \{ a + sn \mid s \in \mathbb{Z} \}$$

werden Kongruenzklassen genannt.

Schreiben $\mathbb{Z}/n\mathbb{Z} = \{ [a] \mid a \in \mathbb{Z} \}$

Auf $\mathbb{Z}/n\mathbb{Z}$ werden Verknüpfungen definiert

$$[a] + [b] = [a+b]$$
$$[a] \cdot [b] = [a \cdot b]$$

Dadurch wird $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ zu einem Ring. Er enthält genau n Elemente

$[0], [1], \ldots, [n-2], [n-1]$.

Haben in Übung folgendes gesehen:
Sei $U \subset K^n$ ein UVR. Dann existiert eine Matrix $A \in \mathrm{Mat}_{m \times n}(K)$, so daß $\mathrm{Ke}(A) = U$.
Wie kann man das genau verstehen?
Mit Hilfe von Äquivalenzrelationen auf K^n!

Sei V ein K-VR und $U \subset V$ ein UVR. Definieren auf V eine Relation R durch

$$a \sim b \iff b - a \in U$$

Dies ist Äquivalenzrelation:
zu (i) $a \sim a$, da $a - a = 0 \in U$.

zu (ii): Sei $a \sim b$, also $b-a \in U$. Dann gilt auch $\lambda(b-a) \in U$ für alle $\lambda \in K$. Insbesondere für $\lambda = -1$. Also $a-b \in U$, d.h. $b \sim a$.

zu (iii): Seien $a \sim b$ und $b \sim c$, d.h. $b-a \in U$ und $c-b \in U$. Dann gilt $(c-b)+(b-a) = c-a \in U$, also $a \sim c$.

Die Äquivalenzklassen sind

$$[a] = \{x \in V \mid x-a \in U\}$$
$$= \{x \in V \mid x = a+r \text{ für } r \in U\}$$
$$= a + U$$

Wir schreiben nun

$$V/U := \{a+U \mid a \in V\}$$

Definieren auf V/U Vektoraddition und Skalarmultiplikation durch:

$[a] + [b] = [a+b]$ und $\lambda[a] = [\lambda a]$.

Die Verknüpfungen sind wohldefiniert; d.h. Längen nicht von der Wahl der Repräsentanten ab. Seien $a \in [a]$, $b \in [b]$ und wähle $a' \in [a]$, $b' \in [b]$ so gilt

$$a'+b' - (a+b) = (a'-a) + (b'-b) \in U,$$

d.h. $[a+b] = [a'+b']$. Weiter gilt

$$\lambda \cdot a' - \lambda \cdot a = \lambda(a-a') \in U.$$

Man rechnet jetzt nach, daß V/U ein K-VR ist. Man hat kanonische Abb.

$$\pi : V \to V/U, \quad a \mapsto a+U,$$

welche linear ist. Man sieht

$$\ker \pi = \{x \in V \mid x+U = U\}$$
$$= \{x \in V \mid x \in U\} = U.$$

Der K-VR V/U heißt Quotienten-vektorraum.

§11

Determinanten

Haben auf Übungsblatt 10 gesehen, daß aus $ad - bc \neq 0$, $a,b,c,d \in K$ folgt: Die Matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Mat_2(K)$ ist invertierbar. Man kann auch zeigen, daß aus der Invertierbarkeit von $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ auch $ad - bc \neq 0$ folgt. Wie ist das zu verstehen? Das verstehen soll mit Hilfe des Begriffs der Determinante.

Propo 11.1 Sei $\det : Mat_n(K) \to K$ eine Abb. mit den folgenden Eigenschaften:

(i) $\det$ ist linear in jeder Zeile

(ii) Ist $\operatorname{rank}(A) < n$, so ist $\det(A) = 0$

(iii) $\det(E) = 1$.

Dann ist die Abb. $\det : Mat_n(K) \to K$ eindeutig. Man nennt diese Abb. Determinante und die Zahl $\det(A) \in K$ die Determinante von A.

Um obige Proposition zu beweisen, benötigen wir folgendes

Lemma M.2 Sei $\det : Mat_n(K) \to K$ eine Abb mit Eigenschaften (i) und (ii). Dann gilt:

① $\det(A) = -\det(E_s^r \cdot A)$

② $\det(E_r(\lambda) \cdot A) = \lambda \cdot \det(A)$

③ $\det(A) = \det(E_s^r(\lambda) \cdot A)$

Beweis ② folgt direkt aus der Linearität von $\det$ in den Zeilen.

(3): Zunächst bilden wir aus A die Matrix A'', in dem wir das Vielfache der r-ten Zeile nicht zur s-ten Zeile addieren, sondern indem wir die s-te Zeile durch das Vielfache der r-ten ersetzen. Dann sind die Zeilen in A'' linear abhängig und es gilt $\operatorname{rang}(A'') < n$, also $\det(A'') = 0$. Aus der Dreiecksform folgt dann $\det(E_s^r(\lambda) A) = \det(A) + \det(A'') = \det(A)$.

(1): Seien die r-te und s-te die beiden zu vertauschenden Zeilen. Nach (3) gilt $\det(A) = \det(E_s^r(1) \cdot A)$. Ebenfalls nach (3) gilt

$$\det(E_s^r(1)\cdot E_s^r\cdot A) = \det(E_s^r\cdot A).$$

Die Matrizen $E_s^r(1)\cdot A$ und $E_s^r(1)\cdot E_s^r\cdot A$ unterscheiden sich dann nur in der r-ten Zeile. In der s-ten Zeile steht bei beiden die Summe der r-ten und s-ten Zeile. Wegen der Linearität in der s-ten Zeile ist dann

$$\det(E_s^r(1)\cdot A) + \det(E_s^r(1)\cdot E_s^r\cdot A)$$

gleich der Determinante einer Matrix, welche in der s-ten und r-ten Zeile jeweils die Summe aus r-te und s-te Zeile stehen hat.

Also

$$\det(E_s^r(1)\,A) + \det(E_s^r(1)\,E_s^r\cdot A) = 0,$$

folglich

$$\det(A) + \det(E_{sr} \cdot A) = 0 \qquad \square$$

Beweis von 10.1

Seien $\det$ und $\det'$ zwei Abb. mit Eigenschaften (i), (ii), (iii). Sei B eine Matrix, welche aus A durch Zeilenoperationen hervorgeht, so folgt $\det(A) = \det'(A) \Leftrightarrow \det(B) = \det'(B)$.

Angenommen $\operatorname{rang}(A) < n$, dann gilt trivialerweise $\det(A) = 0 = \det'(A)$.

Sei also $\operatorname{rang}(A) = n$. Dann kann man A durch Zeilenoperationen in Einheitsmatrix E verwandelt werden.

Aus $\det(E) = \det'(E) = 1$ folgt dann induktiv $\det(A) = \det'(A)$ $\square$

Wir haben also gesehen: Falls $\det : Mat_n(K) \to K$ existiert, so ist die Abb. eindeutig.

Frage: existiert so eine Abb?

Propo M.3 Sei $A = (a_{ij}) \in Mat_n(K)$. und

$$\det(A) = \sum_{\sigma \in S_n} sign(\sigma)\, a_{1\sigma(1)} \cdots a_{n\sigma(n)}.$$

Dann erfüllt det die Eigenschaften (i), (ii), (iii).

Die obige Formel für det heißt Leibnizsche Formel.

Beweis (i): Die Linearität in den Zeilen hat offensichtlich jede der $n!$ Summanden, also auch die Summe.

(iii): Ist $A = E$, so ist nur ein Summand von Null verschieden,

nämlich $\operatorname{sign}(\mathrm{id})\, a_{11} \cdots a_{nn}$ und $a_{ii} = 1$.

Also $\det(E) = 1$. Es bleibt zu zeigen, daß

(ii) gilt. Dazu genügt es zu zeigen, daß

$\sum_{\sigma \in S_n} \operatorname{sign}(\sigma)\, a_{1\sigma(1)} \cdots a_{n\sigma(n)}$ verschwindet,

sobald A zwei gleiche Zeilen hat. Seien

also r-te und s-te Zeile gleich und $\alpha \in S_n$

die Permutation welche nur $r, s \in \{1, \dots, n\}$

vertauschen. // Sei nun A_n die Menge

der geraden Permutationen, so gilt

$$\sum_{\gamma \in S_n} \operatorname{sign}(\gamma)\, a_{1\gamma(1)} \cdots a_{n\gamma(n)} =$$

$$\sum_{\tau \in A_n} \left(\operatorname{sign}(\tau)\, a_{1\tau(1)} \cdots a_{n\tau(n)} + \operatorname{sign}(\tau \circ \sigma)\, a_{1\tau\sigma(1)} \cdots a_{n\tau\sigma(n)} \right)$$

Nun gelt $a_{1\tau\sigma(1)} \cdots a_{n\tau\sigma(n)}$ aus

$a_{1\tau(1)} \cdots a_{n\tau(n)}$ dadurch hervor, daß

von den r-ten Faktor $a_{r\tau(r)}$ durch

$a_{r\tau(s)}$ und $a_{s\tau(s)}$ durch $a_{s\tau(r)}$ ersetzt.

