Vorlesung Lineare Algebra und Zahlentheorie für Informatikstudierende

Humboldt-Universität zu Berlin, Prof. Nietzsch, WS2000/2001

Inhaltsverzeichnis

1 Elementare Zahlentheorie **2**
- 1.1 Zahlensysteme, Abzählbarkeit, Dichtheit . . . 2
- 1.2 Induktionsprinzip, Beispiele . . . 2
- 1.3 Zahlenkongruenzen . . . 3
  - 1.3.1 Teilbarkeit . . . 3
  - 1.3.2 Zahlenkongruenzen . . . 5
- 1.4 $\mathbb{Z}_p$-Ringe und Kryptographie . . . 7
  - 1.4.1 Theoretische Aspekte . . . 7
  - 1.4.2 Einige Sätze . . . 7
  - 1.4.3 Kryptographie . . . 8
  - 1.4.4 Polynome . . . 9

2 Lineare Gleichungssysteme **9**
- 2.1 Grundlagen . . . 9
- 2.2 Das Gaußsche Eliminationsverfahren . . . 11

3 Mathematische Grundlagen **15**
- 3.1 Gruppen . . . 15
- 3.2 Ringe und Körper . . . 17

4 Vektorräume **18**
- 4.1 Vektorräume und Untervektorräume . . . 18
- 4.2 Lineare Abhängigkeit, Basis, Dimension . . . 20
- 4.3 Der Faktorraum . . . 22

5 Lineare Abbildungen **23**

6 Matrizen und Determinanten **26**
- 6.1 Definitionen, Eigenschaften . . . 26
- 6.2 Lineare Gleichungssysteme . . . 29
- 6.3 Volumen und Determinante . . . 30

7 Eigenwerte **34**
- 7.1 Einführung . . . 34
- 7.2 Definitionen und Beispiele . . . 36
- 7.3 Charakteristisches Polynom . . . 37
- 7.4 Diagonalisierung, Tridiagonalisierung . . . 38
- 7.5 Endomorphismuspotenzen, Nilpotenz, JORDANsche Normalform . . . 39

8 Orthogonalität **40**
- 8.1 Innere Produkte . . . 40
- 8.2 Orthogonalbasis, GRAM-SCHMIDT-Verfahren . . . 42

1 Elementare Zahlentheorie

1.1 Zahlensysteme, Abzählbarkeit, Dichtheit

Literatur: Bartholomé, Zahlentheorie für Einsteiger, Vieweg 1998
Aus dem Schulunterricht bzw. aus der Vorlesung von Prof.Starke ist bekannt (Def. 1.5.1 ff.) $\mathbb{N} := \{1, 2, 3, \dots\}$ mit $\text{card}(\mathbb{N}) = \aleph_o$. Wir betrachten $\mathbb{Z}$ und $\mathbb{Q}$, d.h. die Menge der ganzen bzw. der rationalen Zahlen und stellen fest: $\text{card}(\mathbb{Z}) = \text{card}(\mathbb{Q}) = \text{card}(\mathbb{N}) = \aleph_o$, da es eine Bijektion ϕ gibt, so daß $\phi : \mathbb{N} \to \mathbb{Z}$, und eine Bijektion ψ existiert, so daß $\psi : \mathbb{N} \to \mathbb{Q}$. (Man konstruiere diese Bijektionen!).
Nach Def. 1.5.15 sind die Mengen $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ abzählbar. Aus der Kenntnis, daß z.B. $\sqrt{2}, \sqrt{5}$ etc. nicht in $\mathbb{Q}$ enthalten sind, folgt: Es gibt eine mächtigere Menge $\mathbb{R}$, so daß $\mathbb{N}, \mathbb{Z}, \mathbb{Q} \subset \mathbb{R}$. ($\mathbb{R}$ hat die Kardinalität $\aleph_1$, siehe VL von Prof.Starke)

Lemma 1.1.
Sei $p \in \mathbb{N}$ Primzahl, dann ist $\sqrt{p} \notin \mathbb{Q}$.

Beweis: Annahme: $\sqrt{p} \in \mathbb{Q} \Leftrightarrow \sqrt{p} = \frac{a}{b}$ und $a, b \in \mathbb{N},\ b \neq 0$. Dann folgt: $p = \frac{a^2}{b^2}$. Wir nehmen an, a, b sind teilerfremd (z.B. wir kürzen vollständig). Dann gilt $p \cdot b^2 = a^2 = a \cdot a$. Das bedeutet: $p \cdot b \cdot b = a \cdot a$, somit gilt entweder $b \mid a$ (Widerspruch zur Teilerfremdheit) oder $p \mid a$, d.h. es gibt ein $m \in \mathbb{N}$ mit $a = p \cdot m$, somit $p \cdot b \cdot b = p \cdot m \cdot p \cdot m$, d.h. $b^2 = p \cdot m^2$. Da $m \nmid a$, wegen Teilerfremdheit, so $p \mid b$, Widerspruch, d.h. $\sqrt{p} \neq \frac{a}{b},\ a, b \in \mathbb{N}$ und $b \neq 0$. ■
Wir sehen somit: $\mathbb{R}$ umfaßt die Zahlenbereiche $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$

In den Zahlenbereichen kann man Abstände einführen. Wir suchen den kleinsten Abstand in $\mathbb{N}$ und $\mathbb{Z}$, d.h. $\min\{|a - b| \ :\ a, b \in \mathbb{Z}\ , a \text{ fest},\ a \neq b\} = \rho(a, b)$; natürlich folgt: $\rho(a, b) = 1$.

$\mathbb{Q}$ hat eine bemerkenswerte Eigenschaft:
Sei $\frac{a}{b} \in \mathbb{Q}$ gegeben ($b \neq 0,\ a, b \in \mathbb{Z}$). Wir geben eine kleine Schranke $\frac{\alpha}{\beta}$ vor, $\alpha, \beta \in \mathbb{Z},\ \beta \neq 0$ und fragen, gibt es immer ein $\frac{c}{d} \in \mathbb{Q},\ c, d \in \mathbb{Z},\ d \neq 0$, so daß $|\frac{a}{b} - \frac{c}{d}| < \frac{\alpha}{\beta}$ gilt.
O.B.d.A.[1] führen wir die Betrachtungen in $\mathbb{N}$ durch, weiterhin sei $\frac{a}{b} > \frac{c}{d}$ gesucht, der umgekehrte Fall ist völlig analog zu behandeln. Dann lautet die Frage so: Hat das Ungleichungssystem $\frac{a}{b} - \frac{c}{d} < \frac{\alpha}{\beta}$ bei gegebenen a, b, α, β mindestens eine Lösung $\frac{c}{d}$?
Wir rechnen: $\frac{a}{b} - \frac{c}{d} < \frac{\alpha}{\beta} \Leftrightarrow \frac{ad-bc}{bd} < \frac{\alpha}{\beta}$ Eine Lösung, die immer existiert, wäre z.B. $\beta = b \cdot d$, d.h. $d = \frac{\beta}{b}$ und $ad - bc < \alpha$, also $ad - \alpha < bc$ oder $c > \frac{ad-\alpha}{b} = \frac{\frac{a\beta}{b} - \alpha}{b} = \frac{a\beta - \alpha b}{b^2}$. Mit dieser Rechnung ist gezeigt, daß c und d im gewünschten Sinn immer existieren. Ist $\frac{\alpha}{\beta} =: \varepsilon \in \mathbb{Q}$ und ε „hinreichend“ klein, so bedeutet unsere Betrachtung: In der „Nähe“ einer rationalen Zahl $r = \frac{a}{b}$ findet man bei gegebener Größe ε immer eine andere rationale Zahl $r_1 = \frac{c}{d}$, so daß $\rho(r, r_1) < \varepsilon$ ist. Diese Eigenschaft heißt die Dichtheit von $\mathbb{Q}$.

Führt man die Relationszeichen $<, >, =$ ein, dann gilt für die Systeme $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$: Für je 2 Elemente aus dem jeweiligen Zahlensystem ist immer genau eine der Aussagen wahr: $a < b$ oder $a > b$ oder $a = b$, damit sind diese Zahlensysteme wohlgeordnet.

1.2 Induktionsprinzip, Beispiele

Wir betrachten: $1 = 1^2,\ 1 + 3 = 4 = 2^2,\ 1 + 3 + 5 = 9 = 3^2,\ 1 + 3 + 5 + 7 = 16 = 4^2$, d.h. man vermutet die Formel: Sei $n \in \mathbb{N}$, dann gilt (*) $1 + 3 + 5 + \cdots + (2n - 1) = n^2$. Stimmt das?
Sei dazu $U := \{n \in \mathbb{N} \mid \text{Formel (*) ist nicht richtig}\}$. Wenn es mindestens ein solches n gibt, dann ist $U \neq \emptyset$. U kann man ordnen, also gibt es ein kleinstes Element $m \in U$ und $m > 1$. Für $m - 1$ gilt aber (*). (Wir haben ja vier Beispiele gerechnet!) Damit ist

$$\begin{aligned} 1 + 3 + \cdots + (2(m-1) - 1) &= (m-1)^2 && \mid + (2m - 1) \\ 1 + 3 + \cdots + (2(m-1) - 1) + (2m - 1) &= (m-1)^2 + 2m - 1 = m^2 \end{aligned}$$

d.h. (*) gilt auch für m. Dies ist ein Widerspruch, da m kleinste Zahl, so daß (*) falsch. Somit ist $U = \emptyset$ und (*) gilt für alle $n \in \mathbb{N}$.

Def.1.1.
Sei $\mathbb{T} \subset \mathbb{N}$. Dann heißt $\mathbb{T}$ induktiv genau dann, wenn für alle $t \in \mathbb{T}$ gilt: $t + 1 \in \mathbb{T}$. ($\emptyset$ ist auch induktiv!)

Folgerung
Induktion: Für jede induktive Menge $\mathbb{T} \subset \mathbb{N}$ gilt: Ist $a \in \mathbb{T}$, so sind alle $b \geq a$ in $\mathbb{T}$.

[1] Ohne Beschränkung der Allgemeinheit

Damit folgt die induktive Beweismethode: Sei A eine Aussage, die für $A(a)$ gilt.
Induktionsprinzip:
1. Induktionsanfang: Wir zeigen, $A(a)$ ist wahr.
2. Wir zeigen, der Gültigkeitsbereich der Aussage A ist induktiv, d.h. abgeschlossen gegenüber Nachfolgern.
Aus dem Beweis von 1. und 2. folgt dann, $A(n)$ ist richtig für alle $n \geq a$.

Beispiel
Zu zeigen: Für alle n gilt:

$$\frac{1}{1\cdot 3}+\frac{1}{3\cdot 5}+\cdots+\frac{1}{(2n-1)(2n+1)}<\frac{1}{2}$$

Beweis:
1. Induktionsanfang: $\frac{1}{3}<\frac{1}{2}$, wahre Aussage.
2. Schluß von m auf $m+1$: Sei

$$\frac{1}{1\cdot 3}+\frac{1}{3\cdot 5}+\cdots+\frac{1}{(2m-1)(2m+1)}<\frac{1}{2},$$

dann addieren wir auf beiden Seiten (Induktionsannahme): $\frac{1}{(2m+1)(2m+3)}$. Dann folgt

$$\frac{1}{1\cdot 3}+\frac{1}{3\cdot 5}+\cdots+\frac{1}{(2m+1)(2m+3)}<\underbrace{\frac{1}{2}+\frac{1}{(2m+1)(2m+3)}}_{>\frac{1}{2}?}$$

Wir betrachten

$$\frac{1}{2}-\frac{1}{3}=\frac{1}{6}=\frac{1}{2\cdot 3};$$

$$\frac{1}{2}-\frac{1}{3}-\frac{1}{3\cdot 5}=\frac{1}{2}-\frac{5}{3\cdot 5}-\frac{1}{3\cdot 5}=\frac{1}{2}-\frac{6}{3\cdot 5}=\frac{3\cdot 5-2\cdot 6}{2\cdot 3\cdot 5}=\frac{3}{2\cdot 3\cdot 5}=\frac{1}{2\cdot 5}.$$

Analog ergibt sich

$$\frac{1}{2}-\frac{1}{3}-\frac{1}{3\cdot 5}-\frac{1}{5\cdot 7}=\frac{1}{2\cdot 7}.$$

Man kann somit vermuten:

$$\frac{1}{1\cdot 3}+\frac{1}{3\cdot 5}+\cdots+\frac{1}{(2n-1)(2n+1)}=\frac{1}{2}-\frac{1}{2\ (2n+1)}<\frac{1}{2}\qquad (**)$$

Wir starten einen neuen Versuch: Für $n=1$ ist (**) richtig. Wir addieren auf beiden Seiten $\frac{1}{(2n+1)(2n+3)}$ und erhalten:

$$\begin{aligned}\frac{1}{1\cdot 3}+\frac{1}{3\cdot 5}+\cdots+\frac{1}{(2n+1)(2n+3)} &= \frac{1}{2}-\frac{1}{2\ (2n+1)}+\frac{1}{(2n+1)(2n+3)}\\ &= \underbrace{\frac{1}{2}-\frac{1}{2\ (2n+3)}}_{<\frac{1}{2}},\ \text{also (**)}\end{aligned}$$

Man sieht, es war leichter, eine Gleichung zu beweisen als eine Ungleichung.

1.3 Zahlenkongruenzen

1.3.1 Teilbarkeit

Def.1.2.
Seien $a,b\in\mathbb{N}$. Dann $a \mid b$ genau dann, wenn ein $c\in\mathbb{N}$ existiert mit $b=c\cdot a$.

Satz 1.1.
1) 1 teilt jede natürliche Zahl.
2) Jede natürliche Zahl teilt 0.
3) $\forall^2\ n\in\mathbb{N}$ gilt $n \mid n$. Wenn $a \mid b$ und $b \mid c$, so $a \mid c$.
4) $x,a,b\in\mathbb{N}$. Wenn $x \mid a$ und $x \mid b$, so $x \mid (a+b)$.
5) $x,a,b\in\mathbb{N}$. Wenn $x \mid a$ dann $x \mid (a\cdot b)$.
6) n gerade, $2 \mid a$; dann gibt es ein $m\in\mathbb{N}$ mit $n=2m$.
7) $n\in\mathbb{N}$. Die Zahlen $2n+1$ sind ungerade.
Beweis offensichtlich.

[2] $\forall$ ist Abk. für: für alle

Satz 1.2.
Vor.: $a, b \in \mathbb{N},\ b > 0$.
Beh.: Es gibt $q, r \in \mathbb{N}$, so daß $a = q \cdot b + r$ und $0 \leq r < b$. q, r eindeutig bestimmt.
Beweis: V_b sei die Menge der Vielfachen von $b \leq a$, d.h. $V_b := \{k \cdot b \mid k \cdot b \leq a,\ k \in \mathbb{N}\}$; $V_b \neq \emptyset$, denn $0 \in V_b$. V_b ist aber endlich, enthält somit ein größtes Element $g = q \cdot b$ und $qb \leq a < (q+1)b$, d.h. $0 \leq r := a - qb < (q+1)b - qb = b$, d.h. $a = qb + r$.
Annahme: $a = qb + r = q_1 b + r_1$. Wenn $r_1 = r$, so $q_1 b = qb \Rightarrow q_1 = q$. Wäre $r_1 > r$ (o.B.d.A.), dann $r_1 - r = (q - q_1)b > 0 \Leftrightarrow q > q_1$, so daß $(q - q_1)b \geq 1 \cdot b$. Da aber $b > r_1 - r = (q - q_1)b$, so ist dies ein Widerspruch und der Satz gilt. ■

Wir beschäftigen uns mit allgemeinen Positionssystemen und stellen Zahlen dar. Bekannt: 10-er-System, 2-er-System.

Satz 1.3.
$\mathcal{B}$-adisches Positionssystem, $\mathcal{B} \in \mathbb{N}, \mathcal{B} > 1$.
Beh.: Jedes $n \in \mathbb{N}$ läßt sich eindeutig in der Form $n = a_0 + a_1\mathcal{B} + a_2\mathcal{B}^2 + \cdots + a_m\mathcal{B}^m$ schreiben und $a_k \in \{0, 1, \ldots, \mathcal{B} - 1\},\ k = 1(1)m$.
Beweis: Wir führen den Beweis induktiv.
a) Sei $n < \mathcal{B} \Rightarrow a_0 = n$ und $n = a_0 + 0 \cdot \mathcal{B}$.
b) Annahme: Darstellung für n gelte für alle Zahlen kleiner n. Wegen Satz 1.2.: $n = q \cdot \mathcal{B} + r$. $a_0 := r < \mathcal{B}$. Da $q < n$, so läßt sich q schreiben: $q = a_1 + a_2\mathcal{B} + \cdots + a_m\mathcal{B}^{m-1}$ (Induktionsvoraussetzung). Dann folgt aber die Formel $n = a_0 + a_1\mathcal{B} + a_2\mathcal{B}^2 + \cdots + a_m\mathcal{B}^m$.
Eindeutigkeit: Sei $n = a_0 + a_1\mathcal{B} + a_2\mathcal{B}^2 + \cdots + a_m\mathcal{B}^m = b_0 + b_1\mathcal{B} + b_2\mathcal{B}^2 + \cdots + b_m\mathcal{B}^m$. Wir berechnen $\frac{n}{\mathcal{B}} \Rightarrow$Satz 1.2., Reste eindeutig, d.h. $a_0 = b_0$. Dann gilt $a_1\mathcal{B} + \cdots + a_m\mathcal{B}^m = b_1\mathcal{B} + \cdots + b_m\mathcal{B}^m$. Wir teilen durch $\mathcal{B} \Rightarrow Satz1.2. \Rightarrow a_1 = b_1$ usw., d.h. $\forall\ k : a_k = b_k$. ■

Anwendungen: $\mathcal{B} = 2, 4, 8, 10, 16$.
Künftig werden wir alle Aussagen in $\mathbb{Z}$ aussprechen.