Wegen der Gleichheit des s-ten und r-ten

Zeile ändert das nichts und die Beh.

folgt aus $\operatorname{sgn}(\tau\circ\sigma) = -\operatorname{sgn}(\tau)$. ⊠

Bsp 11.4 $n=2$, $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, dann

(a_{11}: a; a_{12}: b; a_{21}: c; a_{22}: d)

gilt

$$\det(A) = \operatorname{sgn}(\sigma)\, a_{1\sigma(1)} \cdot a_{2\sigma(2)} + \operatorname{sgn}(\tau)\, a_{1\tau(1)} \cdot a_{2\tau(2)}$$

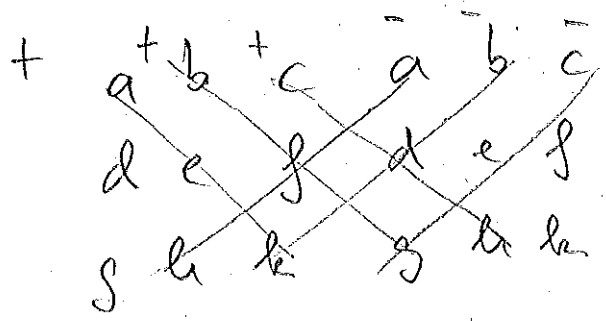
$$= ad - bc$$

$n=3$, $A = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & k \end{pmatrix}$, dann

gilt mit Leibnizscher Formel:

$$\det(A) = (aek + bfg + cdh) - (gec + hfa + kdb)$$

Merkregel: (Sarrus'sche Regel)



Für $n \geq 4$ gibt es keine so einfache Regeln, wie für $n = 2, 3$.

Sehr nützlich ist jedoch

Propo 11.5 Für obere Dreiecksmatrizen

$$\begin{pmatrix} \lambda_1 & & * \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} = A \text{ gilt}$$

$$\det(A) = \prod_{i=1}^{n} \lambda_i$$

Beweis Schreiben $A = (a_{ij})$ und betrachten

$$\det(A) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma)\, a_{1\sigma(1)} \cdots a_{n\sigma(n)}.$$

Das Produkt $a_{1\sigma(1)} \cdots a_{n\sigma(n)}$ verschwindet, es sei denn $\sigma(i) \geq i$ für alle $1 \leq i \leq n$.

Das gelt nur für $\sigma = \mathrm{id}$. Also

$$\det(A) = \operatorname{sgn}(\mathrm{id}) \cdot a_{11} \cdots a_{nn} = \prod_{i=1}^{n} a_{ii}. \qquad \square$$

Man kann mit Hilfe von Lemma 11.2 und Propo. 11.5 ebenfalls Determinanten ausrechnen!

Bsp 11.6 $A = \begin{pmatrix} 1 & 1 & 1 \\ 4 & 2 & 1 \\ 9 & 3 & 1 \end{pmatrix} \in \mathrm{Mat}_3(\mathbb{R})$.

$$\begin{pmatrix} 1 & 1 & 1 \\ 4 & 2 & 1 \\ 9 & 3 & 1 \end{pmatrix} \xleftarrow{(-4)} \text{I} \qquad \begin{pmatrix} 1 & 1 & 1 \\ 0 & -2 & -3 \\ 9 & 3 & 1 \end{pmatrix} \xleftarrow{(-9)} \text{II}$$

$$\begin{pmatrix} 1 & 1 & 1 \\ 0 & -2 & -3 \\ 0 & -6 & -8 \end{pmatrix} \xleftarrow{(-3)} \text{III} \qquad \begin{pmatrix} 1 & 1 & 1 \\ 0 & -2 & -3 \\ 0 & 0 & 1 \end{pmatrix}$$

Nach Lemma 11.2 ändern Schritte I, II und III an der Determinante von A nichts.

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

Propo. M.5

Wir wollen eine weitere Formel zur Berechnung der Determinante einer Matrix kennenlernen.

Sei $A \in Mat_n(K)$ eine Matrix, so bezeichne A_{ij} die aus A durch Weglassen der i-ten Zeile und j-ten Spalte entstehende $(n-1) \times (n-1)$ Matrix.

Bsp M.7 $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$, dann

ist $A_{13} = \begin{pmatrix} 4 & 5 \\ 7 & 8 \end{pmatrix}$

Propo 11.8 Sei $A=(a_{ij}) \in \mathrm{Mat}_n(K)$. Dann gilt

① $\det(A) = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \cdot \det A_{ij}$

② $\det(A) = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det A_{ij}$

Diese Formeln heißen Laplace-Entwicklung von det nach i-te Zeile bzw. j-ter Spalte.

Beweis Wir zeigen nur ①. ② geht genauso.

Wir müssen zeigen, daß die rechte Seite von ① die Eigenschaften (i), (ii) und (iii) hat. Beweis per Induktion nach n.

(i): Um Linearität in der k-ten Zeile von A nachzuweisen,

Zeigen wir, daß jeder einzelne Summand $(-1)^{i+j} a_{ij} \det A_{ij}$ linear in der k-ten Zeile ist.

Für $k \neq i$ folgt, daß

$$\det : \mathrm{Mat}_{(n-1)}(K) \longrightarrow K$$

linear in den Zeilen ist, während a_{ij} von der k-ten Zeile nicht abhängt.

Für $k = i$ hängt A_{ij} von der i-ten Zeile nicht ab (wird weggelassen).

Aber nun ist die Abb. $A \mapsto a_{ij}$ linear in der i-ten Zeile.

Also hat $\det$ die Eigenschaft (i).

(iii): Wir berechnen $\det(E)$:

$$\det(E) = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det E_{ij}$$

In der Summe auf der rechten Seite tritt nur ein einziger von Null verschiedener Summand auf, nämlich $(-1)^{i+j} \alpha_{ij} \det E_{ij}$.

Da $E_{ij} = E_{(n-1)}$ die Einheitsmatrix

$E_{(n-1)} \in Mat_{(n-1)}(K)$ ist folgt nach Induktionsvoraussetzung $\det E_{ij} = 1$. Also folgt

$\det E = 1$.

(ii): Sei nun $\operatorname{rang}(A) < n$. Dann gibt es eine Zeile, die aus den anderen linearkombiniert werden kann. Daraus folgt, daß man durch Zeilenoper. vom Typ II diese Zeile zu Null machen kann. Eine Matrix mit einer Null-Zeile hat Determinante Null.

Wir müssen zeigen, daß Zeilenop. vom Typ II das Ergebnis der Formel für det nicht ändert.

Wegen der bereits gezeigten Linearität, reicht es zu zeigen, daß die Determinante jede Matrix verschwindet, welche zwei gleiche Zeilen hat.

Nehmen wir an, die r-te und s-te Zeile von A sind gleich. Dann ist nach Induktionsvoraussetzung

$$\sum_{i=1}^{n} (-1)^{i+j} \alpha_{ij} \det A_{ij} = (-1)^{r+j} \alpha_{rj} \det A_{rj} + (-1)^{s+j} \alpha_{sj} \det A_{sj},$$

da alle anderen Summanden verschwinden. (die betreffenden A_{ij} haben zwei gleiche Zeilen)

Man sieht leicht, daß man

A_{rj} durch $|r-s|-1$ Zeilen[illegible]

vertauschungen in A_{sj} umgewandelt werden.

Da nach Induktionsannahme Zeilen-

vertauschungen bei $(n-1)\times(n-1)$ Matrizen

den Vorzeichenwechsel der Determinante

führen [illegible]:

$$\det(A) = (-1)^{r+j} a_{rj} \det A_{rj} + (-1)^{s+j} a_{sj} \det A_{sj}$$

$$\overset{\text{Ind.}}{=} (-1)^{r+j} a_{rj} \det A_{rj} +$$

$a_{rj} = a_{sj}$

$$(-1)^{s+j} a_{rj} (-1)^{r-s+1} \det A_{rj}$$

$$= \underbrace{\left((-1)^{r+j} + (-1)^{r+j+1}\right)}_{=0} a_{rj} \det A_{rj} = 0$$

□

Bsp 11.9 $A = \begin{pmatrix} 1 & 1 & 1 \\ 4 & 2 & 1 \\ 9 & 3 & 1 \end{pmatrix}$ aus Bsp 11.6.

Sei $j = 1$. Dann folgt aus Laplace-Entwicklung

$$\det(A) = \sum_{i=1}^{n} (-1)^{i+1} a_{i1} \det A_{i1}$$

$$= (-1)^{1+1} a_{11} \det \begin{pmatrix} 2 & 1 \\ 3 & 1 \end{pmatrix} +$$

$$(-1)^{2+1} a_{21} \det \begin{pmatrix} 1 & 1 \\ 3 & 1 \end{pmatrix} +$$

$$(-1)^{3+1} a_{31} \det \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}$$

$$= 1 \cdot \det \begin{pmatrix} 2 & 1 \\ 3 & 1 \end{pmatrix} - 4 \cdot \det \begin{pmatrix} 1 & 1 \\ 3 & 1 \end{pmatrix}$$

$$+ 9 \det \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}$$

Bsp. 11.4

$$= (2-3) - 4(1-3) + 9 \cdot (1-2)$$

$$= -1 + 8 - 9 = -2$$

Kommen wir nochmal zur Tatsache, daß $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Mat_2(K)$ invertierbar ist, genau dann, wenn $ad - bc \neq 0$.

Bsp. 11.4 zeigt $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$.

Also $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ invertierbar $\Leftrightarrow \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq 0$.

Das gilt ganz allgemein:

Prop. 11.10 Sei $A \in Mat_n(K)$. Dann ist A invertierbar genau dann, wenn $\det(A) \neq 0$.

Beweis „$\Rightarrow$" Sei A invertierbar. Dann ist $\operatorname{rang}(A) = n$. Durch Zeilenoperationen kann A in E umgewandelt werden. Aus $\det(E) = 1 \neq 0$ und Lemma 11.2 folgt $\det(A) \neq 0$.

„$\Leftarrow$" Angenommen A nicht invertierbar.
Dann folgt $\operatorname{rank}(A) < n$. Also
$\det(A) = 0$.

Propo 11.11 $A, B \in \mathrm{Mat}_n(K)$. Dann gilt
$$\det(AB) = \det(A) \cdot \det(B)$$

Beweis Wir halten B fest und betrachten die Abb.

$$f: \mathrm{Mat}_n(K) \longrightarrow K$$
$$A \longmapsto \det(A \cdot B)$$

Dann ist f linear in den Zeilen von A. Denn wenn man i-te Zeile von A ändert, so ändert das nur die i-te Zeile von AB.

Bei festgehaltenen übrigen Zeilen und

Festgehaltenem B ist also

$$K^n \longrightarrow K^n$$
$$(i\text{-te Zeile von } A) \longmapsto (i\text{-te Zeile von } AB)$$

linear. Ist nun $\operatorname{rank}(A) < n$, so auch $\operatorname{rank}(AB) < n$, da $\operatorname{Im}(AB) \subset \operatorname{Im}(A)$.

Also $\det(AB) = 0 = 0 \cdot \det(B)$
$= \det(A) \cdot \det(B)$.

Es gilt $f(E) = \det(EB) = \det(B)$. Falls $\det(B) \neq 0$, so hat die Abb

$$A \longmapsto (\det(B))^{-1} \det(AB)$$

die Eigenschaften (i), (ii), (iii) aus Propo. M.1. Also $(\det(B))^{-1} \det(AB) = \det(A)$.

Falls $\det(B) = 0$, so ist mit Propo 11.10 B nicht invertierbar, also $\operatorname{rank}(B) < n$.

Also dim $\ker(B) > 0$. Daraus folgt dass $\ker(AB) > 0$, da $\ker(B) \subset \ker(AB)$. Also $\operatorname{rank}(AB) < n$. Deshalb

$$\det(AB) = 0 = \det(A) \cdot 0 = \det(A) \cdot \det(B)$$

□

Korollar M.12 $A \in \mathrm{Mat}_n(K)$ invertierbar, so gilt

$$\det(A^{-1}) = (\det(A))^{-1}$$

Beweis $\det(AA^{-1}) = \det(E) = 1$,

also $\det(A) \cdot \det(A^{-1}) = 1$, d.h.

$$\det(A^{-1}) = \frac{1}{\det(A)}$$

□

Sei nun $f: V \to V$ linear und $\dim(V) = n$.

Betrachte folgendes Diagram: $A = \{a_1, \dots, a_n\}$ Basis von V

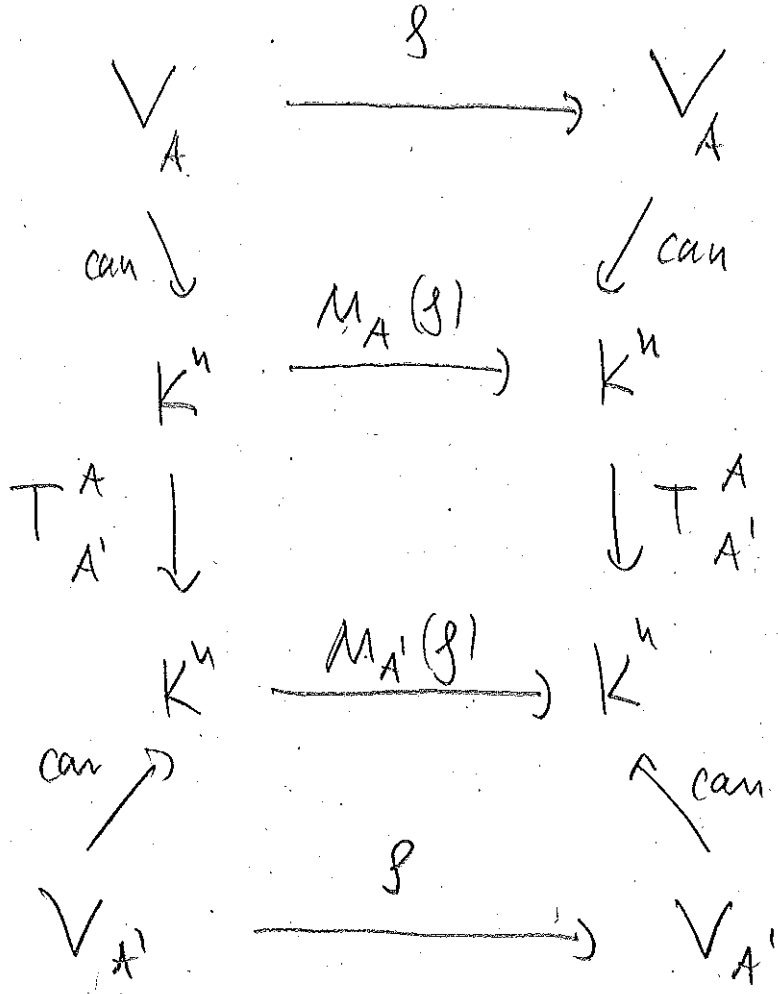
$$\begin{array}{ccc} V & \xrightarrow{f} & V \\ {\scriptstyle can}\downarrow & & \downarrow{\scriptstyle can} \\ K^n & \xrightarrow{M_A(f)} & K^n \end{array}$$

$M_A(f)$ ist Abbildungsmatrix von f bezgl. der Basis $a_1, \dots, a_n \in V$.

Lemma 11.13 Ist $f: V \to V$ linear und $A = \{a_1, \dots, a_n\}$ und $A' = \{a_1', \dots, a_n'\}$ Basen von V. Dann gilt

$$\det(M_A(f)) = \det(M_{A'}(f))$$

Beweis Wir erinnern an die Basiswechselmatrix. Haben folgendes Diagram



Lön wissen, daß $M_A(f) = \left(T^A_{A'}\right)^{-1} \cdot M_{A'}(f) \cdot T^A_{A'}$,

mit Propo. 11.11 folgt

$$\det\left(M_A(f)\right) = \left(\det\left(T^A_{A'}\right)\right)^{-1} \det\left(M_{A'}(f)\right) \det\left(T^A_{A'}\right)$$

$$= \det\left(M_{A'}(f)\right)$$

□

Def 11.14 Sei $f: V \to V$ linear und $A = \{a_1, \dots, a_n\}$ eine Basis von V. Dann

$$\det(f) := \det(M_A(f)).$$

Wir kommen nun zu einem interessanten Problem. Frage: Könnte man aus einer Matrix $A \in \mathrm{Mat}_n(K)$ die „Wurzel" ziehen?