Def.1.3.
Seien $a, b \in \mathbb{Z}$.Wir definieren $a\mathbb{Z} := \{ax \mid x \in \mathbb{Z}\}$ und $a\mathbb{Z} + b\mathbb{Z} := \{ax + by \mid x, y \in \mathbb{Z}\}$

z.B. $a = 3 \Rightarrow a\mathbb{Z} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$
$b = 4 \Rightarrow b\mathbb{Z} = \{\ldots, -12, -8, -4, 0, 4, 8, 12, \ldots\}$
$a\mathbb{Z} + b\mathbb{Z} = \{\ldots, -13, -10, -7, -1, 0, 1, 7, 10, 13, 17, \ldots\} = d\mathbb{Z} = \mathbb{Z}$, da $\mathrm{ggT}(a, b) = 1$.

Wir suchen den größten gemeinsamen Teiler (ggT) zweier Zahlen $(a, b); a, b \in \mathbb{Z}$.

Satz 1.4.
Teil 1: Vor. Sei $a > b > 0;\ r_o := a;\ r_1 := b$, dann führt der nachfolgende Algorithmus auf den ggT:
Bew.
Satz 1.2. $\Rightarrow \quad r_o = q_1 r_1 + r_2 \qquad\qquad q_k, r_k \in \mathbb{Z},\ 0 \leq r_k < r_{k-1}$
Wenn $r_2 \neq 0 :\ r_1 = q_2 r_2 + r_3$
Wenn $r_3 \neq 0 :\ r_2 = q_3 r_3 + r_4$
$\quad\vdots$
$(n-1)$ter Schritt : $r_{n-2} = q_{n-1} r_{n-1} + r_n$
Wenn $r_n \neq 0 : \quad r_{n-1} = q_n r_n + r_{n+1}$
und $r_{n+1} = 0$, weil die endliche Folge $r_1 > r_2 > \cdots > r_n > r_{n+1} = 0$ abbrechen muß.
Zu zeigen: $r_n \mid a$ und $r_n \mid b$ und r_n ist $\mathrm{ggT}(a, b)$.
Wir rechnen rückwärts $r_{n-2} = q_{n-1} r_{n-1} + r_n = q_{n-1}(q_n r_n) + r_n = \tilde{q}_{n-1} r_n,\ \tilde{q}_{n-1} \in \mathbb{Z}$.
Führt man dieses Verfahren fort, so erhält man schließlich:
Es gibt $\tilde{q}_2$ und $\tilde{q}_1 \in \mathbb{Z}$, so daß $r_1 = r_n \cdot \tilde{q}_2,\ r_0 = r_n \cdot \tilde{q}_1$ und in $\tilde{q}_k$ sind Summen und Produkte der q_k nach Substitution.
Dann $r_n \mid a$ und $r_n \mid b$ und somit ist r_n gemeinsamer Teiler.
Wenn aber $\lambda \in \mathbb{N}$ und $\lambda \mid a,\ \lambda \mid b \Leftrightarrow \lambda \mid r_o$ und $\lambda \mid r_1$, dann auch $\lambda \mid r_o = q_1 r_1 + r_2 \Rightarrow \lambda \mid r_2$, man führt bis r_{n-1} fort, also $\lambda \mid r_n$, dann aber ist $r_n = \mathrm{ggT}(a, b)$.

Teil 2: Es ist $d = ggT(a, b)$ genau dann, wenn $\underbrace{a\mathbb{Z} + b\mathbb{Z}}_{=:M_1} = \underbrace{d\mathbb{Z}}_{=:M_2}$.
Beweis:
Wir beweisen die Gleichheit zweier Mengen M_1, M_2, d.h. zu zeigen $M_1 \subset M_2$ und $M_2 \subset M_1 (\Rightarrow M_1 = M_2)$.
Sei $d = \mathrm{ggT}(a, b)$.
1) $d\mathbb{Z} \supset a\mathbb{Z} + b\mathbb{Z}$, dies ist offensichtlich, da $a = dr;\ b = ds; r, s \in \mathbb{Z}$.
Dann nach Def. von $a\mathbb{Z} + b\mathbb{Z} : ax + by = drx + dsy = d(rx + sy) \in d\mathbb{Z}\ \forall\ x, y \in \mathbb{Z}$.
2) Wir benutzen den Teil 1:

$a = bq_1 + r_1$ z.z. $r_k \in a\mathbb{Z} + b\mathbb{Z}$

$\vdots \quad \vdots$ $r_1 = a + (-q_1)b \in a\mathbb{Z} + b\mathbb{Z}$ nach Def.

$r_{n-1} = q_n d.$

Sei Beh. bis k richtig $\begin{cases} r_{k-2} = ax_2 + by_2 \\ r_{k-1} = ax_1 + by_1 \end{cases}$

andererseits ist $r_{k-2} = q_k r_{k-1} + r_k;\ r_k = r_{k-2} - q_k r_{k-1}$.

Einsetzen liefert $r_k = (ax_2 + by_2) - q_k(ax_1 + by_1) = a \cdot \alpha + b \cdot \beta \in a\mathbb{Z} + b\mathbb{Z}$, α, β in Abhängigkeit von x_k, y_k, q_k, d.h. für k gilt die Inklusion ebenfalls.

3) Wenn $a\mathbb{Z} + b\mathbb{Z} = c\mathbb{Z}$, dann $c = d$. Dies folgt so:

Sei $c\mathbb{Z} = d\mathbb{Z}$, denn es war schon $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z} \Rightarrow c \in d\mathbb{Z}$ und $d \in c\mathbb{Z}$. Es gibt ein solches $q \in \mathbb{Z}$ mit $c = d \cdot q$ und ein $\tilde{q}$, so daß $d = c \cdot \tilde{q} \Rightarrow c = d \cdot q = c \cdot \tilde{q} \cdot q \Rightarrow q \cdot \tilde{q} = q_o = \pm 1$. Wenn $c > 0, d > 0 \Rightarrow q_o = 1$ und $c = d$.■

Folgerung

Die Diophantische Gleichung $c = ax + by;\ a, b, c \in \mathbb{Z}$ ist in $\mathbb{Z}$ lösbar g.d.w.[3] d=ggT(a, b) ist Teiler von c.

Beweis: Seien $x, y \in \mathbb{Z}$ und $c = ax + by$. Dann $d \mid c$, da $d \mid a$ und $d \mid b$.

Umgekehrt: $d \mid c$, dann gibt es $s \in \mathbb{Z}$ mit $c := d \cdot s$. Weiterhin existieren $x_1, y_1 \in \mathbb{Z}$, so daß $d = ax_1 + by_1$ (Satz 1.3.). Somit $c = ds = a(x_1 s) + b(y_1 s)$. ■

1.3.2 Zahlenkongruenzen

Def.1.4.

Seien $a, b \in \mathbb{Z}, n \in \mathbb{N}$ fest. Dann $a \equiv b \mod m$ g.d.w. $m \mid a - b$. [4]

Da $a = q_1 m + r_1;\ b = q_2 m + r_2$, so $a - b = (q_1 - q_2)m + (r_1 - r_2)$ und $r_1 = r_2$.

z.B. $5 \equiv 3 \mod 2$, denn $2 \mid (5 - 3)$,

$-10 \equiv -1 \mod 3$, denn $3 \mid (-9)$ usw.

Wir definieren sog. Restklassen modulo m:

Sei $m \in \mathbb{N},\ a \in \mathbb{Z}$. Dann ist mit $[a]_m := \{a + mz \mid z \in \mathbb{Z}\}$ eine Restklasse modulo m definiert. Alle Restklassen modulo m schreibt man $\mathbb{Z}_m \equiv \mathbb{Z}/m\mathbb{Z} := \{[0]_m, [1]_m, \ldots, [m-1]_m\} \Rightarrow$ Es gibt m-Restklassen $[0], [1], \ldots, [m-1]$.

Man kann alle $z \in \mathbb{Z}$ in Restklassen ordnen, z.B. $m = 7$.

[0]	[1]	[2]	[3]	[4]	[5]	[6]	Restklasse
-14	-13	-12	-11	-10	-9	-8	
-7	-6	-5	-4	-3	-2	-1	
0	1	2	3	4	5	6	
7	8	9	10	11	12	13	
14	15	16	17	18	19	20	
...							

Wir lernen nun das Rechnen in $\mathbb{Z}/m\mathbb{Z}$.

Satz 1.5.

Seien $a, b, c, d \in \mathbb{Z},\ m \in \mathbb{N}$. Dann gilt: Aus $a \equiv b \mod m$ und $c \equiv d \mod m$ folgt

(i) $(a \pm c) \equiv (b \pm d) \mod m$ sowie

(ii) $a \cdot c \equiv b \cdot d \mod m$.

Beweis: Wir beweisen nur (ii):

$a \equiv b \mod m$ bedeutet $a = q_1 m + b$ und $c \equiv d \mod m$ bedeutet $c = q_2 m + d;\ q_1, q_2 \in \mathbb{Z}$. Dann folgt:

$$a \cdot c = (q_1 m + b)(q_2 m + d) = q_1 m \cdot q_2 m + q_1 \cdot dm + q_2 \cdot bm + b \cdot d,$$

d.h. es gibt ein q_0, so daß $a \cdot c = q_0 \cdot m + b \cdot d$ und hieraus $a \cdot c \equiv bd \mod m$. ■

Folgerung

Durch Definition der Restklassen mod m wird eine Äquivalenzrelation $a \sim b$ über $\mathbb{Z}$ definiert (siehe Bemerkung zur Def.1.4.):

Reflexivität: $a \sim a \Leftrightarrow a \equiv a \mod m$, trivial, da $m \mid 0$;

Symmetrie: $a \sim b \Leftrightarrow b \sim a$ g.d.w. $a \equiv b \mod m \Leftrightarrow -(b - a)$ wird von m geteilt, also auch $b \equiv a \mod m$.

Transitivität: $a \equiv b \mod m,\ b \equiv c \mod m$. Zu zeigen: $a \equiv c \mod m$.

Nach Satz 1.4.(i): $a - b \equiv 0 \mod m,\ b - c \equiv 0 \mod m$ also bei Addition $a - c \equiv 0 \mod m$ oder $a \equiv c \mod m$. ■

Beispiele

1) Man bestimme ggT$(1450, 928) = 58$.

[3] genau dann, wenn

[4] für '$b \mod m$' sprich 'b modulo m'

2) Man bestimme die letzte Ziffer von 2^{1000}.
Lösung: $2^{1000} = 2^{4\cdot 250} = (2^4)^{250}$.
Für $a = c$ und $b = d$ folgt aus Satz 1.5.: $a^2 \equiv b^2 \mod n$
oder allgemein: $a^m \equiv b^m \mod n$ für $m \geq 1,\ n \in \mathbb{N},\ n > 1$.
Somit schließen wir weiter: $2^4 = 16 \equiv 6 \mod 10$, somit $(2^4)^{250} \equiv 6^{250} \mod 10$;
$6^{250} = (6^2)^{125} \Leftrightarrow 6^2 \equiv 6 \mod 10$, so daß $(6^2)^{125} \equiv 6^{125} \mod 10$ und $6^k \equiv 6 \mod 10$ für $k = 1, 2, 3, \ldots$.
Somit $6^{250} \equiv 6 \mod 10$ und schließlich $(2^4)^{250} \equiv 6^{250} \mod 10$, also $2^{1000} \equiv 6 \mod 10$, die letzte Ziffer ist somit eine 6.
3) Teilbarkeit: Wir betrachten das 10er-System für $m = 11$ und möchten für die 11 eine Regel ableiten.
Sei $z \in \mathbb{Z} (z \in \mathbb{N}_o)$.
Dann gilt bekanntlich $z = a_n a_{n-1} \cdots a_2 a_1 a_0$ oder $z = a_0 \cdot 10^0 + a_1 \cdot 10^1 + \cdots + a_n \cdot 10^n,\ a_k \in \{0, 1, \ldots, 9\}$.
Wir rechnen $\mod 11$:

$$\begin{array}{ll} 10^0 \equiv 1 \mod 11 & \mid \cdot a_o \\ 10^1 \equiv -1 \mod 11 & \mid \cdot a_1 \\ 10^2 \equiv 1 \mod 11 & \mid \cdot a_2 \\ 10^3 \equiv -1 \mod 11 & \mid \cdot a_3 \\ \vdots & \\ 10^k \equiv (-1)^k \mod 11 & \mid \cdot a_k,\ k = n \end{array}$$

Addition ergibt: $z = 10^0 \cdot a_o + 10^1 \cdot a_1 + \cdots + 10^n \cdot a_n) \equiv (a_o - a_1 + a_2 - a_3 + \cdots \pm a_n) \mod 11$. Dann folgt: $11 \mid z \Leftrightarrow 11 \mid (a_o - a_1 + a_2 - \cdots \pm a_n)$, d.h. die Regel lautet:
Lemma: $11 \mid z\ \ (z \in \mathbb{N})$ g.d.w. 11 teilt die alternierende Quersumme von z.
4) Diophantische Gleichungen (linear)
Wir betrachten die Gleichung

$$ax + by = c \quad \text{(DG)}$$

mit $a, b, c \in \mathbb{Z}$ und fragen: Gibt es $x, y \in \mathbb{Z}$, so daß (DG) erfüllt ist?
(DG) heißt eine Diophantische Gleichung.
Wir nehmen an: $x_o, y_o \in \mathbb{Z}$ erfüllen bei gegebenen a, b, c die Gleichung (DG). Sei $d = \text{ggT}(a, b)$, dann auch $d \mid ax_o,\ d \mid by_o$. Aufgrund von $ax_o + by_o = c$ folgt: $d \mid c$. Somit ist notwendig für die Lösbarkeit von (DG): $\text{ggT}(a, b) = d \mid c$.
Umgekehrt: Sei $d = \text{ggT}(a, b) \mid c$. Dann gibt es Zahlen $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}$, so daß $a = \bar{a}d,\ b = \bar{b}d,\ c = \bar{c}d$, wobei noch $\text{ggT}(\bar{a}, \bar{b}) = 1$ (!). Dann hat aber nach Satz 1.4. die Gleichung (DG'): $\bar{a}\xi + \bar{b}\eta = 1$ mindestens eine Lösung $\xi, \eta \in \mathbb{Z}$. Setzen wir $x_o := \bar{c}\xi, y_0 := \bar{c}\eta$ so folgt: $ax_o + by_o = \bar{a}d \cdot \bar{c}\xi + \bar{b}d \cdot \bar{c}\eta = \bar{c}d(\bar{a}\xi + \bar{b}\eta) = \bar{c}d = c$, d.h. für die definierten Zahlen x_o, y_o gilt: $ax_o + by_o = c$ und $x_o, y_o \in \mathbb{Z}$ ist Lösung von (DG) unter der Bedingung $\text{ggT}(a, b) \mid c$, dies ist somit auch hinreichend. Dann folgt

Satz 1.6
Die Diophantische Gleichung

$$ax + by = c \quad \text{(DG)}$$

ist lösbar genau dann, wenn $\text{ggT}(a, b) \mid c$.

Folgerung
Lösungsdarstellung: $x_0, y_0 \in \mathbb{Z}$ mögen (DG) erfüllen. Seien $x, y \in \mathbb{Z}$ und $ax + by = ax_o + by_o$
$\Rightarrow a(x - x_o) = b(y_o - y)$. Nach Satz 1.6.: $a = \bar{a}d,\ b = \bar{b}d \Rightarrow \bar{a}(x - x_o) = \bar{b}(y_o - y)$ und $\text{ggT}(\bar{a}, \bar{b}) = 1$. Weiterhin $\bar{b} \mid \bar{a}(x - x_o) \Leftrightarrow \bar{b} \mid x - x_o$. Dann gibt es ein $\bar{t} \in \mathbb{Z}$, so daß $x - x_o = \bar{b}\bar{t} \Leftrightarrow \bar{a}(x - x_o) = \bar{a}\bar{b}\bar{t}$. Da $\bar{b} \neq 0$ folgt: $\bar{a}\bar{b}\bar{t} = \bar{b}(y_o - y)$ und somit $\bar{a}\bar{t} = (y_o - y)$, oder andererseits $\bar{a}(x - x_o) = \bar{a}\bar{b}\bar{t}$ mit $\bar{a} \neq 0$, so daß

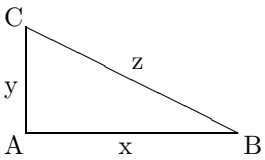
$$y = y_o - \bar{a}\bar{t},\ x = x_o + \bar{b}\bar{t}.$$

Dies ist unter den genannten Voraussetzungen die allgemeine Lösung der Gleichung (DG).
$(\bar{t} = 0; \pm 1; \pm 2; \pm 3;$ usw.)