Nehmen wir an $A \in \mathrm{Mat}_n(\mathbb{C})$ und

$$A = \begin{pmatrix} z_1 & & 0 \\ & \ddots & \\ 0 & & z_n \end{pmatrix}.$$

Dann erfüllt $B = \begin{pmatrix} \sqrt{z_1} & & 0 \\ & \ddots & \\ 0 & & \sqrt{z_n} \end{pmatrix}$

die Bedingung $B^2 = A$. Also hätte A eine „Wurzel".

Was macht man, wenn $A \in \mathrm{Mat}_n(\mathbb{C})$ beliebig?

Idee: Gäbe es invertierbare Matrix $T \in \mathrm{Mat}_n(\mathbb{C})$, so daß

$$T^{-1} A T = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} =: D,$$

so könnte man mit $\sqrt{D} := \begin{pmatrix} \sqrt{\lambda_1} & & 0 \\ & \ddots & \\ 0 & & \sqrt{\lambda_n} \end{pmatrix}$

folgendes erreichen.

$$\left(T \sqrt{D} T^{-1}\right)^2 = T \sqrt{D} T^{-1} T \sqrt{D} T^{-1}$$
$$= T \sqrt{D} \sqrt{D} T^{-1} = T D T^{-1} = A$$

Setzen wir also $B = T \sqrt{D} T^{-1}$, so gilt $B^2 = A$. Es stellt sich also die Frage, wann es solche T gibt?

Das führt auf den Begriff der Diagonalisierbarkeit einer Matrix $A \in Mat_n(K)$.

§ 12

Eigenwerte, Eigenvektoren, Diagonalisierbarkeit

Def 12.1 Eine Matrix $A \in Mat_n(K)$ heißt diagonalisierbar, wenn sie zu einer Matrix der Gestalt

$$\begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$$

ähnlich ist.

Lemma 12.2 Ist A die Abbildungsmatrix von $f: V \to V$ bezüglich einer Basis

$v_1, \dots, v_n \in V$, so hat A die Gestalt

$$A = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$$

genau dann, wenn $f(v_i) = \lambda_i v_i$, für $i = 1, \dots, n$.

Beweis: Betrachten das Diagram

$$\begin{array}{ccc} V & \xrightarrow{f} & V \\ {\scriptstyle can}\downarrow & & \downarrow{\scriptstyle can} \\ K^n & \xrightarrow{A} & K^n \end{array}$$

„$\Leftarrow$" Sei $f(v_i) = \lambda_i v_i$, dann hat A die Gestalt $\begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$.

„$\Rightarrow$" Sei nun $A = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$, dann

gilt

$$f(v_i) = \text{can}^{-1}\left(A \cdot \text{can}(v_i)\right)$$
$$= \text{can}^{-1}\left(A \cdot e_i\right)$$
$$= \text{can}^{-1}\left(\lambda_i e_i\right) = \lambda_i \cdot \text{can}^{-1}(e_i)$$
$$= \lambda_i v_i$$

□

Dies führt auf folgende Definition:

Def 12.3 Sei V ein K-VR und $f: V \to V$ linear. Unter einem **Eigenvektor** von f zum **Eigenwert** $\lambda \in K$ versteht man einen Vektor $v \neq 0$ mit $f(v) = \lambda v$.

Lemma 12.4 Ein Vektor $v \in V \setminus \{0\}$ ist genau dann Eigenvektor von $f: V \to V$ zum Eigenwert $\lambda \in K$, wenn $v \in \text{Ke}(f - \lambda \cdot \text{id})$.

Beweis $f(v) = \lambda v$ bedeutet

$f(v) - \lambda v = 0$ und wegen der Linearität gilt

$f(v) - \lambda v = (f - \lambda id)(v)$.

Also ist $v \in \ker(f - \lambda id)$.

□

Def 12.5 Ist $\lambda \in K$ ein Eigenwert von $f: V \to V$, so heißt

$E_\lambda = \ker(f - \lambda id)$

Eigenraum von f zu λ.

Die Zahl $\dim E_\lambda$ heißt geometrische Vielfachheit.

Lemma 12.6 Sind $v_1, \dots, v_r$ Eigenvektoren von f zu Eigenwerten $\lambda_1, \dots, \lambda_r$ mit gilt $\lambda_i \neq \lambda_j$ für $i \neq j$, so sind $v_1, \dots, v_r$ linear unabhängig.

Beweis Induktion nach r.

Für $r = 1$ ist v_1 linear unabhängig, da $v_1 \neq 0$ nach Voraussetzung.

Nehmen an, die Aussage stimmt für $r = k$.

Seien $v_1, \dots, v_{k+1}$ Eigenvektoren zu Eigenwerten $\lambda_1, \dots, \lambda_{k+1}$, $\lambda_i \neq \lambda_j$ für $i \neq j$ und sei

$$\alpha_1 v_1 + \dots + \alpha_{k+1} v_{k+1} = 0.$$

Dann ist

$$\alpha_1 \lambda_{k+1} v_1 + \dots + \alpha_{k+1} \lambda_{k+1} v_{k+1} = 0. \quad (*)$$

Anwendung von f liefert:

$$\alpha_1 f(v_1) + \dots + \alpha_{k+1} f(v_{k+1}) = 0 \text{ , d.h.}$$

$$\alpha_1 \lambda_1 v_1 + \dots + \alpha_{k+1} \lambda_{k+1} v_{k+1} = 0 \qquad (**)$$

Subtrahiert man $(*)$ von $(**)$ so erhält man

$$\alpha_1 (\lambda_1 - \lambda_{k+1}) v_1 + \dots + \alpha_k (\lambda_k - \lambda_{k+1}) v_k = 0.$$

Nach Induktionsvoraussetzung folgt

$$\alpha_1 (\lambda_1 - \lambda_{k+1}) = \dots = \alpha_k (\lambda_k - \lambda_{k+1}) = 0.$$

Wegen $\lambda_i \neq \lambda_j$, folgt

$$\alpha_1 = \dots = \alpha_k = 0,$$

also auch $\alpha_{k+1} = 0$.

□

Bemerkung 12.7 Aus 12.6 folgt auch folgendes: Es gibt nur endlich viele verschiedene Eigenwerte zu $f: V \to V$, wenn $\dim(V) = n$.

Gäbe es nämlich unendlich viele verschiedene Eigenwerte, so gäbe es eine Folge $v_1, v_2, \ldots, \ldots$ von linear unabhängigen Vektoren. Dann aber $\dim(V) = \infty$.

Propo 12.8 Sei $\dim(V) = n$ und $f: V \to V$ linear. Seien $\lambda_1, \ldots, \lambda_r$ die verschiedenen Eigenwerte und $\mu_1, \ldots, \mu_r$ deren geometrische Vielfachheiten.

Sei $v_1^{(i)}, \dots, v_{n_i}^{(i)}$ eine Basis von E_{n_i}. Dann sind

$$v_1^{(1)}, \dots, v_{n_1}^{(1)}, v_1^{(2)}, \dots, v_{n_2}^{(2)}, \dots, v_1^{(r)}, \dots, v_{n_r}^{(r)}$$

linear unabhängig. Insbesondere ist $\sum_{i=1}^{r} n_i \leq n$. f ist diagonalisierbar genau dann, wenn $\sum_{i=1}^{r} n_i = n$.

Beweis Sei

$$\sum_{i=1}^{r} \sum_{k=1}^{n_i} \alpha_k^{(i)} v_k^{(i)} = 0 \,,$$

so sind nach Lemma 12.6 gerade

$$\sum_{k=1}^{n_i} \alpha_k^{(i)} v_k^{(i)} = 0$$

und wegen $v_1^{(i)}, \dots, v_{n_i}^{(i)}$ linear

unabhängig, gilt $\alpha_1^{(i)} = \dots = \alpha_{n_i}^{(i)} = 0$.

Durch Aneinanderreihung von Basen der Eigenräume E_{λ_i} entsteht so ein linear unabhängiges $(n_1 + \dots + n_r)$-Tupel von Eigenvektoren. Falls $\sum_{i=1}^{r} n_i = n$, erhalten wir aus Dimensionsgründen eine Basis aus Eigenvektoren.