Beispiel
a) $314x + 100y = 18 \mid : 2 \Rightarrow 157x + 50y = 9;\ \text{ggT}(157, 50) = 1;\ 1 \mid 9 \Rightarrow$ Gleichung lösbar.
Wir betrachten (DG'): $157\xi + 50\eta = 1$. Als Lösung ist $\xi = -7; \eta = 22$ akzeptabel,
denn $157 \cdot (-7) = 1099;\ 50 \cdot 22 = 1100;\ 1100 - 1099 = 1$.
Nun ist $\bar{c} = 9$, d.h. $x_o = 9 \cdot (-7) = -63; y_o = 9 \cdot 22 = 198$.
Damit erhält man die allgemeine Lösung $x = -63 + 50t;\ y = 198 - 157t;\ t \in \mathbb{Z}$.

b) Gegeben sei ein rechtwinkliges Dreieck ABC.
Vergrößert man die erste Kathete um 8 cm, die zweite um 5cm, so vergrößert sich das Hypothenusenquadrat um 325cm^2. Wie groß sind die Katheten?
Lösung: Es gilt $x^2 + y^2 = z^2$. Nach Aufgabe hat das neue Dreieck folgenden Seitenbeziehung: $(x + 8)^2 + (y + 5)^2 = z^2 + 325$

$\Rightarrow x^2+16x+64+y^2+10x+25 = x^2+y^2+325$
$\Rightarrow 16x+10y = 325-89 = 236 \quad |: 2$
$\Rightarrow 8x+5y = 118$
also ggT$(8,5)=1$ und $1 \mid 118$, Gleichung lösbar.
Wir betrachten (DG'): $8\xi+5\eta=1$. Man erkennt: $\xi=2, \eta=-3$, denn $16-15=1$, also:
$x_o = 2\cdot 118 = 236;\ y_o = (-3)\cdot 118 = -354$. Man erhält die allgemeine Lösung: $x = 236+5t;\ y=-354-8t$. Wenn x,y negativ oder Null, Lösung ist sinnlos. Nur für $t=-45;-46;-47$ ergeben sich positive x,y, dann entsprechen die Kathetenpaare $(11,6);\ (6,14);\ (1,22) = (x,y)$. ■



1.4 $\mathbb{Z}_p$-Ringe und Kryptographie

1.4.1 Theoretische Aspekte

Wir untersuchen das Rechnen im Restklassenring $\mathbb{Z}/m\mathbb{Z}$.

Def.1.5.
Sei $m>1,\ m\in\mathbb{N};\ a,b\in\mathbb{Z}/m\mathbb{Z}$. a heißt bzgl. der Multiplikation in $\mathbb{Z}/m\mathbb{Z}$ invers, wenn $a\cdot b=1$ gilt in $\mathbb{Z}/m\mathbb{Z}$. In diesem Fall heißen die Zahlen a,b invertierbar.

Folgerung
1) Sei ggT$(a,m)=1$, dann existieren die Inversen zu $a\in\mathbb{Z}$ immer in $\mathbb{Z}/m\mathbb{Z}$, denn: Es gibt nach Satz 1.4. $x,y\in\mathbb{Z}$, so daß $1=ax+my$. Gilt $a\cdot b=1$, dann bedeutet das $a\cdot b = ax+my$ oder $a(b-x)=my;\ a\nmid m$, jedoch es gibt immer ein y, so daß $a\mid y$, d.h. b kann immer eindeutig bestimmt werden.

2) Besonders interessant sind $\mathbb{Z}/p\mathbb{Z}$ Ringe, $p\in\mathbb{P}$ Primzahl.
Wir wollen den Begriff „Ring" spezifizieren.
Sei $m\geq 1, m\in\mathbb{N}$. Betrachte $\mathbb{Z}/m\mathbb{Z}$:
(1)(i) Für alle $a,b,c\in\mathbb{Z}/m\mathbb{Z}$ ist $(a+b)+c = a+(b+c)\ (\mod m)$.
(ii) Für alle $a\in\mathbb{Z}/m\mathbb{Z} : a+0=a$.
(iii) Für alle $a\in\mathbb{Z}/m\mathbb{Z}$ gibt es ein $b\in\mathbb{Z}/m\mathbb{Z}$ mit $a+b=0$ und es gilt allgemein $a+b=b+a\ (\mod m)$.
(2)(i) $1\cdot a=a;\ a\cdot(b\cdot c)=(a\cdot b)\cdot c$ in $\mathbb{Z}/m\mathbb{Z}$,
(ii) $a\cdot(b+c)=a\cdot b+a\cdot c$ in $\mathbb{Z}/m\mathbb{Z}$,
(iii) $a\cdot b=b\cdot a$ in $\mathbb{Z}/m\mathbb{Z}$.
Wir beweisen (2)(ii): Nach Voraussetzung gibt es $q_k,r_k\in\mathbb{Z}$, so daß
$a=q_1m+r_1,\ b=q_2m+r_2,\ c=q_3m+r_3,\ 0\leq|r_k|<m,\ k=1,2,3$. Dann rechnen wir $\mod m$:
$(q_1m+r_1)(q_2m+r_2+q_3m+r_3)$
$= q_1q_2\cdot m\cdot m+q_1r_2m+q_1q_3m\cdot m+q_1r_3m+q_2r_1m+r_1r_2+q_3r_1m+r_1r_3 \equiv (r_1r_2+r_1r*3) \mod m$, d.h. $a(b+c)\equiv(a\cdot b+a\cdot c) \mod m$. Gilt in einer Struktur (1) und (2), dann bezeichnet man diese Struktur als einen kommutativen Ring, d.h. $\mathbb{Z}/m\mathbb{Z}$ ist ein kommutativer Ring, $\mathbb{N}$ nicht.

Beispiel
1) Wir wollen Gleichungen in $\mathbb{Z}_p := \mathbb{Z}/p\mathbb{Z}$ lösen, z.B. $11392^{25}\equiv x \mod 7;\ m=7\in\mathbb{P},\ 25=5\cdot 5$. Es gilt: $11392 = 3 \mod 7$. Also kann man schreiben: $11392^{25}\equiv(3^5)^5 \mod 7 \equiv (3^6)^4\cdot 3 \mod 7;\ 3^6 = 27\cdot 27 = 729 = 7\cdot 104+1$, d.h. $3^6\equiv 1 \mod 7$ und damit $11390^{25}\equiv 3 \mod 7$, d.h. die Lösung ist $x=3$.
2) Wir fragen gemäß Def.1.5. nach Inversen.
$p=41$ in $\mathbb{Z}_{41}$ suchen wir $(13)^{-1}$. Wir rechnen $\mod 41$: $41=3\cdot 13+2;\ 13=2\cdot 6+1$, d.h. wir haben die 1 erzeugt. Dann $1=13-2\cdot 6 = 13-6(41-3\cdot 13) = 19\cdot 13-6\cdot 41\equiv 19\cdot 13 \mod 41$, d.h. in $\mathbb{Z}_{41}$ ist $(13)^{-1}=19$.
3) $p=17$. Löse in $\mathbb{Z}_{17}$ die Gleichung $3x+2=5x-7\Leftrightarrow 2x=9$. Wir suchen wieder die Inverse zu 2, denn dann $a\cdot x=1$.
$17=2\cdot 9-1$, also $1=2\cdot 9-17\Leftrightarrow$ in $\mathbb{Z}_{17}$ ist $(2)^{-1}=9$. Nun multiplizieren wir $2x=9$ mit 9 und rechnen in $\mathbb{Z}_{17}$: $4\cdot 17=68; (2)^{-1}\cdot 9=1; 81=68+13$, d.h. wir suchten die allgemeine Lösung von $13\equiv x \mod 17$. Damit haben wir als allgemeine Lösung: $x=13+k\cdot 17;\ k\in\mathbb{N}$.

1.4.2 Einige Sätze

1) Der kleine Fermatsche Satz
Sei $p\in\mathbb{P},\ a\in\mathbb{Z},\ a\neq np,\ n\in\mathbb{Z}$. Dann gilt: $a^{p-1}\equiv 1 \mod p \Leftrightarrow a^p\equiv a \mod p$.
Beweis: Die Reste mod p sind: $1\cdot a,\ 2\cdot a,\ldots,(p-1)a$ und diese sind paarweise verschieden und $\neq 0$.
Wenn $i\cdot a\equiv j\cdot a \mod p; 1\leq i,j\leq p-1$ und da ggT$(a,p)=1$, so $i\equiv j \mod p\Leftrightarrow i=j$.
$p-1$ verschiedene Reste existieren, diese sind $1,2,\ldots,p-1$, d.h. es gilt
$(1\cdot a)\ (2\cdot a)\cdots(p-1)a\equiv 1\cdot 2\cdot 3\cdots(p-1) \mod p\Leftrightarrow (p-1)!\ a^{p-1}\equiv(p-1)! \mod p$
$\Leftrightarrow a^{p-1}\equiv 1 \mod p,\ p\in\mathbb{P}$. ■

Folgerung
Gilt $p \mid a$, so $a^p \equiv 0 \mod p \equiv a \mod p$, d.h. auch dann gilt der Satz.

Anwendung
Man beweise: Für alle $n \in \mathbb{N}: \ 42 \mid n^7 - n; \ n > 1$.
Lösung: $42 = 6 \cdot 7 = 2 \cdot 3 \cdot 7$. $7 \in \mathbb{P}$. $n^7 - n = n(n^6 - 1)$. Also $(n^6 - 1) = 0 \mod 7$ nach kleinen FERMAT $(a = n)$, d.h. $n^7 - n$ ist teilbar durch 7. $n(n^6 - 1) \equiv 0 \mod 3$, denn: Reste von 3: 0,1,2; Reste von n^2: 0,1. $n^6 = (n^3)^2$, d.h. wenn $3 \mid n \Rightarrow 3 \mid n(n^6 - 1)$; wenn $3 \nmid n \Rightarrow ((n^3)^2 - 1) = 0 \mod 3$. $((n^3)^2 - 1) \equiv 0 \mod 2$, denn: Wenn $2 \mid n \Rightarrow 2 \mid n(n^6 - 1)$, wenn $2 \nmid n$, dann n^6 hat Rest 1 und damit $(n^6 - 1) \equiv 0 \mod 2$, also ist $n^7 - n$ durch $2 \cdot 3 \cdot 7 = 42$ teilbar.

2) Der chinesische Restsatz
Seien $m, n \in \mathbb{N}, \text{ggT}(m, n) = 1$. Dann hat für jedes Zahlenpaar $a, b \in \mathbb{Z}$ das System
(i) $x \equiv a \mod m$ und
(ii) $x \equiv b \mod n$ eine eindeutige Lösung $x \in \mathbb{N}, \ x < m \cdot n$.
Beweis: Wir betrachten (i). Die Menge $\underbrace{a, a + m, a + 2m, \ldots, a + (n-1)m}_{(*)}$ ist Lösung von (i).

Sei $a + im \equiv a + jm \mod n, \ 0 \leq i, j \leq n - 1 \Rightarrow (i - j)m \equiv 0 \mod n \Leftrightarrow n \mid i - j \Leftrightarrow i = j$. Damit liegen die Zahlen (*) in n verschiedenen Restklassen $\mod n$.
Dann gibt es eindeutig ein i, so daß $a + im \equiv b \mod n$. ■

Folgerung
Allgemein gilt für $\{m_k \mid \text{ggT}(m_i, m_k) = 1, \ i \neq k\}, \ a_1, \ldots, a_n \in \mathbb{Z}$:
Das System $x \equiv a_1 \mod m_1, \ldots, x \equiv a_n \mod m_n$ besitz genau eine Lösung $\mod m_1 \cdots m_n$.

Beispiel
Wir haben 45 Karten numeriert von 1 bis 45. Wir legen die Karten wie folgt auf:

1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18
19	20	21	22	[23]	24	25	26	27
28	29	30	31	32	33	34	35	36
37	38	39	40	41	42	43	44	45

} 9 Spalten und 5 Zeilen

Jemand merkt sich eine Zahl, z.B. 23, diese liegt in der 5.Spalte. Nun legt man die Karten neu, in 9 Zeilen.

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	[23]	24	25
26	27	28	29	30
31	32	33	34	35
36	37	38	39	40
41	42	43	44	45

} 5 Spalten und 9 Zeilen

Die 23 liegt jetzt in Spalte 3. Man „rät“ 23, warum?
Wir haben die Restklassen aufgeschrieben: x läßt Rest 5 bei Division durch 9 und x läßt Rest 3 bei Division durch 5, also gilt: $x \equiv 5 \mod 9, \ x \equiv 3 \mod 5, \ \text{ggT}(9, 5) = 1$. Es gibt genau eine Lösung. Dann heißt das, es gibt $a, b \in \mathbb{Z}$, so daß $x = 3 + 5a = 5 + 9b \Leftrightarrow 5a = 9b + 2$. Wir rechenen $\mod 9$, dann $5a = 2$ oder $a = 2k, \ 5k = 1 \Leftrightarrow 2 \cdot 5 = 9 + 1$, also $a = 4, \ k = 2, \ a \equiv 4 \mod 9$. Dann gibt es ein l so, daß $a = 4 + 9l$, das aber bedeutet: $x = 3 + 5(4 + 9l) = 23 + l \cdot 45$. Da $x < 45$ folgt $l = 0$ und $x = 23$.
Zusammenfassung Beim chinesischen Restsatz ist die Menge der Lösungen aus $\{\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}\}$, d.h. wir suchen $f : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/mn\mathbb{Z}$, wobei $f(a, b) \equiv a \mod m$ und $f(a, b) \equiv b \mod n$.
Spezialfall: Es gibt $x \in \mathbb{Z}$, so daß $x \equiv 1 \mod m$ und $x \equiv 1 \mod n$.

1.4.3 Kryptographie

Grundaufgabe Buchstaben, Zahlen, Symbole wie +, !, ?, etc. in andere Symbole umsetzen.
bekannt: Cäsarcode: A=00, B=01,..., N=13,..., Y=24, Z=25 $\Rightarrow$ 26 Buchstaben. Wir verschieben um vier Buchstaben. Aus MATHEMATIK $\xrightarrow{\text{Cäsar}}$ QEXLIQEXMO.
Mathematisch rechnen wir also $\mod 26 \mathrel{\hat{=}} \mathbb{Z}/26\mathbb{Z}$. Nimmt man noch +,!,? hinzu, dann $\mathbb{Z}_{29}$ Primzahlring.
Im Alphabet: $n \mapsto n + 4 (\mod 26)$. Allgemeiner kann man verschlüsseln:
Sei $\text{ggt}(26, a) = 1$, dann $E(n) = a \cdot n + t \mod 26$ und t beliebig. Wir wollen an Hand eines Beispiels die

Verschlüsselung und die Dechiffrierung studieren. Sei $a = 3$ und somit wäre

$$E(n) = 3n + t \mod 26 \qquad (C)$$

Man vergleiche Cäsar:

$$E(n) = n + 4 \mod 26 \qquad (DC)$$

Mit dieser Methode also wird komplizierter verschlüsselt. Nun erhebt sich dabei die Frage, wie wird dechiffriert? Zuerst betrachten wir ein Beispiel: Gemäß (C): $a = 3,\ t = 10$. Dann ist eine Dechiffrierung gefunden, wenn es ein $\tilde{a} \in \mathbb{Z}$ gibt, so daß $\tilde{a}(\underbrace{E(n) - t}_{D(n)}) = \tilde{a}an = n$. Wir müssen somit das Reziproke von $3 \mod 26$ ausrechnen. $\tilde{a}\cdot a = \tilde{a}\cdot 3 = 9\cdot 3 \equiv 1 \mod 26$, d.h. $\tilde{a} = 9$. Wenn $n' = E(n)$, so $D(n') = \tilde{a}(n'-t) = 9n'-90 = 9n'+14$, damit erhält man den codierten Buchstaben n' aus der Relation $D(n') = 9n + 14 \mod 26$.
Nach dem bekannten Satz von Heinz Erhardt: Noch'n Gedicht, also noch'n Beispiel: $a = t = 11$. Codiert wird nach der Formel $E(n) = 11n + 11 \mod 26$. Zuerst suchen wir $\tilde{a}a = 1 \mod 26 \Leftrightarrow \tilde{a} \cdot 11 = 1$ in $\mathbb{Z}/26\mathbb{Z}$. Nun ist $26 \cdot 8 = 208$ und $19 \cdot 11 = 209$, also $(11)^{-1} = 19$ in $\mathbb{Z}_{26}$ oder $D(n') = \tilde{a}(n' - t) = 19n' - 9$ oder $D(n') = 19n' + 25 \mod 26$.
Literatur: Beutelsbacher, Kryptographie, Vieweg 1998.

1.4.4 Polynome

Eine Abbildung $f(x) = a_0 + a_1x + \cdots + a_nx^n,\ f : \mathbb{Z}_p \to \mathbb{Z}_p$ heißt Polynomfunktion vom Grade n, wenn $a_n \neq 0$. $\alpha \in \mathbb{Z}_p$ heißt Nullstelle von f, wenn $f(\alpha) = 0$ in $\mathbb{Z}_p$.

Satz 1.8.
$f : \mathbb{Z}_p \to \mathbb{Z}_p$ vom Grad n, $\alpha \in \mathbb{Z}_p$ Nullstelle. Dann gibt es ein Polynom g vom Grad $n - 1$, so daß $f(x) = (x - \alpha) \cdot g(x),\ \forall\ x \in \mathbb{Z}_p$.
Beweis: $f(x) = f(x)-f(\alpha) = a_0+a_1x+\cdots+a_nx^n-(a_0+a_1\alpha+\cdots+a_n\alpha^n) = a_1(x-\alpha)+\cdots+a_n(x^n-\alpha^n) = (x-\alpha)(1+\cdots+a_n\xi(x,\alpha))$ und $\xi(x,\alpha)$ ist vom Grad $n-1$, denn:
z.B. für $n = 3$: $\xi(x,\alpha) = x^3-\alpha^3 \equiv (x-\alpha)(ax^2+bx+c) = ax^3+bx^2+cx-\alpha ax^2-\alpha bx-\alpha c = x^3-\alpha^3;\ a,b,c \in \mathbb{Z}_p \Rightarrow (a = 1) = x^2(b-\alpha)+(c-\alpha b)x+x^3-\alpha c \Rightarrow 1 = \alpha c$.

2 Lineare Gleichungssysteme

2.1 Grundlagen

Wir betrachten den Zahlenkörper $\mathbb{R}$ und die Zahlengerade. Dort in $\mathbb{R}$ sind Addition und Multiplikation erklärt. Betrachten wir die Ebene $\mathbb{R}^2 \cong E^2$, dann verstehen wir darunter die Menge der Paare, d.h. $x \in \mathbb{R}^2 \Leftrightarrow x := \{(x_1, x_2) \mid x_1, x_2 \in \mathbb{R}\}$.
Allgemein wird für $n \in \mathbb{N},\ n > 1$ definiert: Sei $x_k \in \mathbb{R}$, dann $\mathbb{R}^n := \{x := (x_1, \ldots, x_n) \mid x_k \in \mathbb{R}, k = 1(1)n\}$. Dies ist die Menge der geordneten Tupel.
Beispiel
x_k sei Nennwert von Aktien, a_k der zugehörige Börsenkurs, dann hat der Anleger das Kapital $b = a_1x_1 + \cdots + a_nx_n$ für $n \in \mathbb{N}$ (Lineare Relation).
Wir definieren: $(x_1, \ldots, x_n) + (y_1, \ldots, y_n) := (x_1 + y_1, \ldots, x_n + y_n)$ für $x_k, y_k \in \mathbb{R}$ und für $\lambda \in \mathbb{R}$: $\lambda(x_1, \ldots, x_n) = (\lambda x_1, \ldots, \lambda x_n)$. Man veranschauliche dies in der Ebene und im Raum.

Def. 2.1.
1) Seien $x, y \in \mathbb{R}^n$, dann heißen x, y linear unabhängig, wenn es kein $\lambda \in \mathbb{R}$ gibt, so daß $y = \lambda x$.
2) Seien k Vektoren $x^1, \ldots, x^k$ gegeben mit $x^k := (x_1^k, \ldots, x_n^k)$. Dann heißt die Menge der $\{x^j\}_{j=1}^k$ linear unabhängig, wenn aus $\lambda_1x^1 + \cdots + \lambda_kx^k = 0$ immer folgt $\lambda_1 = \lambda_2 = \cdots = \lambda_k = 0$.

Gleichungssysteme Wir haben eine Menge reeller Zahlen $\{a_{kj}\}, 1 \leq k \leq m$ (Anzahl der linearen Bedingungen) und $1 \leq j \leq n$ (Anzahl der Unbekannten). Sei $b = (b_1, \ldots, b_m)^t$, dann heißt die Struktur

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\ \vdots \qquad\qquad\qquad\qquad &\ \ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= b_m \end{aligned}$$

ein lineares Gleichungssystem, $\{a_{kj}\}$ und b sind gegeben, das Tupel $(x_1, \ldots, x_n), x_k \in \mathbb{R}$ ist gesucht.

Wir vereinbaren: $A := \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$ Ein solches Schema heißt Matrix, hier Koeffizientenmatrix.

$b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$ heißt Spalte [5], man schreibt auch $b = (b_1, \ldots, b_m)^t$ [6].

Wir definieren $A \cdot x = \begin{pmatrix} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n \end{pmatrix}$

Der Index n bei x muß mit dem Index m in der Matrix A übereinstimmen. Dann kann man kurz schreiben

$$A \cdot x = b \qquad (1).$$

Als $(A, b) := \begin{pmatrix} a_{11} & \cdots & a_{1n} & b_1 \\ \vdots & & & \vdots \\ a_{m1} & \cdots & a_{mn} & b_m \end{pmatrix}$ bezeichnet man die erweiterte Koeffizientenmatrix. A heißt kurz $(m \times n)$-Matrix. Man kann (1) auch mit dem Summenzeichen schreiben:

$$\sum_{j=1}^{n} a_{kj}x_j = b_k, \quad k = 1(1)m.$$

Man nennt $\text{Lös}(A, b) := \{x \in \mathbb{R}^n \mid Ax = b\}$ die Lösungsmenge des linearen Gleichungssystems (1). Was aber heißt Lösung des System (1)?
Wir werden sehen, daß mit der Definition von A der Begriff der Abbildung zwischen Mengen angesprochen ist. Aus diesem Grund wollen wir einen kurzen Exkurs über Abbildungen durchführen.

Seien X, Y Mengen. f heißt dann Abbildung von X nach Y, wenn es für jedes $x \in X$ eindeutig ein Element $y = f(x) \in Y$ zuordnet.
Symbol: $f : X \to Y;\ x \mapsto f(x) = y$. (Mengen- und Elementrelation)
z.B. $X = Y = \mathbb{R};\ f(x) = ax,\ x \in \mathbb{R} \Rightarrow$ Gerade durch 0.
$f(x) = \sqrt{x}$, man muß $X = Y = \mathbb{R}_+$ und $x \mapsto +\sqrt{x}$ setzen. $\mathbb{R}_+ := \{x \in \mathbb{R} \mid x \geq 0\}$.

Sei $f : X \to Y$ und $M \subset X,\ N \subset Y$.
Dann bezeichnet man $f(M) := \{y \in Y \mid \exists\ x \in M \text{ mit } y = f(x)\} \subset Y$ [7] Bild von M,
$f^{-1}(N) := \{x \in X \mid f(x) \in N\} \subset X$ Urbild von N in X,
$f^{-1}(y) := f^{-1}(\{y\}) \subset X$ für einelementige Mengen, kann auch leer sein, also f^{-1} problematisch!

Def.2.2
Die Abbildung $f : X \to Y$ heißt
injektiv, falls aus $x_1, x_2 \in X$ und $f(x_1) = f(x_2)$ immer folgt: $x_1 = x_2$;
surjektiv, falls $f(X) = Y \Leftrightarrow$ d.h. zu jedem $y \in Y$ gibt es ein $x \in X$ mit $y = f(x)$;
bijektiv, falls f injektiv und surjektiv ist.

Folgerung I
Ist f bijektiv, so gibt es zu jedem $y \in Y$ genau ein $x \in X$ mit $f(x) = y$. Dann gibt es die Umkehrabbildung f^{-1}, d.h. $f^{-1} : Y \to X,\ y \mapsto x = f^{-1}(y)$ mit $y = f(x)$.

Folgerung II
Sei X eine endliche Menge, dann sind für eine Abbildung $f : X \to Y$ folgende Aussagen äquivalent:
(i) f ist injektiv
(ii) f ist surjektiv
(iii) f ist bijektiv.
Beweis: Man zeigt dies durch Auszählen mit dem Schubfachprinzip.

Komposition von Abbildungen
Sind X, Y, Z Mengen, $f : X \to Y,\ g : Y \to Z$, dann bezeichnet $g \circ f : X \to Z, x \mapsto g(f(x)) =: (g \circ f)(x)$ die Komposition von f und g. $(X \xrightarrow{f} Y \xrightarrow{g} Z)$.
Gibt es noch eine Menge W und $Z \xrightarrow{h} W$, dann ist $(h \circ g) \circ f = h \circ (g \circ f)$, denn:
Für $x \in X$ ist $((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x))) = h((g \circ f)(x)) = (h \circ (g \circ f))(x)$.
Wir definieren $Id_x : X \to X,\ x \mapsto x$ die identische Abbildung.

[5] oder Vektor in Spaltenschreibweise oder Spalte der Länge m
[6] transponierter Vektor
[7] $\exists$ ist Abk. für: es existiert

Lemma 2.1.
Vor.: $X, Y \neq \emptyset,\ f : X \to Y$.
Beh.: 1) f ist injektiv genau dann, wenn es eine Abbildung $g : Y \to X$ gibt, so daß $g \circ f = Id_x$.
2) f ist surjektiv genau dann, wenn es $g : Y \to X$ gibt, so daß $f \circ g = Id_Y$.
3) f ist bijektiv genau dann, wenn es $g : Y \to X$ gibt, so daß $g \circ f = Id_x,\ f \circ g = Id_Y$.
Dann ist auch $g = f^{-1}$.
Beweis: 1) f injektiv. Zu jedem $y \in f(X)$ gibt es genau ein $x \in X$ mit $y = f(x)$. Sei $g(y) := x$. Sei $x_o \in X$ beliebig, dann def. $g(y) = x_o$ für alle $y \in Y \setminus f(X)$. Dann ist $g : Y \to X$ und $g \circ f = Id_x$.
Umgekehrt: $g : Y \to X$ und $g \circ f = Id_x$. Wenn $f(x) = f(\tilde{x}),\ x, \tilde{x} \in X$, so $x = Id_x(x) = g(f(x)) = g(f(\tilde{x})) = Id_x(\tilde{x}) = \tilde{x}$, also ist f injektiv.
2) f surjektiv. $\forall\ y \in Y$ sei $x \in X$ fest mit $f(x) = y$. Wir def. $g(y) = x$. Dann $g : Y \to X$ und $f \circ g = Id_Y$.
Umgekehrt: $g : Y \to X$ und $f \circ g = Id_Y,\ y \in Y$, so daß $y = f(g(y))$, dann ist $f(g(y))$ Bild von $g(y)$ und f ist surjektiv.
3) Ist f bijektiv, dann ist 1) und 2) mit $g := f^{-1}$ erfüllt. Ist umgekehrt $g : Y \to X$ mit $g \circ f = Id_x$ und $f \circ g = Id_Y$ gegeben, dann ist wegen 1) und 2) f bijektiv und es gilt: $g = f^{-1}$. ■

Beispiel
1) $M = \{1, 2, 3, 4, 5\},\ N = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$.
Wir definieren f: $f(1) = 2, f(2) = 2, f(3) = 2, f(4) = 5, f(5) = 8, f(6) = 8$.
Dann folgt: $f(\{1, 2, 5, 6\}) = \{2, 8\},\ f^{-1}(\{2, 8\}) = \{1, 2, 3, 5, 6\}$,
$f^{-1}(\{2\}) = \{1, 2, 3\},\ f^{-1}(\{5\}) = \{4\},\ f^{-1}(\{9\}) = \emptyset,\ f(M) = \{2, 5, 8\},\ f^{-1}(N) = M$.
2) Sei $M \neq \emptyset$. Die Menge der bijektiven Abbildungen von M auf sich bezeichnet man mit $\Sigma(M)$. Man nennt $\Sigma(M)$ auch die symmetrische Gruppe auf M, $\pi \in \Sigma(M)$ heißt Permutation.

Mit diesem Einschub können wir die Lösung von Gleichungssystemen besser verstehen. Das Gleichungssystem lösen bedeutet dann, eine Methode entwickeln, um die Menge Lös(A, b) zu berechnen. Mathematisch bedeutet dies, wir suchen ein $k \in \mathbb{N}$ und eine explizite Bijektion $\phi : \mathbb{R}^k \to$ Lös$(A, b) \subset \mathbb{R}^n$. ϕ heißt Parametrisierung.

2.2 Das Gaußsche Eliminationsverfahren

Wir betrachten das Gleichungssystem

$$\begin{array}{rrrrrrcr} x_1 & +3x_2 & -2x_3 & & +2x_5 & & = & 0 \\ 2x_1 & +6x_2 & -5x_3 & -2x_4 & +4x_5 & -3x_6 & = & -1 \\ & & 5x_3 & +10x_4 & & +15x_6 & = & 5 \\ 2x_1 & +6x_2 & & +8x_4 & +4x_5 & +18x_6 & = & 6 \end{array}$$

Die erweiterte Matrix hat die Form

$$\begin{pmatrix} 1 & 3 & -2 & 0 & 2 & 0 & 0 \\ 2 & 6 & -5 & -2 & 4 & -3 & -1 \\ 0 & 0 & 5 & 10 & 0 & 15 & 5 \\ 2 & 6 & 0 & 8 & 4 & 18 & 6 \end{pmatrix}$$

Wir addieren das -2fache der 1.Zeile zur 2. und 4.Zeile.

$$\begin{pmatrix} 1 & 3 & -2 & 0 & 2 & 0 & 0 \\ 0 & 0 & -1 & -2 & 0 & -3 & -1 \\ 0 & 0 & 5 & 10 & 0 & 15 & 5 \\ 0 & 0 & 4 & 8 & 0 & 18 & 6 \end{pmatrix}$$

Nun multiplizieren wir die 2 Zeile mit -1. Weiter addieren wir das -5fache der 2.Zeile zur 3.Zeile und das -4fache der 2.Zeile zur 4.Zeile.

$$\begin{pmatrix} 1 & 3 & -2 & 0 & 2 & 0 & 0 \\ 0 & 0 & 1 & 2 & 0 & 3 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 6 & 2 \end{pmatrix}$$

Wir vertauschen jetzt die 3. mit der 4.Zeile und multiplizieren die 3.Zeile mit $\frac{1}{6}$.

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

Zuletzt addieren wir das -3fache der 3.Zeile zur 2.Zeile und das 2fache der 2.Zeile zur 1.Zeile.

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

Diese erweiterte Matrix entspricht jetzt dem Gleichungssystem

$$\begin{array}{rrrrrrrr} x_1 & +3x_2 & & +4x_4 & +2x_5 & & = & 0 \\ & & x_3 & +2x_4 & & & = & 0 \\ & & & & & x_6 & = & \frac{1}{3} \end{array}$$

Dies bedeutet:

$$\begin{array}{rcrrr} x_1 & = & -3x_2 & -4x_4 & -2x_5 \\ x_3 & = & & -2x_4 & \\ x_6 & = & \frac{1}{3} & & \end{array}$$

x_2, x_4, x_5 sind freie Variable, sie können unabhängige Werte $\lambda_1, \lambda_2 \lambda_3 \in \mathbb{R}$ annehmen.
Dann folgt: $x_1 = -3\lambda_1 - 4\lambda_2 - 2\lambda_3,\ x_2 = \lambda_1,\ x_3 = -2\lambda_2,\ x_4 = \lambda_2,\ x_5 = \lambda_3,\ x_6 = \frac{1}{3}.$ $(*)$
Damit ist $\text{Lös}(A, b) = \{(x_1, x_2, x_3, x_4, x_5, x_6) \mid x_k \text{ aus } (*)\}$.

Einige summarische Aussagen
Mit $Ax = 0$ ist das sog. homogene Gleichungssystem definiert (H),
mit $Ax = b,\ b \neq 0$ das sog. inhomogene Gleichungssystem (IH).
Es gilt dann sofort:
1) H hat immer eine Lösung, nämlich $(0, \ldots, 0)$.
2) Ist x Lösung von H, dann ist $\lambda \cdot x,\ \lambda \in \mathbb{R}$ Lösung von H.
3) Sind x, y Lösung von H, dann ist auch $x + y$ Lösung von H.
4) Sind x^k Lösungen von H, dann auch $x = \sum \lambda_k x^k$ (Linearkombination).
5) Ist y Lösung von (IH), x Lösung von (H), dann ist $y + x$ Lösung von (IH).
6) Jede Lösung von (IH) hat die Form $y + x$, wobei y Lösung von (IH), x Lösung von H.
Bew.: $y, \tilde{y}$ Lösung von (IH): $Ay = b,\ A\tilde{y} = b$. Dann $A(\tilde{y} - y) = 0,\ x = \tilde{y} - y$ Lösung von H und somit $\tilde{y} = y + x$. ■

Wir werden nun Operationen mit den Gleichungen eines gegebenen Gleichungssystems einführen, die uns bei der Bestimmung der Lösungsmenge nützlich sein werden.
Sei das folgende lineare Gleichungssystem S gegeben:

$$\begin{array}{rrrrrr} a_{11}x_1 & +a_{12}x_2 & +\cdots & +a_{1n}x_n & = & b_1 \\ \vdots & & & & & \vdots \\ a_{m1}x_1 & +a_{m2}x_2 & +\cdots & +a_{mn}x_n & = & b_m \end{array}$$

Typ 1. Sei $c \neq 0$ eine Zahl, $1 \leq k \leq m$, dann sei S_1 das folgende System:

$$\begin{array}{rrrrrr} a_{11}x_1 & +a_{12}x_2 & +\cdots & +a_{1n}x_n & = & b_1 \\ \vdots & & & & & \vdots \\ ca_{k1}x_1 & +ca_{k2}x_2 & +\cdots & +ca_{kn}x_n & = & cb_k \\ \vdots & & & & & \vdots \\ a_{m1}x_1 & +a_{m2}x_2 & +\cdots & +a_{mn}x_n & = & b_m \end{array}$$

Typ 2. Seien $1 \leq i, k \leq m$; dann sei S_2 das folgende System:

$$\begin{array}{rrrrrr} a_{11}x_1 & +a_{12}x_2 & +\cdots & +a_{1n}x_n & = & b_1 \\ \vdots & & & & & \vdots \\ (a_{i1} + a_{k1})x_1 & +(a_{i2} + a_{k2})x_2 & +\cdots & +(a_{in} + a_{kn})x_n & = & b_i + b_k \\ \vdots & & & & & \vdots \\ a_{m1}x_1 & +a_{m2}x_2 & +\cdots & +a_{mn}x_n & = & b_m \end{array}$$

Typ 3. Seien $1 \leq i, k \leq m$; dann sei S_3 das folgende System:

$$\begin{array}{rcccl} a_{11}x_1 & +a_{12}x_2 & +\cdots & +a_{1n}x_n & = & b_1 \\ \vdots & & & & \vdots & \\ a_{k1}x_1 & +a_{k2}x_2 & +\cdots & +a_{kn}x_n & = & b_k \\ \vdots & & & & \vdots & \\ a_{i1}x_1 & +a_{i2}x_2 & +\cdots & +a_{in}x_n & = & b_i \\ \vdots & & & & \vdots & \\ a_{m1}x_1 & +a_{m2}x_2 & +\cdots & +a_{mn}x_n & = & b_m \end{array}$$

(Die i-te und k-te Gleichung werden vertauscht.)

Dann gilt der folgende

Satz 2.1.