Ist nun umgekehrt f diagonalisierbar und seien m_i die Anzahl der Eigenvektoren zu λ_i, so ist offenbar $m_i \leq n_i$. Daher gilt

$$n = \sum_{i=1}^{r} m_i \leq \sum_{i=1}^{r} n_i \leq n.$$

Also $m_i = n_i$.

□

Wir sehen, wie vorgehen müssen, um eine Basis von Eigenvektoren zu finden.

1. Schritt: Man sucht alle $\lambda \in K$, für die $\ker(f - \lambda \cdot id) \neq 0$, oder äquivalent davon, für die $\det(f - \lambda \cdot id) \neq 0$.

2. Schritt: Seien $\lambda_1, \ldots, \lambda_r$ alle Eigenwerte. Dann bestimme man eine Basis $v_1^{(i)}, \ldots, v_{n_i}^{(i)}$ von E_{λ_i}.

3. Schritt: Die Aneinanderreihung dieser Basen ist die gesuchte Basis aus Eigenvektoren.

Hier bei stellen sich zwei praktische Probleme.

1.) Wie berechnet man alle Eigenwerte?

2) Wie berechnet man eine Basis von E_λ, wenn λ Eigenwert.

zu 1): Die Suche nach den Eigenwerten lässt sich zurückführen auf die Suche nach den Nullstellen der Abb. $K \to K$,

$$\lambda \longmapsto \det(f - \lambda \cdot id).$$

Wir werden sehen, dass diese Abb durch ein Polynom beschrieben wird.

Sei also $f: V \to V$ linear und $A = \{a_1, \dots, a_n\}$ eine Basis von V.

Sei nun T eine Unbestimmte, so definieren wir

$$\chi_f(T) = \det(M_A(f) - T \cdot E)$$

$$= \det \begin{pmatrix} a_{11} - T & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} - T & \cdots & \vdots \\ \vdots & & & \\ a_{n1} & \cdots & & a_{nn} - T \end{pmatrix}$$

Bsp 12.3 $M_A(f) = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 3 \\ 2 & 1 & 1 \end{pmatrix}$, dann

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

$$= (-1)^3 (T-1)^3 + 3(T-1) + 12 .$$

Wir sehen, $\chi_f(T)$ ist ein Polynom in T.

Dies ist kein Zufall!

Wir schauen uns $\chi_f(T)$ an.

Aus Leibnizsche Formel für die Determinante ergibt sich

$$\chi_f(T) = (\alpha_{11} - T) \cdots (\alpha_{nn} - T) + Q,$$

wobei der erste Summand zu $\sigma = id \in S_n$ gehört und Q die restliche Summe über $S_n \setminus \{id\}$ ist. Da in einem Summanden von Q als Faktoren höchstens $n-2$ Diagonalkomponenten auftreten können, ist Q ein Polynom von Grad $\leq n-2$.

Da formal gelten

$$(f - T \cdot id)(a_i) = f(a_i) - T a_i =$$

$$= (\alpha_{1i} a_1 + \cdots + (\alpha_{ii} - T \cdot 1) \cdot a_i + \cdots + \alpha_{ni} a_n$$

ist $M_A(f) - TE$ die Abbildungsmatrix

Da f - T.id. Aus Lemma 11.13 folgt, daß für weitere Basis $A' = \{q_1', \dots, q_n'\}$ folgendes gilt:

$$\det(M_A(f) - T \cdot E) = \det(M_{A'}(f) - T E).$$

Das rechtfertigt folgende Definition.

Def 12.10 Sei $f: V \to V$ linear mit $\dim(V) = n$. Sei $A = \{q_1, \dots, q_n\}$ eine Basis von V. Dann heißt

$$\chi_f(T) = \det(M_A(f) - T E)$$

das charakteristische Polynom von f.

Es gilt: $\deg(\chi_f(T)) = n$.

Man sieht, daß die Nullstellen von $\chi_f(T)$ die Eigenwerte von f sind.

Bevor wir zu 2), der Berechnung einer Basis von E_λ, kommen, werden wir an einem Beispiel erklären, wie man entscheidet, ob f diagonalisierbar ist.

Hier ist zunächst das Rezept:

1) $\chi_f(T)$ bestimmen und die Nullstellen $\lambda_1, \dots, \lambda_r$ berechnen.

2) $\dim E_{\lambda_i}$ mit Gauß-Algorithmus bestimmen.

3) Falls $\sum_{i=1}^{r} \dim E_{\lambda_i} = n$, so ist f diagonalisierbar.

Bsp 12.11 Sei $A = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 2 & 3 \\ 5 & 0 & 4 \end{pmatrix}$, aufgefasst als lineare Abb. $A: \mathbb{R}^3 \to \mathbb{R}^3$ bzgl. der Basis e_1, e_2, e_3.

1) $\chi_A(T) = \det \begin{pmatrix} 3-T & 0 & 0 \\ 0 & 2-T & 3 \\ 5 & 0 & 4-T \end{pmatrix}$

$= (3-T)(2-T)(4-T)$

Die Nullstellen sind $\lambda_1 = 3$, $\lambda_2 = 2$, $\lambda_3 = 4$.

2) Betrachte

$$A - \lambda_1 E = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 2-3 & 3 \\ 5 & 0 & 4-3 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & -1 & 3 \\ 5 & 0 & 1 \end{pmatrix}$$

$\operatorname{rank}(A - \lambda_1 E) = 2$, also $\dim E_{\lambda_1} = 1$.

$$A - \lambda_2 E = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 3 \\ 5 & 0 & 2 \end{pmatrix}.$$ Dann

gilt $\operatorname{rank}(A - \lambda_2 E) = 2$, also

$\dim E_{\lambda_2} = 1$.

analog für E_{η_3}.

3) Es gilt $\sum_{i=1}^{3} \dim E_{\eta_i} = 3$. Also ist

A diagonalisierbar.

Ganz allgemein gilt:

Propo 12.12 Sei $f: V \to V$ linear mit $\dim(V) = n$. Seien $\eta_1, \dots, \eta_n$ die verschiedenen Eigenwerte. Dann ist f diagonalisierbar.

Beweis Da $\det(f - \eta_i \mathrm{id}) = 0$ gilt $\dim E_{\eta_i} \geq 1$. Wir wissen $\sum_{i=1}^{n} \dim E_{\eta_i} \leq n$. Also

$$\sum_{i=1}^{n} \dim E_{\eta_i} = n.$$

□

Welcher Zusammenhang besteht zwischen Diagonalisierbarkeit und charakteristischem Polynom?

Nehmen wir an $\chi_f(T)$ hat keine Nullstelle in K. Dann gibt es keinen Eigenwert, keinen Eigenvektor und somit ist f <u>nicht</u> diagonalisierbar.

Nehmen wir an $\chi_f(T) = (\lambda_1 - T)^{m_1} \cdots (\lambda_r - T)^{m_r}$.

Dann sind $\lambda_1, \ldots, \lambda_r$ die Eigenwerte.

Die Zahlen $m_1, \ldots, m_r$ nennt man <u>algebraische Vielfachheiten</u> der λ_i.

Es gilt nun folgender Zusammenhang.

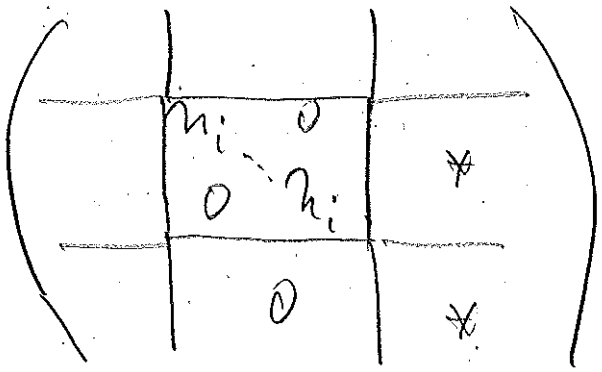
Propo 12.13 Sei $f: V \to V$ linear und $\dim(V) = n$. Sei

$$\chi_f(T) = (\lambda_1 - T)^{\mu_1} \cdots (\lambda_r - T)^{\mu_r}.$$

Dann gilt $\mu_i \geq \dim E_{\lambda_i}$.

Ist $\mu_i = \dim E_{\lambda_i}$ für $i = 1, \ldots, r$, so ist f diagonalisierbar.