Die Operationen vom Typ 1,2,3 verändern die Lösungsmenge des Gleichungssystems nicht, d.h. es gilt $\text{Lös}(A,b) = \text{Lös}(S) = \text{Lös}(S_1) = \text{Lös}(S_2) = \text{Lös}(S_3)$.

Beweis: 1. Sei $x = (x_1, \ldots, x_n) \in \text{Lös}(S)$, dann gilt $\sum_{j=1}^{n} a_{ij}x_j = b_i$ für $i = 1(1)m$.

Wir betrachten die k-te Gleichung: $\sum_{j=1}^{n} a_{kj}x_j = b_k$.

Dann ist auch $c\sum_{j=1}^{n} a_{kj}x_j = cb_k$, die anderen Gleichungen sind auch erfüllt, also ist $x \in \text{Lös}(S)$. Folglich ist $\text{Lös}(S)$ bei beliebigen Operationen von Typ 1 in $\text{Lös}(S_1)$ enthalten; umgekehrt läßt sich S_1 durch eine Operation vom Typ 1 (nämlich durch Multiplikation der k-te Gleichung mit $\frac{1}{c}$) in S überführen, also müssen beide Lösungsmengen gleich sein.

2. Sei wieder $x = (x_1, \ldots, x_n) \in \text{Lös}(S)$, also $\sum_{j=1}^{n} a_{ij}x_j = b_i$ für $i = 1(1)m$.

Wir betrachten die i-te Gleichung und die k-te Gleichung: $\sum_{j=1}^{n} a_{ij}x_j = b_i$, $\sum_{j=1}^{n} a_{kj}x_j = b_k$.

Dann ist $\sum_{j=1}^{n} a_{ij}x_j + \sum_{j=1}^{n} a_{kj}x_j = b_i + b_k = \sum_{j=1}^{n}(a_{ij} + a_{kj})x_j$ also $x \in \text{Lös}(S_2)$ für beliebige Operationen vom Typ 2. Umgekehrt läßt sich S_2 durch Operationen der Typen 1 und 2 wieder in S überführen, also stimmen beide Lösungsmengen überein.

3. Eine Operation vom Typ 3 läßt sich aus Operationen der Typen 1 und 2 zusammensetzen, jedesmal bleibt die Lösungsmenge ungeändert. ■

Def.2.3.

Eine $m \times n$-Matrix $A = (a_{kj})$ heißt in Zeilenstufenform, wenn A in folgender Form schreibbar ist:

$$A = \begin{pmatrix} * & \cdots & & & & \cdots & \\ 0 & * & \cdots & & & & \vdots \\ \vdots & 0 & \cdots & 0 & * & \cdots & \\ & & & & 0 & * & \cdots \\ \vdots & \vdots & & & \vdots & 0 & \cdots \\ 0 & 0 & \cdots & \cdots & 0 & 0 & \cdots \end{pmatrix}$$

* bedeuten Elemente $\neq 0$; darunter nur Null

In diesem Fall sind folgende Aussagen gültig:

1. Es gibt $r \in \mathbb{N},\ 0 \leq r \leq m$, so daß für $1, \ldots, r$ Zeilen existieren, die nicht nur Nullelemente enthalten, ab der $r+1$ Zeile bis zur m-ten Zeile stehen nur Nullen.

2. Für alle $k,\ 1 \leq k \leq r$ sei $j_k := \min\{j \mid a_{kj} \neq 0\}$, dies ist der niedrigste Spaltenindex mit Eintrag ungleich Null. Dann gilt $1 \leq j_k \leq n$ und es folgt die Stufenbedingung $j_1 < j_2 < \cdots < j_r$.

Auch $r = 0$ ist möglich. Dies definiert die Nullmatrix.

3. Die Einträge * sind $a_{1j_1}, \ldots, a_{rj_r}$, alle $\neq 0$, und diese heißen Pivots [8] von A.

Vertauschen wir die Spalten so, daß in unserem Beispiel dieser Fall entsteht, dann können wir o.B.d.A. immer so verfahren, daß die Pivots in der Diagonalen sitzen, d.h. wir nehmen an, daß unsere erweiterte Matrix die Gestalt hat

[8] auch Pivotelemente [Angelpunkte, aus dem franz.]

$$A = \begin{pmatrix} a_{11} & \cdots & & \cdots & b_1 \\ 0 & a_{22} & \cdots & & \vdots \\ \vdots & 0 & \ddots & \vdots & \\ & \vdots & & a_{rr} & b_r \\ 0 & 0 & & 0 & b_{r+1} \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & & 0 & b_m \end{pmatrix}$$

Diese Struktur soll immer die Gestalt unseres Gelichungssystems annehmen, dann ist nach Vor. $a_{11} \neq 0, \ldots, a_{rr} \neq 0$. Da $b = (b_k)$ gegeben ist, werden wir die $b_{r+1}, \ldots, b_m$ zu untersuchen haben, ob es Lösungen gibt.

Lemma 2.2.
Gibt es ein $b_k \neq 0$ und $r+1 \leq k \leq m$, dann gibt es keine Lösung, d.h. die Menge $\text{Lös}(A, b)$ ist leer.
Beweis: k-te Gleichung: $0 \cdot x_1 + \cdots + 0 \cdot x_n = b_k \neq 0$. Daraus folgt, es gibt kein $\{x_k\}_1^n$, so daß diese Bedingung erfüllt ist. ■

Folgerung
Ist $b_{r+1} = \cdots = b_m = 0$, dann kann man Lösungen konstruieren, nämlich so:
Wir sagen, die Unbekannten $\{x_k \mid k = r+1(1)m\}$ heißen freie Variable und können beliebige Werte annehmen. Die Unbekannten $x_1, \ldots, x_r$ heißen gebundene Variable und werden durch die freien Variablen festgelegt. Wir argumentieren so:
Sei $l := m - r$ und sei $\lambda_1, \ldots, \lambda_l \in \mathbb{R}$ eine noch offene Parametermenge, so folgt: $x_{r+1} = \lambda_1, \ldots, x_n = \lambda_l$.
Nun kann man so rechnen: Wir beginnen mit der letzten (r-ten) Zeile $a_{rr}x_r + a_{r,r+1}\lambda_1 + \cdots + a_{rn}\lambda_l = b_r$.
Damit ist x_r berechenbar:

$$x_r = \frac{1}{a_{rr}}(b_r - a_{r,r+1}\lambda_1 - \cdots - a_{rn}\lambda_l), \text{ da } a_{rr} \neq 0.$$

In der $r-1$-ten Zeile stehen nur $x_r,\ x_{r-1}$, somit kann man x_r dort einsetzen und weiterrechnen

$$x_{r-1} = \frac{1}{a_{r-1,r-1}}(b_{r-1} - a_{r-1,r}x_r) \equiv d_{r-1,r-1}b_{r-1} + d_{r-1,r}b_r + c_{r-1,1}\lambda_1 + \cdots + c_{r-1,l}\lambda_l.$$

Diese Verfahren führt man bis x_1 fort und erhält analog

$$x_1 = d_{11}b_1 + d_{12}b_2 + \cdots + d_{1r}b_r + c_{11}\lambda_1 + \cdots + c_{1l}\lambda_l.$$

Somit gibt es eine Abbildung $\mathbb{R}^l \to \text{Lös}(A, b) \subset \mathbb{R}^n$, die wie folgt schreibbar ist:

$$(\lambda_1, \ldots, \lambda_l) \mapsto (x_1, \ldots, x_r, \lambda_1, \ldots, \lambda_k),\ r + k = n.$$

Damit haben wir eine Lösung erhalten.

Unser Beispiel:
Wir bringen die Matrix auf Standardform:

$$A = \begin{pmatrix} 1 & 3 & 0 & 4 & 2 & 0 & 0 \\ 0 & 0 & 1 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & \frac{1}{3} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \Leftrightarrow \begin{pmatrix} 1 & 0 & 0 & 4 & 2 & 3 & 0 \\ 0 & 1 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & \frac{1}{3} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} = \tilde{A}$$

Die Spalten 1,5 und 6 bleiben fest. Aus Spalte 2 wird Spalte 6, aus Spalte 6 wird Spalte 3 und aus Spalte 3 wird Spalte 2. Hierbei ist $r = 3$, und $a_{11} = 1,\ a_{22} = 1,\ a_{33} = 1$ sind die Pivots.

$$\text{Also } \tilde{A} \cdot \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \end{pmatrix} = A \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{pmatrix} \text{ mit } \begin{array}{lcll} y_1 & = & -4y_4 - 2y_5 - 3y_6 & (= x_1) \\ y_2 & = & -2y_4 & (= x_3) \\ y_3 & = & \frac{1}{3} & (= x_6) \end{array} \text{ und somit } \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_3 \\ x_6 \\ x_4 \\ x_5 \\ x_2 \end{pmatrix}.$$

Die hier vorgeführte Routine heißt das Gaußsche Eliminationsverfahren [9].
Dann gibt es eine Abbildung $\phi : \mathbb{R}^{n-r} \to \text{Lös}(\tilde{A}, \tilde{b}) = \text{Lös}(A, b) \subset \mathbb{R}^n$ (Parametrisierung der Lösung). Je nach Wahl der Parameter $\{\lambda_i\}_1^l$ erhält man verschiedene Lösungen. Damit ist ϕ injektiv.

[9] benannt nach Carl Friedrich Gauß (1777-1855) dt. Mathematiker

3 Mathematische Grundlagen

Aus der Vorlesung von Prof.Starke entnehmen wir die Begriffe Mengen, Relationen, Abbildungen, Mächtigkeit, wobei wir zur Abbildung auf die bereits im vorhergehenden Kapitel gemachten Ausführungen verweisen.

3.1 Gruppen

Def. 3.1.
Sei $G \neq \emptyset$ eine Menge und $\circ$ eine Verknüpfung, d.h. $\circ : G \times G \to G$ wofür gilt: $g_k \in G \Rightarrow g_1 \circ g_2 \in G$.
Seien folgende Bedingungen erfüllt:
(i) $\forall a, b, c \in G$ gilt $a \circ (b \circ c) = (a \circ b) \circ c$ (Assoziatiivität),
(ii) 1) $\exists e \in G$ mit $\forall\ a \in G$ gilt $e \circ a = a$ (neutrales Element),
2) $\forall\ a \in G\ \exists\ b \in G$ mit $b \circ a = e$ (Linksinverses Element) $(g = a \Rightarrow g^{-1} = a^{-1})$[10]
Dann heißt die Menge G eine Gruppe bzgl. $\circ$ [Schreibweise $(G, \circ)$].
(iii) Gilt zusätzlich für alle $a, b \in G : a \circ b = b \circ a$, dann heißt g abelsche Gruppe [11] (und $\circ$ heißt kommutativ).
Beispiele
1) $\mathbb{Z}$ mit $\circ = +$ ist abelsche Gruppe [Schreibweise $(\mathbb{Z}, +)$],
2) $\mathbb{Q}$ mit $\circ = +$ ist abelsche Gruppe, $\mathbb{Q} \setminus \{0\}$ mit $\circ = \cdot$ (Multiplikation) ist abelsche Gruppe; $\mathbb{Z} \setminus \{0\}$ mit $\circ = \cdot$ (Multiplikation) ist keine Gruppe, da es zu 2,3, etc. keine Inverses gibt ($e = 1$!).

Es folgt der wichtige
Satz 3.1.
Sei $(G, \circ)$ Gruppe, e neutrales Element. Dann gilt:
(i) $\forall\ a \in G$ gilt auch $a \circ e = a$,
(ii) Wenn $c \circ a = a$ für ein $c \in G$ und $\forall\ a \in G$, dann $c = e$,
(iii) Ist $b \circ a = e$, so ist auch $a \circ b = e$ und b ist eindeutig definiert.
Beweis:
(i) $a \in G$. Dann gibt es ein $b \in G$ mit $b \circ a = e$, weiterhin ein $d \in G$ mit $d \circ b = e$. Somit folgt:
$d \circ e = d \circ (b \circ a) = (d \circ b) \circ a = e \circ a = a$, d.h. $a = d \circ e = d \circ (e \circ e) = (d \circ e) \circ e = a \circ e$.
(ii) Mit $a = e$ in (i) gilt: $c = c \circ e = e$.
(iii) Es gibt $c \in G$ mit $c \circ b = e$, dann folgt:
$e = c \circ b = c \circ (e \circ b) = c \circ ((b \circ a) \circ b) = (c \circ (b \circ a)) \circ b = ((c \circ b) \circ a) \circ b = (e \circ a) \circ b = a \circ b$.
Die Eindeutigkeit sieht man so:
Sei $x \circ a = b \circ a = e \Rightarrow x = x \circ e = x \circ (a \circ b) = (x \circ a) \circ b = e \circ b = b$. Damit $x = b$ und b eindeutig. ■

Def.3.2.
Sei $(G, \circ)$ Gruppe. $U \subseteq G$ heißt Untergruppe von G, wenn $U \neq \emptyset$ und U bzgl. $\circ$ eine Gruppe ist.

Satz 3.2.
Sei $(G, \circ)$ Gruppe, $U \subseteq G,\ U \neq \emptyset$.
U ist Untergruppe g.d.w. (i) $\forall\ u, v \in U : u \circ v \in U$ und (ii) $u \in U \Rightarrow u^{-1} \in U$.
Beweis:
Nach Definition 3.2. erfüllt eine Untergruppe (i) und (ii). Wenn U aber die Bedingungen (i) und (ii) erfüllt, dann muß ein $e \in U$ existieren, und $e \in G$ neutrales Element von G. Da $u \neq \emptyset \Rightarrow u \in U$ und $u^{-1} \in U$. Dann ist aber nach (i) $e = u \circ u^{-1} \in U$. Die anderen Bedingungen aus Def. 3.1. gelten in U, da sie in ganz G gelten. ■

Beispiele
(i) $(\mathbb{Z}, +)$ ist Untergruppe von $(\mathbb{Q}, +)$. $(\mathbb{N}, +)$ ist keine Untergruppe von $(\mathbb{Z}, +)$, da zu $n \in \mathbb{N}$ kein $n^{-1} \in \mathbb{N}$ existiert.
(ii) $n\mathbb{Z} := \{nz \mid z \in \mathbb{Z}\},\ n \in \mathbb{N}$. Dann ist $n\mathbb{Z}$ Untergruppe von $(\mathbb{Z}, +)$.
Beweis: (1) $n\mathbb{Z} \neq \emptyset$, da $0 \in n\mathbb{Z}$,
(2) $nz_1, nz_2 \in n\mathbb{Z} \Rightarrow nz_1 + nz_2 = n(z_1 + z_2) \in n\mathbb{Z}$,
(3) $nz \in n\mathbb{Z}$, dann auch $-nz = n(-z) \in n\mathbb{Z}$.
(iii) Bewegungen eines Würfels bzgl. gegebenen Achsen, die bei Drehung den Würfel in sich überführen:
1. Achsen durch Flächenmitten, $\alpha = 90^o, 180^o, 270^o \Rightarrow 3 \cdot 3 = 9$ Drehungen.
2. Raumdiagonalen 4 Stück, Drehungen um $120^o, 240^o$, d.h. $4 \cdot 2 = 8$ Drehungen.
3. Achsen durch die Mitten gegenüberliegender Kanten: Drehung um $180^o \Rightarrow 6$ Drehungen.
$\sum$ Drehungen $= 23 + 1$, 1 Identität, d.h. 24 verschiedene Drehungen möglich.
$\Rightarrow$ Jede Symmetrie bildet eine Raumdiagonale in sich ab $\Rightarrow$ Permutation von 4 Raumdiagonalen, $1, 2, 3, 4 \Rightarrow$ $\sum\{1, 2, 3, 4\}$ Gruppe. Diese hat 24 Elemente $(4! = 1 \cdot 2 \cdot 3 \cdot 4 = 24)$.

[10] Das inverse Element von a wird auch mit a^{-1} bezeichnet.
[11] benannt nach Niels Henrik Abel (1802-1829) norweg. Mathematiker

Def.3.3.
Seien $(G,\circ)$, $(H,*)$ Gruppen. $f: G \to H$ heißt Homomorphismus, falls $f(g\circ h) = f(g) * f(h)\ \forall\ g,h \in G$ gilt.
Wenn f ein surjektiver Homomorphismus ist, bezeichnet man f als Epimorphismus.
Wenn f ein injektiver Homomorphismus ist, bezeichnet man f als Monomorphismus.
Wenn f ein bijektiver Homomorphismus ist, bezeichnet man f als Isomorphismus.
Falls $G = H$ ist und f ein Homomorphismus, dann bezeichnet man f als Automorphismus.

Beispiele
1) Sei $f: (\mathbb{Z},+) \to (\mathbb{R}\setminus\{0\},\cdot)$ mit $f(z) = r^z,\ r \in \mathbb{R}$ fixiert.
Dann ist f ein Homomorphismus, weil $f(z_1+z_2) = r^{z_1+z_2} = r^{z_1}\cdot r^{z_2} = f(z_1)\cdot f(z_2)$.

2) $P = \{x \in \mathbb{R} \mid x > 0\}$, $(P,\cdot)$ ist Gruppe (mit Multiplikation in den reellen Zahlen).
$\log: (P,\cdot) \to (\mathbb{R},+),\ \log(x_1\cdot x_2) = \log(x_1)+\log(x_2) \Rightarrow$ log ist ein Homomorphismus von $(P,\cdot)$ auf $(\mathbb{R},+)$.
Sei $x \in \mathbb{R}$, dann ist $x = \log(10^x)$ und somit log ein Epimorphismus.
Aus $\log x = \log y$ folgt $x = 10^{\log x} = 10^{\log y} = y$ und damit ist log ein Isomorphismus.