Beweis Sei $v_1^{(i)}, \ldots, v_{\mu_i}^{(i)}$ eine Basis von E_{λ_i}, so hat Abb.-matrix von f bzgl. dieser Basis die Gestalt



Deshalb kommt in der

Linearfaktorzerlegung von $\chi_f(T)$ da Faktor $(\lambda_i - T)$ mindestens dim E_{λ_i} mal vor. Da $\sum_{i=1}^{r} m_i = n$ folgt im Fall $m_i = \dim E_{\lambda_i}$ gerade $\sum_{i=1}^{r} \dim E_{\lambda_i} = n$. Also war f diagonalisierbar. ☐

Es kann sein, daß eine Matrix $A \in \mathrm{Mat}_n(K)$ über K nicht diagonalisierbar ist, über einem Erweiterungskörper $K \subset L$ jedoch schon!

Bsp 12.14 Sei $A = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & -1 \\ 0 & 1 & 1 \end{pmatrix} \in \mathrm{Mat}_3(\mathbb{R})$.

Dann gilt $\chi_A(T) = (1-T)(T^2+1)$.

Im $\mathbb{R}$ hat $\chi_A(T)$ nur die Nullstelle

$\lambda = 1$. Es gilt

$$A - \lambda E = \begin{pmatrix} -1 & 0 & 1 \\ 1 & -1 & -1 \\ 0 & 1 & 0 \end{pmatrix}, \text{ also}$$

$\operatorname{rank}(A - E) = 2$, d.h. $\dim E_\lambda = 1 \neq 3$.

Also ist A über $\mathbb{R}$ nicht diagonalisierbar.

Betrachten wir $A \in \operatorname{Mat}_3(\mathbb{C})$, so ist

$$\begin{aligned} \chi_A(T) &= (1-T)(T+i)(T-i) \\ &= (1-T)(-i-T)(i-T), \end{aligned}$$

also sind $\lambda_1 = 1$, $\lambda_2 = i$, $\lambda_3 = -i$ die 3 Eigenwerte. Nach Prop. 12.12 ist A über $\mathbb{C}$ diagonalisierbar!

Wir wollen den Zusammenhang zum Basiswechsel verstehen.

Sei $A \in \mathrm{Mat}_n(K)$ und betrachte

Basiswechsel diagram: $B = \{e_1, \dots, e_n\}$,

$$\begin{array}{ccc} K^n & \xrightarrow{D} & K^n \\ {\scriptstyle T^{B'}_{B}}\downarrow & & \downarrow{\scriptstyle T^{B'}_{B}} \\ K^n & \xrightarrow{A} & K^n \end{array}$$

Dann gilt $D = \left(T^{A'}_{A}\right)^{-1} A \, T^{A'}_{A}$. Wir suchen eine Basis $B' = \{v_1, \dots, v_n\}$ aus Eigenvektoren. Dann ist D von der Gestalt

$$D = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix},$$

wobei λ_i nicht notwendigerweise verschieden. Die Matrix $T^{B'}_{B}$ ist von der Gestalt

$$T_B^{B'} = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ \vdots & \vdots & & \vdots \\ \alpha_{n1} & \alpha_{n2} & \cdots & \alpha_{nn} \end{pmatrix}, \text{ wobei}$$

$$v_i = \begin{pmatrix} \alpha_{1i} \\ \vdots \\ \alpha_{ni} \end{pmatrix}.$$

Wenn wir also die Eigenvektoren kennen, können wir auch die Basiswechselmatrix $T_B^{B'}$ angeben.

Bestimmung einer Basis von E_λ:

Sei λ ein Eigenwert von $f: V \to V$, dann $(V) = n$. Wähle Basis $A = \{a_1, \ldots, a_n\}$ und betrachte $M_A(f) - \lambda \cdot E$:

Basis von $\ker(M_A(f) - \lambda \cdot E)$ ermittelt man mit Gauß-Algorithmus.

Bsp 12.15

Sei $A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 2 & 0 \\ 1 & 0 & 1 \end{pmatrix} \in Mat_3(\mathbb{R})$. Wir fassen $A : \mathbb{R}^3 \to \mathbb{R}^3$ als lineare Abb auf, Basis ist $e_1, e_2, e_3 \in \mathbb{R}^3$.

1) $\chi_A(T) = (2-\lambda)^2(-\lambda) = -\lambda(2-\lambda)^2$.

Die Eigenwerte sind also $\lambda_1 = 0$, $\lambda_2 = 2$.

2) $\lambda_1 = 0$: $A - 0 \cdot E = A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 2 & 0 \\ 1 & 0 & 1 \end{pmatrix}$.

$$\left(\begin{pmatrix} 1 & 0 & 1 \\ 0 & 2 & 0 \\ 1 & 0 & 1 \end{pmatrix} \right] (-1) \quad \left(\begin{array}{c|c|c} 1 & 0 & 1 \\ \hline 0 & 2 & 0 \\ \hline 0 & 0 & 0 \end{array} \right)$$

$$Ker(A) = \left\{ \begin{pmatrix} -\alpha_3 \\ 0 \\ \alpha_3 \end{pmatrix} \mid \alpha_3 \in \mathbb{R} \right\} = \left\langle \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix} \right\rangle.$$

$\lambda_2 = 2$: $A - 2E = \begin{pmatrix} -1 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & -1 \end{pmatrix}$

$$\begin{pmatrix} -1 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & -1 \end{pmatrix} \overset{(1)}{\rightsquigarrow} \left(\begin{array}{ccc} -1 & 0 & 1 \\ \hline 0 & 0 & 0 \\ 0 & 0 & 0 \end{array}\right), \text{ also}$$

$$\ker(A-2E) = \left\{ \begin{pmatrix} \alpha_3 \\ \alpha_2 \\ \alpha_3 \end{pmatrix} \mid \alpha_3, \alpha_2 \in \mathbb{R} \right\}$$

$$= \left\langle \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\rangle.$$

3) Wir sehen, daß A diagonalisierbar ist. $A' = \left\{ \begin{pmatrix} 1 \\ 0 \\ -1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\}$ ist Basis aus Eigenvektoren. Somit

$$T_A^{A'} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & 1 & 0 \end{pmatrix}.$$ Wir rechnen nach:

$$\left(T_A^{A'}\right)^{-1} = \begin{pmatrix} \frac{1}{2} & 0 & -\frac{1}{2} \\ \frac{1}{2} & 0 & \frac{1}{2} \\ 0 & 1 & 0 \end{pmatrix}$$

Dann gilt

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

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

$$\begin{pmatrix} \boxed{0} & 0 & 0 \\ 0 & \boxed{2} & 0 \\ 0 & 0 & \boxed{2} \end{pmatrix}.$$

§13
Euklidische Vektorräume

Def 13.1 Sei V ein $\mathbb{R}$-Vektorraum. Ein <u>Skalarprodukt</u> auf V ist eine Abb.

$$V \times V \longrightarrow \mathbb{R},$$
$$(x,y) \longmapsto \langle x,y\rangle$$

mit folgenden Eigenschaften:

1) <u>Bilinearität</u>: Für jedes $x \in V$ sind die Abb.

$\langle -, x\rangle : V \to \mathbb{R}$, $v \mapsto \langle v, x\rangle$ und

$\langle x, -\rangle : V \to \mathbb{R}$, $v \mapsto \langle x, v\rangle$

linear.

2) <u>Symmetrie</u>: Es gilt $\langle x,y\rangle = \langle y,x\rangle$ für alle $x,y \in V$

3) <u>positive Definitheit</u>: Es gilt $\langle x,x\rangle > 0$ für alle $x \neq 0$.

Def 13.2 Unter einem euklidischen Vektorraum versteht man ein Paar $(V, \langle -,- \rangle)$, bestehend aus einem $\mathbb{R}$-VR V und einem Skalarprodukt auf V.

Bsp 13.3 Standardskalarprodukt:

$V = \mathbb{R}^n$ und dann ist

$$\langle -,- \rangle : \mathbb{R}^n \times \mathbb{R}^n \longrightarrow \mathbb{R},$$

$$(x, y) \longmapsto x_1 y_1 + x_2 y_2 + \dots + x_n y_n,$$

wobei $x = (x_1, \dots, x_n)$, $y = (y_1, \dots, y_n)$.

Man rechnet nach, daß diese Abb. ein Skalarprodukt ist.

Bsp 13.4 $V = \{ f : [-1,1] \to \mathbb{R} \mid f \text{ stetig} \}$.

Dann ist

$$V \times V \longrightarrow \mathbb{R}, \qquad (f,g) \longmapsto \langle f,g\rangle = \int_{-1}^{1} f(x)\,g(x)\,dx$$

ein Skalarprodukt auf V.

1) Bilinearität: $g(x)$ fest, dann gilt

$$\begin{aligned}
\langle f+h, g\rangle &= \int_{-1}^{1} (f+h)(x)\,g(x)\,dx \\
&= \int_{-1}^{1} \big(f(x)+h(x)\big)\,g(x)\,dx \\
&= \int_{-1}^{1} \big(f(x)g(x)+h(x)g(x)\big)\,dx \\
&= \int_{-1}^{1} f(x)g(x)\,dx + \int_{-1}^{1} h(x)g(x)\,dx \\
&= \langle f,g\rangle + \langle h,g\rangle .
\end{aligned}$$

analog $\langle f, g+h\rangle = \langle f,g\rangle + \langle f,h\rangle$.

2) $$\langle f,g\rangle = \int_{-1}^{1} f(x)\,g(x)\,dx = \int_{-1}^{1} g(x)\,f(x)\,dx$$

$$= \langle g,f\rangle .$$

3) positive Definitheit: Aus ANA I folgt

$$\langle f, f\rangle = \int_{-1}^{1} f(x) f(x)\,dx = \int_{-1}^{1} f(x)^2\,dx > 0,$$

falls $f \neq 0$.

Sei $(V, \langle -,- \rangle)$ ein euklidischer VR und $x \in V$. Die Zahl $\|x\| = \sqrt{\langle x, x\rangle} \in \mathbb{R}$, $\|x\| \geq 0$ heißt Norm von $x \in V$.

Propo 13.5 (Cauchy-Schwarz Ungleichung)
Sei $(V, \langle -,- \rangle)$ ein euklidischer VR. Dann gilt $|\langle x, y\rangle| \leq \|x\| \|y\|$ für alle $x, y \in V$.

Beweis. Für $y = 0$ ist die Aussage trivial. Es gilt dann

$$|\langle x, 0\rangle| = |0| = 0 \leq \|x\| \cdot 0.$$

Sei nun $y \neq 0$. Setze

$$\eta := \frac{\langle x, y\rangle}{\|y\|^2}.$$ Dann

Bilinearität

$$\downarrow$$

$$0 \leq \langle x-\lambda y, x-\lambda y\rangle = \langle x,x\rangle - 2\lambda\langle x,y\rangle + \lambda^2\langle y,y\rangle$$

$$= \|x\|^2 - 2\frac{\langle x,y\rangle^2}{\|y\|^2} + \frac{\langle x,y\rangle^2}{\|y\|^2}$$

$$= \|x\|^2 - \frac{\langle x,y\rangle^2}{\|y\|^2}$$

Also gilt $\langle x,y\rangle^2 \leq \|x\|^2\|y\|^2$, d.h.

$|\langle x,y\rangle| \leq \|x\|\,\|y\|$.

□

Propo 13.6 Sei V ein euklidischer VR, so hat die Norm $\|\cdot\| : V \to \mathbb{R}$, folgende Eigenschaften:

(i) $\|x\| \geq 0$ für alle $x \in V$

(ii) $\|x\| = 0 \iff x = 0$

(iii) $\|\lambda x\| = |\lambda|\,\|x\|$ für alle $x \in V$, $\lambda \in \mathbb{R}$

(iv) $\|x+y\| \leq \|x\| + \|y\|$ für alle $x, y \in V$.

↑ heißt man Dreiecksungleichung.

Beweis (i) – (iii) ergeben sich direkt aus der Definition.

Zu (iv): Es gilt

$$(\|x\| + \|y\|)^2 = \|x\|^2 + 2\|x\|\|y\| + \|y\|^2$$

$$\overset{\text{Cauchy-Schwarz}}{\geq} \|x\|^2 + 2\langle x, y\rangle + \|y\|^2 = \|x+y\|^2$$

□

Def 13.7 Sei $(V, \langle \cdot, \cdot \rangle)$ ein euklidischer VR und $x, y \in V$, $x \neq 0$, $y \neq 0$. Man definiert den Winkel α zwischen x und y durch

$$\cos(\alpha) = \frac{\langle x, y \rangle}{\|x\| \, \|y\|}, \quad 0 \leq \alpha \leq \pi.$$

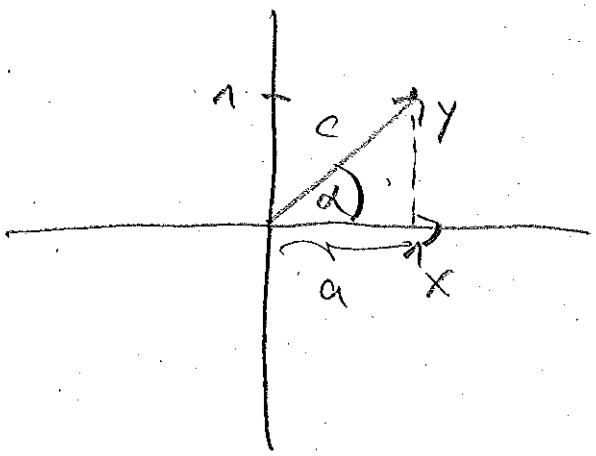
Wegen Cauchy-Schwarz gilt

$$-1 \leq \frac{\langle x, y \rangle}{\|x\| \, \|y\|} \leq 1$$

Bsp 13.8 $V = \mathbb{R}^2$ mit Standardskalarprodukt. Sei $x = (1,0)$ und $y = (1,1)$. Dann gilt

$$\cos(\alpha) = \frac{\langle x, y \rangle}{\|x\| \, \|y\|} = \frac{1}{1 \cdot 2} = \frac{1}{2},$$

also $\alpha = 45°$.



Hier gilt $\frac{a}{c} = \cos(\alpha)$. Nun ist

$a = \|x\|$ und $c = \|y\|$, also $\cos(\alpha) = \frac{\|x\|}{\|y\|}$.

Da $\langle x, x\rangle = \langle x, y\rangle = \|x\|^2$, folgt

$$\cos(\alpha) = \frac{\langle x, y\rangle}{\|x\|\,\|y\|}$$

Def 13.9 Sei $(V, \langle\cdot,\cdot\rangle)$ euklidischer VR und $x, y \in V$. Die Vektoren x und y heißen <u>orthogonal</u>, falls $\langle x, y\rangle = 0$.

(In der Tat gilt dann für $x, y \neq 0$:

$\cos(\alpha) = 0$, also $\alpha = 90°$ /

Def 13.10 Sei $(V, \langle -,- \rangle)$ ein euklidischer VR. Eine Orthonormalbasis $(v_i)_{i \in I}$ ist eine Basis von V mit folgenden Eigenschaften:

(i) $\|v_i\| = 1$ für alle $i \in I$

(ii) $\langle v_i, v_j \rangle = 0$ für $i \neq j$.

Bsp. 13.11 Sei $V = \mathbb{R}^4$ mit Standardskalarprodukt. Dann bilden $e_1, \dots, e_4$ eine Orthonormalbasis. Es gilt

$\|e_i\| = 1$ und

$\langle e_i, e_j \rangle = 0$, $i \neq j$.

Frage: Besitzt jeder euklidische VR eine Orthonormalbasis?

Antwort: Ja! Wir werden das im folgenden zeigen.

Lemma 13.12 Ist $v_1, \dots, v_n$ eine Orthonormalbasis von V, so gilt für jedes $v \in V$

$$v = \sum_{i=1}^{n} \langle v, v_i \rangle v_i$$

Beweis Es gilt $v = c_1 v_1 + \dots + c_n v_n$.

Dann folgt:

$$\langle v, v_i \rangle = \langle c_1 v_1, v_i \rangle + \dots + \langle c_n v_n, v_i \rangle$$

$$= \langle c_i v_i, v_i \rangle = c_i \langle v_i, v_i \rangle = c_i$$

□

Lemma 13.13 Es seien $v_1, \dots, v_r$ Vektoren mit $\|v_i\| = 1$ und $\langle v_i, v_j \rangle = 0$, $i \neq j$ in einem VR V mit $r \leq \dim(V)$.