Lemma 3.1.
Seien $(G,\circ),(\tilde{G},*)$ Gruppen, $e,\tilde{e}$ die zugehörigen neutralen Elemente, $f: G \to \tilde{G}$ ein Homomorphismus.
Dann: $f(e) = \tilde{e},\ f(a^{-1}) = [f(a)]^{-1}\ \forall\ a \in G$.
Beweis: $\tilde{e} = f(e)^{-1} * f(e) = f(e)^{-1} * f(e\circ e) = f(e)^{-1} * f(e) * f(e) = \tilde{e} * f(e) = f(e)$,
$f(a^{-1}) * f(a) = f(a^{-1}\circ a) = f(e) = \tilde{e}$, d.h. $f(a^{-1}) = [f(a)]^{-1}$. ■

Def.3.4.
Seien $(G,\circ),(\tilde{G},*)$ Gruppen, $e,\tilde{e}$ die zugehörigen neutralen Elemente, $f: G \to \tilde{G}$ ein Homomorphismus.
Dann heißt $\ker f := \{x \in G \mid f(x) = \tilde{e}\}$ Kern von f und $\mathrm{Im} f := \{f(x) \mid x \in G\}$ das Bild von f.

Lemma 3.2.
Seien $(G,\circ),(\tilde{G},*)$ Gruppen, $f: G \to \tilde{G}$ ein Homomorphismus.
Dann sind $\ker f$ und $\mathrm{Im} f$ Untergruppen von G und $\tilde{G}$.

Bemerkung $\ker f = f^{-1}(\tilde{e})$ ist das Urbild von $\tilde{e}$.

Lemma 3.3.
Seien $(G,\circ),(\tilde{G},*)$ Gruppen, $e,\tilde{e}$ die zugehörigen neutralen Elemente, $f: G \to \tilde{G}$ ein Homomorphismus.
f ist ein Monomorphismus g.d.w. $\ker f = \{e\}$.
Beweis:
1) f ist injektiv $\Rightarrow \tilde{e}$ hat höchstens ein Urbild. Da $f(e) = \tilde{e}$ folgt $\ker f = f^{-1}(\tilde{e}) = \{e\}$.

2) $\ker f = \{e\},\ a,b \in G$ mit $f(a) = f(b)$. Aus $f(a^{-1}\circ b) = f(a)^{-1} * f(b) = f(a)^{-1} * f(a) = \tilde{e}$ folgt $a^{-1}\circ b \in \ker f = \{e\}$und somit $a = b$, d.h. f ist injektiv. ■

Def.3.5.
Sei $(G,\cdot)$ Gruppe, $U \subset G$ Untergruppe von G.
Wenn $g \in G$ ist, so heißt $g\cdot U := \{g\cdot u \mid u \in U\}$ Linksnebenklasse [bzgl. g] von U in G und
$U\cdot g := \{u\cdot g \mid u \in U\}$ Rechtsnebenklasse [bzgl. g] von U in G.

Interessant ist der Fall, daß Links- und Rechtsnebenklassen zusammenfallen.

Def.3.6.
Eine Untergruppe $N \subseteq G$ heißt Normalteiler, falls $\forall\ g \in G : g\cdot N = N\cdot g$
(Man schreibt $N \trianglelefteq G$ oder $N \triangleleft G$ wenn $N \neq G$).

Folgerung
Bei kommutativen Gruppen ist jede Untergruppe ein Normalteiler.

Def.3.7.
Sei $(G,\cdot)$ Gruppe, $N \trianglelefteq G$. Mit G/N bezeichnen wir die Menge der Nebenklassen $\{a\cdot N \mid a \in G\}$.
Auf G/N definieren wir eine Verknüpfung: $a,b \in G$, dann $(aN)\bullet(bN) := (a\cdot b)N$.
$(G/N,\bullet)$ heißt die Faktorgruppe G nach N.

Satz 3.3.
Sei $(G,\cdot)$ Gruppe, $N \trianglelefteq G$. Dann ist G/N mit Def.3.7. eine Gruppe.
Beweis:
Wir zeigen zuerst, daß $\bullet$ aus Def.3.7. eine Abbildung ist; diese muß unabhängig von a und b sein.
Sei $aN = \hat{a}N,\ bN = \hat{b}N$. Dann ist $\hat{a} = an_1,\ \hat{b} = bn_2,\ n_1,n_2 \in N$. Aus $(\hat{a}\cdot\hat{b})N = (an_1\cdot bn_2)N$ und $N \trianglelefteq G$ folgt $n_1 b \in Nb = bN$, d.h. es gibt $n_3 \in N$, so daß $n_1 b = bn_3$. Dann folgt $(\hat{a}\cdot\hat{b})N = (abn_3n_2)N = (ab)N$, da $n_3n_2N = N$ unabhängig von a,b.
Assoziativität:
$(aN\bullet bN)\bullet cN = (a\cdot b)N\bullet cN = ((a\cdot b)\cdot c)N = (a\cdot(b\cdot c))N = aN\bullet(b\cdot c)N = aN\bullet(bN\bullet cN),\ a,b,c \in G$.

Neutrales Element: $N = eN$ ist neutrales Element, denn $N \bullet (aN) = (a \cdot a)N = aN \ \forall\ a \in G$.
Inverses: $a \in G \Rightarrow (aN) \bullet (a^{-1}N) = (a \cdot a^{-1})N = eN = N$, damit ist $a^{-1}N$ zu aN invers. ■

Gruppen, die keine Normalteiler besitzen, heißen einfach.

Beispiel
$G = (\mathbb{Z}, +)$. Sei $m \in \mathbb{N},\ U := m\mathbb{Z}$. Damit ist $U \trianglelefteq \mathbb{Z}$.
Sei $r \in \mathbb{Z}$. $\quad r + m\mathbb{Z} := \{x \in \mathbb{Z} \mid x \equiv r \mod m\}$.
Damit ist $\mathbb{Z} = \bigcup_{r=0}^{m-1} (r + m\mathbb{Z})$.
$\mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z}$ Restklassen $\mod m$.

Sei $\bar{x} := x + m\mathbb{Z}$. Aus Satz 3.3. folgt dann: $\bar{x} + \bar{y} = \overline{x + y} = x + y + m\mathbb{Z}$.
$f : \mathbb{Z} \to \mathbb{Z}_m$ mit $f(x) := \bar{x}$ ist ein Homomorphismus von $\mathbb{Z}$ auf $\mathbb{Z}_m$.

Satz 3.4. (Homomorphiesatz für Gruppen
Seien $(G, \circ)$, $(\tilde{G}, *)$ Gruppen, $f : G \to \tilde{G}$ ein Homomorphismus. Dann gilt:

$$G/\ker f \cong \mathrm{Im} f \quad \text{(isomorph)}.$$

Beweis:
Sei $i : G/\ker f \to \mathrm{Im} f$ definiert durch $i(a \ \ker f) = f(a),\ a \in G$.
i ist Abbildung, d.h. unabhängig von der Wahl von a.
Sei $a \ \ker f = \tilde{a} \ \ker f$, d.h. $\tilde{a} = ax,\ x \in \ker f$.
Somit gilt $i(\tilde{a} \ \ker f) = f(\tilde{a}) = f(ax) = f(a) * f(x) = f(a) = i(a \ \ker f)$.
i ist Homomorphismus:
Mit $a, b \in G$ ist $i(a \ \ker f \bullet b \ \ker f) = i((a \circ b)\ker f) = f(a \circ b) = f(a) * f(b) = i(a \ \ker f) * i(b \ \ker f)$.
i ist surjektiv: Sei $\tilde{a} \in \mathrm{Im} f$. Dann gibt es ein $a \in G$ mit $f(a) = \tilde{a}$, d.h. $i(a \ \ker f) = f(a) = \tilde{a}$.
i ist injektiv, d.h. $\ker i = \{\ker f\}$:
$\ker i = \{a \ \ker f \mid a \in G,\ i(a \ \ker f) = \tilde{e}\} = \{a \ \ker f \mid a \in G \text{ mit } f(a) = \tilde{e}\} = \{a \ \ker f \mid a \in \ker f\} = \{\ker f\}$. ■

3.2 Ringe und Körper

Def.3.8.
$R \neq 0$. Auf R seien 2 Operationen $+$ und $\cdot$ erklärt, d.h.
$+ : R \times R \to R$ mit $(a, b) \mapsto a + b$ und $\cdot : R \times R \to R$ mit $(a, b) \mapsto a \cdot b =: ab$, so daß gilt:
(i) $(R, +)$ ist abelsche Gruppe,
(ii) $\forall\ a, b, c \in R$ gilt: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ und es existiert ein $e \in R$ mit $e \cdot a = a = a \cdot e\ \forall\ a \in R$,
(iii) $\forall\ a, b, c \in R$ gilt: $(a + b) \cdot c = a \cdot c + b \cdot c$ (Distributivgesetz) und $a \cdot (b + c) = a \cdot b + a \cdot c$.
Dann heißt die Menge ein Ring.
(iv) Ist $R \setminus \{e\}$ bzgl. $\cdot$ eine kommutative Gruppe, dann heißt R ein Körper.

Beispiel
1) $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sind Ringe, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sind Körper.
2) $(\mathbb{Z}_m, +, \cdot)$ ist ein Ring. Es gilt dann (siehe Abschnitt 3.1.):

$$(r + m\mathbb{Z})(s + m\mathbb{Z}) \equiv r \cdot s + m\mathbb{Z} \ (\quad \mod m).$$

Ist $m \notin \mathbb{P},\ m = r \cdot s,\ r \neq m \neq s$, so gilt sogar

$$(r + m\mathbb{Z})(s + m\mathbb{Z}) \equiv r \cdot s + m\mathbb{Z} = m\mathbb{Z}.$$

Damit kann in $\mathbb{Z}_m$ das Produkt $a \cdot b = 0$ sein, auch für $a \neq 0$ und $b \neq 0$.
$\mathbb{Z}_m$ ist kein Körper, denn sei $t + m\mathbb{Z} \in \mathbb{Z}_m,\ (t + m\mathbb{Z})(r + m\mathbb{Z}) = 1 + m\mathbb{Z}$, so

$$\begin{aligned} s + m\mathbb{Z} &= (1 + m\mathbb{Z})(s + m\mathbb{Z}) \\ &= ((t + m\mathbb{Z})(r + m\mathbb{Z}))(s + m\mathbb{Z}) \\ &= (t + m\mathbb{Z})((r + m\mathbb{Z})(s + m\mathbb{Z})) \\ &= (t + m\mathbb{Z})(0 + m\mathbb{Z}) = m\mathbb{Z} \qquad \Rightarrow m \mid s \text{ Widerspruch.} \end{aligned}$$

Def.3.9
(i) R Ring, dann ist R nullteilerfrei, falls $\forall\ a, b \in R$ gilt: Wenn $a \cdot b = 0$, so $a = 0$ oder $b = 0$.

(ii) R heißt Integritätsbereich, falls R nullteilerfrei ist, mindestens zwei Elemente enthält und $a \cdot b = b \cdot a$ für alle $a, b \in R$ gilt.
Obige Beispiele sind Integritätsbereiche.

Lemma 3.4.
Sei K ein Körper. Dann:
(i) $a \in K \Rightarrow \ a \cdot 0 = 0 \cdot a = 0$,
(ii) K ist nullteilerfrei
Beweis:
(i) Da $0 \cdot a + 1 \cdot a = (0+1) \cdot a = 1 \cdot a = 0 + 1 \cdot a$, so $a = 0$.
(ii) Seien $a, b \in K$ und $a \cdot b = 0$. Wenn $a \neq 0$, dann gibt es ein $c \in K$ mit $c \cdot a = 1$.
Damit ist $b = 1 \cdot b = (c \cdot a) \cdot b = c \cdot (a \cdot b) = c \cdot 0 = 0$. ■

Beispiele
1) Sei X Menge, R kommutativer Ring. Sei A die Menge der Abbildungen von $X \to R$ mit den Operationen $f + g : x \mapsto f(x) + g(x)$ und $f \cdot g : x \mapsto f(x) \cdot g(x),\ x \in X$. Dann ist $(A, +, \cdot)$ ein kommutativer Ring und i.a. nicht nullteilerfrei.

2) Sei $(G, +)$ abelsche Gruppe und $\mathrm{End}(G) := \{f \mid f : G \to G \text{ Homomorphismus}\}$.
Sei für $f, g \in \mathrm{End}(G)$: $f + g : x \mapsto f(x) + g(x),\ f \circ g : x \mapsto f(g(x))$. Dann ist $(\mathrm{End}(G), +, \circ)$ ein Ring, der sog. Endomorphismenring von G.

3) Binärmathematik: Sei $R = \{0, 1\}$ und folgende Operationen definiert:

$\oplus$	0	1
0	0	1
1	1	0

$\odot$	0	1
0	0	0
1	0	1

Dann ist $(R, \oplus, \odot)$ ein Körper.

4) $\forall\ p \in \mathbb{P}$ ist $\mathbb{Z}_p$ ein Körper. $p = 2$ und $R = \{\bar{0}, \bar{1}\}$ mit $\bar{0} = 0 + 2\mathbb{Z},\ \bar{1} = 1 + 2\mathbb{Z},\ \overline{x+y} = \bar{x} + \bar{y},\ \overline{x \cdot y} = \bar{x} \cdot \bar{y}$.
Dann erhält man

$+$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

$\cdot$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$

, d.h. es gibt eine Bijektion $i : \begin{cases} \mathbb{Z}_2 \to \{0,1\} \\ \bar{0} \mapsto 0 \\ \bar{1} \mapsto 1 \end{cases}$
Man kann jetzt folgendes definieren:

Def.3.10
$(R, +, \cdot),\ (S, \oplus, \odot)$ seien Ringe, $f : R \to S$ Abbildung.
f heißt (Ring-)Homomorphismus, wenn $\forall\ x, y \in R$ gilt:
$f(x+y) = f(x) \oplus f(y),\ f(x \cdot y) = f(x) \odot f(y)$. Ist der Homomorphismus bijektiv, dann heißt er Isomorphismus.
(d.h. $(\mathbb{Z}_2, +, \cdot) \leftrightarrow (\{0,1\}, \oplus, \odot)$ ist Isomorphismus)

Def.3.11.
Sei $(K, +, \circ)$ Körper.
(i) $\forall\ a \in K,\ n \in \mathbb{N}$ definieren wir $n \cdot a = \underbrace{a + a + \cdots + a}_{n\text{-mal}} = (\underbrace{1 + 1 + \cdots + 1}_{n\text{-mal}}) \circ a = (n \cdot 1) \circ a$,
Die 1 ist dabei das neutrale Element bzgl. $\circ$.
(ii) Ist $m \cdot 1 \neq 0\ \forall\ m \in \mathbb{N}$, dann hat K die Charakteristik 0 ($\mathrm{char}K = 0$). Ist n die kleinste Zahl so, daß $n \cdot 1 = 0$, dann $\mathrm{char}K = n$.
(z.B. $\mathrm{char}\mathbb{Z}_2 = 2,\ \mathbb{Q}, \mathbb{R}, \mathbb{C}$ haben Charakteristik 0.)
Im folgenden wird zwischen $\cdot$ und $\circ$ nicht mehr unterschieden.

Folgerung
Wenn K Körper mit $\mathrm{char}K \neq 0$, dann $\mathrm{char}K = p \in \mathbb{P}$.
Beweis: Annahme: $\mathrm{char}K = pq,\ p \neq 1,\ q \neq 1,\ p, q \in \mathbb{N}$. Dann
$0 = (pq) \cdot 1 = (\underbrace{1 + \cdots + 1}_{pq\text{-mal}}) = (\underbrace{1 + \cdots + 1}_{p\text{-mal}}) \cdot (\underbrace{1 + \cdots + 1}_{q\text{-mal}}) = (p \cdot 1) \cdot (q \cdot 1)$.
K ist nullteilerfrei, so $p \cdot 1 = 0$ oder $q \cdot 1 = 0$. Widerspruch! ■
(Daraus folgt also auch $\mathrm{char}\mathbb{Z}_p = p$)

4 Vektorräume

4.1 Vektorräume und Untervektorräume

Def.4.1.
Sei $\mathbb{K}$ ein Körper. Ein $\mathbb{K}$-Vektorraum oder Vektorraum über $\mathbb{K}$ ist eine abelsche Gruppe mit einer Verknüpfung $\mathbb{K} \times \mathbb{V} \to \mathbb{V},\ (\lambda, v) \mapsto \lambda v$, so daß $\forall\ a, b \in \mathbb{V},\ \forall\ \lambda, \mu \in \mathbb{K}$ gilt:

(i) $\lambda(a+b) = \lambda a + \lambda b$,
(ii) $(\mu+\lambda)a = \mu a + \lambda a$,
(iii) $(\mu\lambda)a = \mu(\lambda a),\ 1 \cdot a = a$

Bemerkung Für $\mathbb{K}$ kann man u.a. $\mathbb{R},\ \mathbb{C},\ \mathbb{Z}_2$ oder $\mathbb{Z}_p$ nehmen.

Beispiele
1) $\mathbb{V} = \mathbb{R}$ mit Addition und Multiplikation.
2) Die Menge der $m \times n$-Matrizen bilden einen Vektorraum, man führt Addition und Multiplikation ein.
3) Menge der Tupel $\{(x_1, \ldots, x_n)\} = \mathbb{R}^n$ bilden einen Vektorraum.
4) M sei eine Menge, $\mathbb{V}$:= Menge der Abbildungen von $M \to \mathbb{R}$. Für $f, g \in \mathbb{V},\ \alpha \in \mathbb{R}$ sei

$$(f+g)(m) := f(m) + g(m),\ (\alpha f)(m) := \alpha f(m),\ m \in M.$$

Mit diesen Verknüpfungen ist $\mathbb{V}$ ein Vektorraum über $\mathbb{R}$.

Lemma 4.1.
Sei $\mathbb{V}$ ein Vektorraum über $\mathbb{K}$. Dann gilt:
1) $\lambda \cdot 0 = 0\ \forall\ \lambda \in \mathbb{K};$ 0 sei dabei das Nullelement in $\mathbb{V}$,
2) $0 \cdot v = 0\ \forall\ v \in \mathbb{V};$ 0 sei dabei das Nullelement in $\mathbb{K}$,
3) $\lambda(-v) = (-\lambda)v = -(\lambda v)\ \forall v \in \mathbb{V}\ \forall\ \lambda \in \mathbb{K}$,
4) Wenn $(\lambda \cdot v) = 0$, so $\lambda = 0$ oder $v = 0$.
Beweis:
1) und 2) offensichtlich.
3) $\lambda v + \lambda(-v) = \lambda(v + (-v)) = \lambda \cdot 0 = 0$, d.h. $\lambda(-v) = -(\lambda v)$.
$(-\lambda)v + \lambda v = ((-\lambda) + \lambda)v = 0 \cdot v = 0$, d.h. $-(\lambda v) = (-\lambda)v$.
4) Sei $\lambda \neq 0 \Rightarrow 0 = \lambda^{-1} \cdot 0 = \lambda^{-1}(\lambda v) = (\lambda^{-1}\lambda)v = 1 \cdot v = v$ ■

Def.4.2.
Sei $\mathbb{V}$ ein Vektorraum über $\mathbb{K},\ U \subseteq \mathbb{V}$. U heißt Unterraum oder Teilraum von $\mathbb{V}$, wenn U mit den auf $\mathbb{V}$ definierten Relationen gemäß Def.4.1. wieder ein Vektorraum ist.

Lemma 4.2.
Sei $\mathbb{V}$ ein Vektorraum über $\mathbb{K},\ U \subseteq \mathbb{V}$.
U ist Teilraum von $\mathbb{V}$ g.d.w. eine der beiden folgenden Eigenschaften erfüllt ist
(1) (i) $(U, +)$ ist Untergruppe von $(\mathbb{V}, +)$, (ii) Wenn $v \in U, \lambda \in \mathbb{K}$, dann auch $\lambda v \in U$,
(2) (i) $U \neq \emptyset$, (ii) $\forall\ u, v \in U\ \forall\ \lambda, \mu \in \mathbb{K}:\ \lambda u + \mu v \in U$.
Beweis:
(1) ist die Def.4.2.
(2) (i),(ii) ist notwendig, da die so gebildeten Elemente wieder in U liegen müssen.
Ist aber (i),(ii) in (2) erfüllt, dann sei $\lambda = \mu = 1$. Aus $u, v \in U$ folgt $u + v \in U$.
Setzt man $\lambda = -1,\ \mu = 0$, so folgt aus $u \in U : (-1)u = -u$ nach Lemma 4.1.(3) und $-u \in U$.
Sei $\mu = 0,\ u \in U,\ \lambda \in \mathbb{K}$ beliebig, dann ist auch $\lambda u \in U$. Somit ist U ein Unterraum. ■

Beispiele
1) $U = \{0\} \subseteq \mathbb{V}$ ist stets Unterraum von $\mathbb{V}$ (0 ist das neutrale Element bzgl. der Addition).
2) Eine Ebene in $\mathbb{R}^3$ ist ein Unterraum von $\mathbb{R}^3$.
$\mathbb{V} = \mathbb{R}^3 = \{(x, y, z) \mid x, y, z \in \mathbb{R}\}$, $\mathbb{V}$ ist $\mathbb{R}$-Vektorraum.
Sei $U := \{(x, y, z) \mid x, y, z \in \mathbb{R},\ ax + by + cz = 0,\ a, b, c \in \mathbb{R}\}$. U ist dann Unterraum:
$(0, 0, 0) \in U \Rightarrow U \neq \emptyset$.
Seien $(x_k, y_k, z_k) \in U,\ k = 1, 2$. Dann gilt $ax_1 + by_1 + cz_1 = 0 = ax_2 + by_2 + cz_2$.
Seien $\lambda, \mu \in \mathbb{R}$ beliebig gewählt. Dann ist

$$\lambda a x_1 + \lambda b y_1 + \lambda c z_1 = \lambda(a x_1 + b y_1 + c z_1) = \lambda \cdot 0 = 0$$

$$\mu a x_2 + \mu b y_2 + \mu c z_2 = \mu(a x_2 + b y_2 + c z_2) = \mu \cdot 0 = 0.$$

Somit ist $a(\lambda x_1 + \mu x_2) + b(\lambda y_1 + \mu y_2) + c(\lambda z_1 + \mu z_2) = 0$. Das aber bedeutet

$$\lambda(x_1, y_1, z_1) + \mu(x_2, y_2, z_2) = (\lambda x_1, \lambda y_1, \lambda z_1) + (\mu x_2, \mu y_2, \mu z_2) = (\lambda x_1 + \mu x_2, \lambda y_1 + \mu y_2, \lambda z_1 + \mu z_2) \in U,$$

damit ist U ein Unterraum.

4.2 Lineare Abhängigkeit, Basis, Dimension

Wir betrachten $\mathbb{V} = \mathbb{R}^n = \{(x_1, \dots, x_n) \mid x_i \in \mathbb{R}\}$.
Wir definieren spezielle Tupel: $e_1 = (1, 0, \dots, 0),\ e_2 = (0, 1, 0, \dots, 0),\ \dots,\ e_n = (0, \dots, 0, 1)$.
Sei $< X >$ der Durchschnitt über alle Teilräume von $\mathbb{V}$, die die Teilmenge X enthalten
($< X >:= \bigcap\{U \subseteq \mathbb{V} \mid U \text{ Teilraum},\ X \subseteq U\}$). $< X >$ heißt das Erzeugnis von X in $\mathbb{V}$.

Dann ist aber $\mathbb{V} =< \{e_1, \dots, e_n\} >$, weil $(x_1, \dots, x_n) := \sum_{k=1}^{n} x_k \cdot e_k$. Damit kann jedes $v \in \mathbb{V}$ eindeutig als solch eine Summe geschrieben werden.

Verallgemeinerung:
Def.4.3.
Sei $\mathbb{V}$ ein $\mathbb{K}$-Vektorraum.
1) $U \subset \mathbb{V}$. Die Teilmenge U heißt linear abhängig, falls es endlich viele paarweise verschiedene $u_k \in U$ und $\lambda_k \in \mathbb{K},\ k = 1(1)n$ gibt, so daß mindestens ein $\lambda_{k_o} \neq 0$ existiert und $\sum_{k=1}^{n} \lambda_k u_k = 0$ ist. Ist U nicht linear abhängig, dann heißt U linear unabhängig.
2) Sei $U \subseteq \mathbb{V},\ v \in \mathbb{V}$.
v heißt linear abhängig von U, falls es endlich viele $u_k \in U,\ \lambda_k \in \mathbb{K},\ k = 1(1)n$ gibt, so daß $v = \sum_{k=1}^{n} \lambda_k u_k$ gilt. Wir sagen, v ist Linearkombination der u_k.
3) Seien $v_k \in \mathbb{V},\ (k \in I)$.
$\{v_k\}_{k \in I}$ heißen linear unabhängig, falls für jede endliche Teilmenge $I_e \subseteq I$ immer aus $\sum_{k \in I_e} \lambda_k v_k = 0,\ \lambda_k \in \mathbb{K}$ folgt $\lambda_k = 0\ \forall\ k \in I_e$.

Beispiele
1. Sei $\mathbb{K}$ Körper, $\mathbb{V} = \mathbb{K}^n := \{(x_1, \dots, x_n) \mid x_k \in \mathbb{K}\}$.
$v_1 = (1, 0, \dots, 0),\ v_2 = (0, 1, 0, \dots, 0),\ \dots,\ v_n = (0, \dots, 0, 1)$.
Behauptung: $\{v_k\}$ sind linear unabhängig.
Beweis: Sei $0 = \sum_{k=1}^{n} \lambda_k v_k = (\lambda_1, \dots, \lambda_n)$, dies ist $(0, \dots, 0)$ g.d.w. $\lambda_1 = \dots = \lambda_n = 0$.

2. Sei $\mathbb{V}$ der Vektorraum, der aus den Potenzen von x gebildet wird ($x \mapsto p(x)$ polynomiale Abbildung), d.h. $v \in \mathbb{V}$ und $v = a_0 + a_1 x + \dots + a_n x^n$ (Polynome). Dann ist $v = 0$ g.d.w. $\lambda_k = a_k = 0$ für alle k.

Lemma 4.3.
Sei $\mathbb{V}$ ein $\mathbb{K}$-Vektorraum.
1) $U \subseteq \mathbb{V}$ und $0 \in U \Rightarrow U$ linear abhängig.
2) $\{v_1, \dots, v_n\}$ linear abhängig. Dann existiert ein v_k, so daß v_k linear abhängig von $\{v_1, \dots, v_{k-1}, v_{k+1}, v_n\}$.
3) $U \subseteq \mathbb{V}$ und $U \subseteq M \subseteq \mathbb{V}$. Ist U linear abhängig, so auch M.
4) Ist U eine linear unabhängige Teilmenge von $\mathbb{V}$ und $M \subseteq U$, so ist auch M linear unabhängig.
Beweis: als Übungsaufgabe

Def.4.4.
Sei $\mathbb{V}$ ein $\mathbb{K}$-Vektorraum.
1) $Y \subseteq \mathbb{V}$ heißt Erzeugendensystem von $\mathbb{V}$, falls $< Y >= \mathbb{V}$.
2) M heißt endlich, falls $M = \emptyset$ oder es gibt $n \in \mathbb{N}$, so daß M und $\{1, 2, \dots, n\}$ gleichmächtig sind. Dann schreiben wir $|M| < \infty$. Ist Y ein Erzeugendensystem von $\mathbb{V}$ und $|Y| < \infty$, dann heißt $\mathbb{V}$ endlich erzeugbar.
3) Sei $B \subseteq \mathbb{V}$. B sei ein linear unabhängiges Erzeugendensystem von $\mathbb{V}$. Dann heißt B Basis in $\mathbb{V}$.

Beispiele
1) Die Vektoren $e_1, \dots, e_n$ vom Beginn des Abschnitts bilden eine Basis in $\mathbb{R}^n$.
2) $\mathbb{V} = \left\{ \sum_{k=0}^{n} a_k x^k \mid n = 0, 1, \dots\ ,\ a_k \in \mathbb{R} \right\}$ Menge der Polynome über $\mathbb{R}$.
Dann ist $B = \{1, x, x^2, x^3, \dots\}$ Basis von $\mathbb{V}$.

Satz 4.1.
Sei $\mathbb{V}$ ein $\mathbb{K}$-Vektorraum und $B \subseteq \mathbb{V}$.
Dann sind folgende Aussagen äquivalent:
(1) B ist Basis in $\mathbb{V}$.
(2) B ist eine maximale, linear unabhängige Teilmenge von $\mathbb{V}$, d.h.: Ist $B \subsetneq B'$, so ist B' linear abhängig.
(3) B ist minimales Erzeugendensystem von $\mathbb{V}$, d.h.: Wenn $B' \subsetneq B$, dann $< B' > \neq \mathbb{V}$.
Beweis:
(1)$\Rightarrow$ (2): Sei $B \subsetneq B'$ und $b \in B' \setminus B$. Da $< B >= \mathbb{V}$, so $b = \sum_{k=1}^{n} \lambda_k b_k,\ b_k \in B,\ \lambda_k \in \mathbb{K}$.

Dann ist aber $0 = (-1) \cdot b + \sum_{k=1}^{n} \lambda_k b_k$. Da auch $b_k \in B'$, so ist B' linear abhängig.

(2)⇒ (3): Zuerst zeigen wir $\mathbb{V} =< B >$. Sei dazu $v \in \mathbb{V}$ beliebig gewählt. Wenn $v \in B$, dann ist auch $v \in < B >$ und wir sind fertig. Sei also $v \notin B$, dann $B \cup \{v\} \supset B$.
Nach Vorauss. aber ist $B \cup \{v\}$ linear abhängig. Dann gibt es $\lambda, \lambda_1, \ldots, \lambda_n \in \mathbb{K}$ und $b_1, \ldots, b_n \in B$, so daß $\lambda v + \sum_{k=1}^{n} \lambda_k b_k = 0$ und nicht alle λ, λ_k sind Null. Sei $\lambda = 0 \Rightarrow \sum_{k=1}^{n} \lambda_k b_k = 0$ und ein $\lambda_k \neq 0$.Dann sind die $\{b_k\}$ aber linear abhänigig und somit auch B linear abhängig, was ein Widerspruch zu (2) ist. Sei also $\lambda = 0$. Dann gilt $v = \sum_{k=1}^{n} (\lambda^{-1}\lambda_k) b_k \in B$. Somit ist B ein Erzeugendensystem von $\mathbb{V}$.

Nun betrachten wir $B' \subsetneq B$. Angenommen $< B' > = \mathbb{V}$. Sei $b \in B \setminus B'$, dann $b = \sum_{k=1}^{n} \lambda_k b'_k,\ b'_k in B,\ \lambda_k \in \mathbb{K}$, da B' ein Erzeugendensystem ist. Damit folgt $0 = (-1) \cdot b + \sum_{k=1}^{n} \lambda_k b'_k$, was zu einem Widerspruch führt, da B linear unabhängig ist.

(3)⇒ (1): als Übungsaufgabe ■

Folgerung
Sei $\mathbb{V}$ ein $\mathbb{K}$-Vektorraum, $\mathbb{V} =< M >,\ |M| < \infty$.
Dann gibt es eine Basis B von $\mathbb{V}$ mit $B \subseteq M$, insbesondere ist $|B| \leq |M|$.
Beweis: Sei $B \subseteq M$ und $< B > = \mathbb{V}$, $|B|$ minimal. Nach Satz 4.1. ist B eine Basis. ■

Zusammenstellung einiger mathematischer Tatsachen
A. M sei eine Menge mit Halbordnung $\sqsubset$.
(i) $\mathcal{K} \subseteq M$ heißt Kette, falls für $a, b \in \mathcal{K}$ immer gilt: $a \sqsubset b$ oder $b \sqsubset a$.
(ii) $\mathcal{K}$ heißt induktiv, falls es ein $m \in M$ gibt, so daß $k \sqsubset m$ für alle $k \in \mathcal{K}$ gilt. m heißt dann obere Schranke von $\mathcal{K}$.
(iii) $m_0 \in M$ heißt maximal in M, falls aus $m \in M$ und $m_o \sqsubset m$ folgt $m = m_o$.

B. Zornsches Lemma[12]: Sei $M \neq \emptyset$ halbgeordnete Menge. Ist jede Kette von $\mathcal{K} \subseteq M$ induktiv, so gibt es mindestens ein maximales Element in M.
Folgerung Sei $\mathbb{V}$ ein beliebiger $\mathbb{K}$-Vektorraum und U eine linear unabhängige Teilmenge von $\mathbb{V}$. Dann gibt es eine maximale, linear unabhängige Teilmenge B von $\mathbb{V}$ und $U \subseteq B$.

C. Jeder Vektorraum hat eine Basis. Da $U = \emptyset$ linear unabhängig ist, existiert nach obiger Folgerung eine maximale, linear unabhängige Teilmenge von $\mathbb{V}$, welche dann Basis ist. Leider kann man die Basis eines Vektorraums nicht immer angeben.

D. Je zwei Basen eines $\mathbb{K}$-Vektorraumes $\mathbb{V}$ haben die gleiche Mächtigkeit.

E. Sei $\mathbb{V}$ ein beliebiger $\mathbb{K}$-Vektorraum. Die Mächtigkeit einer Basis von $\mathbb{V}$ heißt Dimension von $\mathbb{V}$ ($\dim \mathbb{V}$).

Satz 4.2.
Sei $\mathbb{V}$ ein $\mathbb{K}$-Vektorraum, U Unterraum von $\mathbb{V}$, $\dim \mathbb{V} = n < \infty$. Dann gilt:
(i) $\dim U \leq \dim \mathbb{V}$.
(ii) Ist $\{u_1, \ldots, u_k\}$ Basis in U, dann gibt es eine Basis $\{u_1, \ldots, u_k, v_{k+1}, \ldots, v_n\}$ in $\mathbb{V}$.
(iii) Es gibt $U' \subset \mathbb{V}$, so daß U' Unterraum von $\mathbb{V}$ und $\mathbb{V} = U + U'$, $U \cap U' = \{0\}$.
(iv) $\dim U = \dim \mathbb{V}$ ist äquivalent mit $U = \mathbb{V}$.
Beweis:
(i) Ist $U = \{0\}$, so $\dim U = 0 \leq n$.
Sei $U \neq \{0\}$. Sei B linear unabhängige Teilmenge von U, dann ist $|B| \leq n$. Wir wählen B mit $|B|$ maximal. Nach Satz 4.1. ist dann B Basis von U. $\dim U = |B| \leq n = \dim \mathbb{V}$.
(ii) $\{u_1, \ldots, u_k\}$ Basis von U, $\{v_1, \ldots, v_n\}$ Basis von $\mathbb{V}$. Dann folgt die Behauptung, da man Basiselemente austauschen kann (Übungsaufgabe).
(iii) Aus (ii) folgt: $\{u_1, \ldots, u_k\}$ kann zur Basis von $\mathbb{V}$ ergänzt werden, wie angegeben.
Wir setzen $U' :=< \{v_{k+1}, \ldots, v_n\} > \Rightarrow U + U' = \mathbb{V}$.
Ist $v \in U \cap U'$, so $v = \sum_{i=1}^{k} a_i u_i$ und $v = \sum_{j=k+1}^{n} b_j v_j,\ a_i, b_j \in \mathbb{K}$, d.h. $0 = \sum_{i=1}^{k} a_i u_i - \sum_{j=k+1}^{n} b_j v_j$. Da die $\{u_1, \ldots, u_k, v_{k+1}, \ldots, v_n\}$ eine Basis bilden und deswegen linear unabhängig sind, folgt $a_i = 0 = b_j$ und damit $v = 0$.
(iv) Wenn $\dim U = \dim \mathbb{V} = n$, dann kann $\{u_1, \ldots, u_n\}$ in U als Basis für $\mathbb{V}$ genommen werden, d.h. $U =< \{u_1, \ldots, u_n\} > = \mathbb{V}$. ■

[12] benannt nach Max Zorn (1906-1993) dt. Mathematiker

4.3 Der Faktorraum

Wenn G Gruppe und U eine Untergruppe, dann war folgendes wahr:

$$G = \bigcup_{g \in G} gU$$

$$gU \cap hU = \emptyset \text{ oder } gU = hU,\ g, h \in G.$$

Kann das auf Vektorräume übertragen werden?