Dann lässt sich jeder Vektor $v \in V$ auf genau eine Weise als Summe $v = u + w$ mit $u \in \langle v_1, \dots, v_r \rangle = U$, $w \in \langle v_1, \dots, v_r \rangle^\perp = \{ x \in V \mid \langle x, v_i \rangle = 0 \text{ für alle } i \}$ schreiben. Präziser:

$$u = \sum_{i=1}^{r} \langle v, v_i \rangle v_i \quad \text{und} \quad w = v - u.$$

<u>Beweis</u> Dass sich v auf höchstens eine Weise als Summe $v = u + w$ schreiben lässt ergibt sich aus der positiven Definitheit. Denn aus $v = u + w = u' + w'$, mit $u, u' \in U$ und $w, w' \in U^\perp$ folgt $(u - u') + (w - w') = 0$ und $\langle u - u', w - w' \rangle = 0$, also $\langle u - u', u - u' \rangle = 0$ und daher

$u - u' = 0$. Somit auch $w - w' = 0$.

Setze $u = c_1 v_1 + \dots + c_r v_r$.

Wenn rechnet noch, daß für die Koeffizienten c_i, für welche $w := v - u \in U^\perp$ gelten soll, folgendes gilt: $\langle v, v_i \rangle = c_i$.

Wenn nämlich $\langle w, v_i \rangle = 0$ für $i = 1, \dots, r$, so folgt

$$\langle v - u, v_i \rangle = \langle v, v_i \rangle - \langle u, v_i \rangle = 0$$

Also $\langle v, v_i \rangle = \langle u, v_i \rangle = c_i$.

□

Theorem 13.14 (Schmidtsches Orthonormalisierungsverfahren)

Sind $v_1, \dots, v_r$ linear unabhängig in V,

so ist durch

$$\tilde{v}_1 = \frac{v_1}{\|v_1\|}, \quad \tilde{v}_{k+1} = \frac{v_{k+1} - \sum_{i=1}^{k} \langle v_{k+1}, \tilde{v}_i \rangle \tilde{v}_i}{\| v_{k+1} - \sum_{i=1}^{k} \langle v_{k+1}, \tilde{v}_i \rangle \tilde{v}_i \|}$$

ein System von Vektoren gegeben, für die $\|\tilde{v}_i\| = 1$ und $\langle \tilde{v}_i, \tilde{v}_j \rangle = 0$, $i \neq j$. Außerdem sind $\tilde{v}_1, \ldots, \tilde{v}_r$ linear unabhängig

Beweis Folgt aus Lemma 13.13. mit anschließender Normierung. Die lineare Unabhängigkeit rechnet man nach □

Korollar 13.15 Jede endlichdimensionale VR V mit $\dim(V) = n$ besitzt eine Orthonormalbasis.

Beweis Sei $v_1, \ldots, v_n \in V$ Basis. Wende Theorem 13.14 an. □

Def 13.16 Seien V, W euklidische $\mathbb{R}$-VR. Eine lineare Abb $f: V \to W$ heißt orthogonal, wenn $\langle f(v), f(w) \rangle = \langle v, w \rangle$ für alle $v, w \in V$.

Def 13.17 Es sei $(V, \langle -,- \rangle)$ ein euklidischer Vektorraum. Eine lineare Abb. $f: V \to V$ heißt selbstadjungiert, wenn

$$\langle f(v), w \rangle = \langle v, f(w) \rangle$$

für alle $v, w \in V$.

Lemma 13.18 Seien v, w Eigenvektoren einer selbstadjungierten Abb $f: V \to V$ zu Eigenwerten $\lambda \neq \mu$, so gilt $\langle v, w \rangle = 0$

Beweis $\langle f(v), w\rangle = \langle \lambda v, w\rangle = \lambda \langle v, w\rangle$

$= \langle v, f(w)\rangle = \langle v, \mu w\rangle =$

$= \mu \langle v, w\rangle$.

Also $(\lambda - \mu)\langle v, w\rangle = 0$. ∎

Ist $(V, \langle -,- \rangle)$ ein euklidischer VR und $(v_1, \ldots, v_n)$ eine Orthonormalbasis, so ist die Abbildungsmatrix von $f: V \to V$ gegeben durch:

$$A = (\alpha_{ij}), \quad \alpha_{ij} = \langle v_i, f(v_j)\rangle.$$

Da folgt aus Satz 13.12. Es gilt nämlich

$$f(v_j) = \sum_{i=1}^{n} \langle f(v_j), v_i\rangle v_i$$

$$\overset{\text{Symmetrie von } \langle -,- \rangle}{=} \sum_{i=1}^{n} \langle v_i, f(v_j)\rangle v_i$$

Korollar 13.19 Ist $v_1, \dots, v_n$ Orthonormalbasis von V, so ist $f: V \to V$ selbstadjungiert genau dann, wenn die Abbildungsmatrix A bzgl. $v_1, \dots, v_n$ symmetrisch ist, d.h. $\alpha_{ij} = \alpha_{ji}$.

Beweis „$\Rightarrow$" Es gilt

$$\alpha_{ij} = \langle v_i, f(v_j) \rangle = \langle f(v_i), v_j \rangle$$

$$\overset{\text{Symmetrie}}{=} \langle v_j, f(v_i) \rangle$$

$$= \alpha_{ji}$$

„$\Leftarrow$" A symmetrisch, also

$$\alpha_{ij} = \langle v_i, f(v_j) \rangle = \alpha_{ji} = \langle v_j, f(v_i) \rangle$$

$$= \langle f(v_i), v_j \rangle$$

Also ist f selbstadjungiert auf Basiselementen. Also gilt

$$\begin{aligned} \langle f(v), w \rangle &= \langle f(\sum \beta_i v_i), \sum \gamma_j v_j \rangle \\ &= \sum\sum \beta_i \gamma_j \langle f(v_i), v_j \rangle \\ &= \sum\sum \beta_i \gamma_j \langle v_i, f(v_j) \rangle \\ &= \langle v, f(w) \rangle \end{aligned}$$

□

Propo 13.20 Jede selbstadjungierte lineare Abb. $f: V \to V$, $\dim(V) = n > 0$ hat einen Eigenvektor.

Beweis Gemäß Korollar 13.19 reicht es, die Aussage für symmetrische Matrizen $A \in \mathrm{Mat}_n(\mathbb{R})$ zu beweisen! Wir wollen also zeigen, daß $\chi_A(T)$ eine Nullstelle in $\mathbb{R}$ besitzt.

Nach Fundamentalsatz der Algebra existiert komplexe Zahl $\lambda = \gamma + i\omega \in \mathbb{C}$ mit $\chi_A(\lambda) = 0$. Fasst man also die Matrix A also komplexe Matrix auf, d.h. $A \in Mat_n(\mathbb{C})$, so existiert Vektor

$$0 \neq z = \begin{pmatrix} x_1 + iy_1 \\ \vdots \\ x_n + iy_n \end{pmatrix} \in \mathbb{C}^4,$$ mit

$Az = \lambda z$. Also $A(x+iy) = (\gamma + i\omega)(x+iy)$, d.h.

$$Ax = \gamma x - \omega y,$$
$$Ay = \gamma y + \omega x.$$

Nun gilt jedoch $\langle Ax, y \rangle = \langle x, Ay \rangle$, also $\langle \gamma x - \omega y, y \rangle = \langle x, \gamma y + \omega x \rangle$.

Dies liefert:

$$\gamma\langle x,y\rangle - \omega\langle y,y\rangle = \gamma\langle x,y\rangle + \omega\langle x,x\rangle ,$$

oder $\omega(\|x\|^2 + \|y\|^2) = 0$.

Da $x+iy = z \neq 0$, folgt $\omega = 0$.

Also gilt $\eta = \gamma + i\omega = \gamma \in \mathbb{R}$. □

Theorem 13.21 Ist $(V, \langle -,- \rangle)$ ein endlichdimensionaler euklidischer VR und $f: V \to V$ selbstadjungiert. Dann gibt es eine Orthonormalbasis aus Eigenvektoren!

Beweis Per Induktion nach $n = \dim(V)$. Fall $n=0$ trivial. Sei also $n \geq 1$. Nach Propo 13.20 gibt es einen Eigenvektor

und nach Induktionsvoraussetzung eine Orthonormalbasis $v_1, \dots, v_{n-1}$ aus Eigenvektoren für $g = f|_{\langle v \rangle^\perp} : \langle v \rangle^\perp \to \langle v \rangle^\perp$

Setze $v_n = \frac{v}{\|v\|}$. Dann ist $v_1, \dots, v_n$ die gesuchte Basis. □

Korollar 13.22 Ist $A \in \mathrm{Mat}_n(\mathbb{R})$ symmetrisch, so ist A diagonalisierbar.