Sei $\mathbb{V}$ ein $\mathbb{K}$-Vektorraum, U Unterraum von $\mathbb{V}$.

Dann ist $\mathbb{V} = \bigcup_{v \in \mathbb{V}} (v + U)$ und $v + U \cap w + U = \begin{cases} \emptyset \text{ oder} \\ v + U = w + U \end{cases}$ (es ist $v + U = \{v + u \mid u \in U\}$).

Zu jeder disjunkten Zerlegung einer Menge gibt es eine Äquivalenzrelation. Somit gibt es auf $\mathbb{V}$ eine Relation $\sim$, so daß $v + U$ die Äquivalenzklassen sind. $v \sim w \Leftrightarrow v + U = w + U$. Hieraus folgt $v - w \in U$(!). Wenn $v - w \in U$, so $v = w + u,\ u \in U$.

Dann folgt: $v \sim w \Leftrightarrow v - w \in U$ ($a \equiv b \mod n \Leftrightarrow n \mid (a - b)$).

Eigenschaften von $\sim$:
1) $v \sim w, \lambda \in \mathbb{K} \Rightarrow \lambda v - \lambda w = \lambda(v - w) \in U \Rightarrow \lambda v \sim \lambda w$.

2) $v \sim w,\ s \sim t \Rightarrow v - w \in U,\ s - t \in U$, also $(v + s) - (w + t) = (v - w) + (s - t) \in U$, d.h. aus $v \sim w$ und $s \sim t$ folgt $v + s \sim w + t$.

Erfüllt eine Äquivalenzrelation die Eigenschaften 1) und 2), so heißt sie lineare Äquivalenzrelation.

Lemma 4.4.
Sei $\sim$ eine lineare Äquivalenzrelation auf $\mathbb{V}$. Dann gilt:

(i) Die Äquivalenzklasse von 0 ist ein Unterraum von $\mathbb{V}$.

(ii) Ist $v \in \mathbb{V}$, so ist die Äquivalenzklasse von v genau $v + U := \{v + u \mid u \in U\}$.

Beweis als Übungsaufgabe

Def.4.5.
Sei $\mathbb{V}$ ein $\mathbb{K}$-Vektorraum, U Unterraum von $\mathbb{V}$.

$$\mathbb{V}/U := \{v + U \mid v \in \mathbb{V}\},$$

wobei auf $\mathbb{V}/U$ gelten soll

(i) $(v + U) + (w + U) := (v + w) + U,\ v, w \in \mathbb{V}$,

(ii) $\lambda(v + U) := \lambda v + U,\ \lambda \in \mathbb{K},\ v \in \mathbb{V}$.

Dann heißt $\mathbb{V}/U$ der Quotienten- oder Faktorraum von $\mathbb{V}$ nach U. $\mathbb{V}/U$ ist dann ebenfalls ein $\mathbb{K}$-Vektorraum.

Satz 4.2. (Hauptsatz)
Sei $\mathbb{V}$ ein $\mathbb{K}$-Vektorraum, U Unterraum von $\mathbb{V}$. Dann gilt

a) Ist $B = \{v_i \mid i \in I\}$ eine Basis von $\mathbb{V}$, $B' = \{v_j \mid j \in J \subseteq I\}$ eine Basis von U, dann ist $\{v_k + U \mid k \in I \setminus J\}$ Basis in $\mathbb{V}/U$.

b) Ist $B = \{u_i \mid i \in I\}$ Basis von U, $B' = \{v_j + U \mid j \in J\}$ Basis von $\mathbb{V}/U$, dann ist $\{u_i \mid i \in I\} \cup \{v_j \mid j \in J\}$ Basis von $\mathbb{V}$.

c) Ist $\dim \mathbb{V} < \infty$, dann ist $\dim \mathbb{V} = \dim U + \dim \mathbb{V}/U$.

Beweis:

a) Sei $v+U \in \mathbb{V}/U$. Dann gilt $v = \sum\limits_{i\in I} a_i v_i,\ a_i \in \mathbb{K}$. Somit folgt

$$\begin{aligned} v+U &= \left(\sum_{i\in I} a_i v_i\right) + U \\ &= \left(\sum_{i\in J} a_i v_i + \sum_{i\in I\setminus J} a_i v_i\right) + U \\ &= \left(\sum_{i\in I\setminus J} a_i v_i\right) + \left(\sum_{i\in J} a_i v_i + U\right) \\ &= \left(\sum_{i\in I\setminus J} a_i v_i\right) + U \\ &= \sum_{i\in I\setminus J} (a_i v_i + U) \\ &= \sum_{i\in I\setminus J} a_i (v_i + U). \end{aligned}$$

Somit ist $\{v_i + U \mid i \in I \setminus J\}$ ein Erzeugendensystem für $\mathbb{V}/U$.

Ist $\sum\limits_{i\in I\setminus J} b_i(v_i+U) = U,\ b_i \in \mathbb{K}$, dann ist auch $\left(\sum\limits_{i\in I\setminus J} b_i v_i\right) + U = U$, d.h. $\sum\limits_{i\in I\setminus J} b_i v_i \in U$.
Daraus folgt $\sum\limits_{i\in I\setminus J} b_i v_i = \sum\limits_{j\in J} c_j v_i$ mit geeigneten $c_j \in \mathbb{K}$. Dann ist aber $\sum\limits_{i\in I\setminus J} b_i v_i + \sum\limits_{j\in J}(-c_j)v_i = 0$. Da B linear unabhängig ist, so sind die $b_i = 0$ für alle $i \in I$. Dann ist $\{v_i + U \mid i \in I \setminus J\}$ linear unabhängig.

b) Sei $v \in \mathbb{V}$. Dann $v + U = \sum\limits_{j\in J} a_j(v_j+U) = \left(\sum\limits_{j\in J} a_j v_j\right) + U,\ a_j \in \mathbb{K}$. Somit $v - \sum\limits_{j\in J} a_j v_j \in U$. Da B Basis in U, so folgt $v - \sum\limits_{j\in J} a_j v_j = \sum\limits_{i\in I} a_i u_i \Leftrightarrow v = \sum\limits_{j\in J} a_j v_j + \sum\limits_{i\in I} a_i u_i$. Dann ist aber $\{u_i \mid i \in I\} \cup \{v_j \mid j \in J\}$ ein Erzeugendensystem für $\mathbb{V}$.
Ist $\sum\limits_{i\in I} c_i u_i + \sum\limits_{j\in J} d_j v_j = 0,\ c_i, d_j \in \mathbb{K}$, dann rechnet man

$$\begin{aligned} U &= \left(\sum_{i\in I} c_i u_i + \sum_{j\in J} d_j v_j\right) + U \\ &= \left(\left(\sum_{i\in I} c_i u_i\right) + U\right) + \left(\left(\sum_{j\in J} d_j v_j\right) + U\right) \\ &= U + \left(\left(\sum_{j\in J} d_j v_j\right) + U\right) \\ &= \left(\sum_{j\in J} d_j v_j\right) + U \\ &= \sum_{j\in J} ((d_j v_j) + U) \\ &= \sum_{j\in J} d_j (v_j + U). \end{aligned}$$

B' ist linear unabhängig, so folgt $c_i = 0\ \forall\ i \in I$, damit ist $\{u_i \mid i \in I\} \cup \{v_j \mid j \in J\}$ linear unabhängig.
c) Nach Satz 4.2.(ii) gibt es eine Basis $B = \{v_i \mid i \in I\}$, so daß $J \subseteq I$ und $B' = \{v_i \mid i \in J\}$ Basis von U ist. Mit a) folgt c). ■

5 Lineare Abbildungen

Def.5.1.
Seien $\mathbb{V}, \mathbb{W}$ zwei $\mathbb{K}$-Vektorräume.

1) $A : \mathbb{V} \to \mathbb{W}$ heißt $\mathbb{V}$-lineare Abbildung oder Homomorphismus, falls (a) $A(v_1+v_2) = Av_1+Av_2 \; \forall \, v_1, v_2 \in \mathbb{V}$ und (b) $A(\lambda v) = \lambda Av \; \forall \; v \in \mathbb{V}, \; \lambda \in \mathbb{K}$ gilt.
Die Menge dieser Abbildungen heißt $\mathrm{Hom}(\mathbb{V}, \mathbb{W})$.
2) $A \in \mathrm{Hom}(\mathbb{V}, \mathbb{W})$. A heißt Epimorphismus, Monomorphismus, Isomorphismus, falls A surjektiv, injektiv bzw. bijektiv ist. Wenn $\mathbb{V} = \mathbb{W}$, dann heißt A Endomorphismus. Ist A bijektiver Endomorphismus, dann heißt A Automorphismus.
3) Existiert ein Isomorphismus $A : \mathbb{V} \to \mathbb{W}$, so schreibt man $\mathbb{V} \cong \mathbb{W}$ und sagt, $\mathbb{V}$ ist isomorph zu $\mathbb{W}$.

Def.5.2.
Sei $A \in \mathrm{Hom}(\mathbb{V}, \mathbb{W})$, $\mathbb{V}, \mathbb{W}$ seien $\mathbb{K}$-Vektorräume. Dann bezeichnen wir mit $\mathrm{Im}(A) := \{Av \mid v \in \mathbb{V}\}$ das Bild von A und mit $\ker(A) := \{v \in \mathbb{V} \mid Av = 0\}$ den Kern von A.

Nach Homomorphiesatz:
Seien $\mathbb{V}, \mathbb{W}$ zwei $\mathbb{K}$-Vektorräume und $A \in \mathrm{Hom}(\mathbb{V}, \mathbb{W})$.
1) $\mathrm{Im}(A)$ ist ein Unterraum von $\mathbb{W}$ und $\ker(A)$ ein Unterraum von $\mathbb{V}$.
2) A ist Monomorphismus g.d.w. $\ker(A) = \{0\}$.
3) Es gibt einen Epimorphismus $B : \mathbb{V} \to \mathbb{V}/\ker(A)$ und einen Monomorphismus $C : \mathbb{V}/\ker(A) \to \mathbb{W}$ (auf $\mathrm{Im}(A)$), so daß $C \circ B = A$ ist. Es gilt

$$\mathbb{V}/\ker(A) \cong \mathrm{Im}(A).$$

Satz 5.1. (Hauptsatz)
$\mathbb{V}$ sei $\mathbb{K}$-Vektorraum, $\dim \mathbb{V} = n \in \mathbb{N}$. Sei $\mathbb{K}^n := \{(\lambda_1, \ldots, \lambda_n)^t \mid \lambda_k \in \mathbb{K}\}$, dann ist $\mathbb{V} \cong \mathbb{K}^n$.
Beweis: Sei $B := \{v_1, \ldots, v_n\}$ Basis von $\mathbb{V}$. Sei $A : \mathbb{K}^n \to \mathbb{V}$ definiert durch $A \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = \sum_{i=1}^{n} \lambda_i v_i$. Damit ist $A \in \mathrm{Hom}(\mathbb{K}^n, \mathbb{V})$. Da B eine Basis , so ist A surjektiv. Ist $A \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} \in \ker(A)$, dann ist $\sum_{i=1}^{n} \lambda_i v_i = 0$. Da B linear unabhängig, so sind die $\lambda_i = 0$ für $i = 1, \ldots, n$, d.h. A ist ein Isomorphimus. ■

Folgerung
Zwei Vektorräume $\mathbb{V}$ und $\mathbb{W}$ sind genau dann isomorph, wenn sie die gleiche Dimension haben.

Satz 5.2.
Seien $\mathbb{V}, \mathbb{W}$ zwei $\mathbb{K}$-Vektorräume und $A \in \mathrm{Hom}(\mathbb{V}, \mathbb{W})$. Sei $r(A) := \dim \mathrm{Im}(A)$, falls diese Zahl endlich ist. $r(A)$ heißt der Rang von A. Es gilt:
(i) Ist $\dim \mathbb{V} < \infty$, dann $\dim \mathbb{V} = r(A) + \dim \ker(A)$.
(ii) $\dim \mathbb{V} < \infty \Rightarrow r(A) \leq \dim \mathbb{V}$.
(iii) $\dim \mathbb{W} < \infty \Rightarrow r(A) \leq \dim \mathbb{W}$.
Beweis:
(i) Nach Homomorphiesatz: $\mathbb{V}/\ker(A) \cong \mathrm{Im}(A)$.
Somit folgt $r(A) = \dim \mathrm{Im}(A) = \dim \mathbb{V}/\ker(A) = \dim \mathbb{V} - \dim \ker(A)$, nach Definition des Faktorraumes.
(ii) Dies folgt sofort aus (i).
(iii) $\mathrm{Im}(A) \subseteq \mathbb{W}$ ist Unterraum, somit folgt dies aus dem Basissatz (Satz 4.2.) . ■

Folgende Aussagen sind sehr nützlich:
1. Sind $\mathbb{V}, \mathbb{W}$ zwei $\mathbb{K}$-Vektorräume und $A : \mathbb{V} \to \mathbb{W}$ ein Isomorphismus, dann gibt es genau ein $B \in \mathrm{Hom}(\mathbb{W}, \mathbb{V})$ mit $(BA)v = v \; \forall \; v \in \mathbb{V}$ und $(AB)w = w \; \forall \; w \in \mathbb{W}$.
Beweis: A ist bijektiv.
Dann gibt es eine Abbildung $B : \mathbb{W} \to \mathbb{V}$ mit $B(Av) = v \; \forall \; v \in \mathbb{V}$ und $A(Bw) = w \; \forall \; w \in \mathbb{W}$.
Zu zeigen: $B \in \mathrm{Hom}(\mathbb{W}, \mathbb{V})$.
Wenn $v, w \in \mathbb{W}, \alpha, \beta \in \mathbb{K}$, so gilt

$$\begin{aligned} A(B(\alpha v + \beta w)) &= \alpha v + \beta w \\ &= \alpha A(Bv) + \beta A(Bw) \\ &= A(\alpha Bv) + A(\beta Bw) \\ &= A(\alpha Bv + \beta Bw). \end{aligned}$$

Da A bijektiv, so gilt: $B(\alpha v + \beta w) = \alpha Bv + \beta Bw$ und B linear. ■

Bemerkungen
a) Unter den Bedingungen von **1.** bezeichnet man die Abbildung B mit A^{-1}.

b) Sei $A \in \mathrm{Hom}(\mathbb{V},\mathbb{V})$. A heißt regulär oder invertierbar, wenn A Automorphismus auf $\mathbb{V}$ ist. Ist A nicht regulär, dann heißt A singulär.
c) Die Menge aller regulären Abbildungen von $\mathbb{V} \to \mathbb{V}$ heißt $GL(n,\mathbb{V})$, wobei n die Dimension von $\mathbb{V}$ bezeichnet, und heißt die lineare Gruppe.

2. Es gelte **1.** A ist regulär g.d.w. es gibt $B_1, B_2 \in \mathrm{Hom}(\mathbb{V},\mathbb{W})$ mit $AB_1 = B_2A = \mathbb{I}$ $(\mathbb{I}v = v)$.
Beweis: a) Sei A regulär, dann $B_1 = B_2 := A^{-1}$.
b) Seien $B_1, B_2 \in \mathrm{Hom}(\mathbb{V},\mathbb{W})$ mit $AB_1 = B_2A = \mathbb{I}$. Dann ist A bijektiv nach Lemma 2.1.-3). ■

3. Man zeige: $GL(n,\mathbb{V})$ ist eine Gruppe.

Satz 5.3. (Satz über die Basistransformation)
Seien $\mathbb{V},\mathbb{W}$ zwei $\mathbb{K}$-Vektorräume, $\{v_1,\ldots,v_n\}$ eine Basis von $\mathbb{V}$ und $\{w_1,\ldots,w_n\}$ eine Basis von $\mathbb{W}$. Dann gibt es genau ein $A \in \mathrm{Hom}(\mathbb{V},\mathbb{W})$ mit $Av_i = w_i,\ i = 1(1)n$.
Beweis: Seien $a_i \in \mathbb{K}$ und $A\left(\sum_{i=1}^{n} a_iv_i\right) := \sum_{i=1}^{n} a_iw_i$. Da $\{v_i\}$ Basis von $\mathbb{V}$, so gilt für alle $v \in \mathbb{V}$: v ist Linearkombination der v_i mit eindeutig bestimmten a_i. $\Rightarrow A$ ist eine Abbildung und $Av_i = w_i$.
Seien $x, y \in \mathbb{V},\ x = \sum_{i=1}^{n} a_iv_i,\ y = \sum_{i=1}^{n} b_iv_i$, seien $\alpha,\beta \in \mathbb{K}$. Dann rechnet man so:

$$\begin{aligned}
A(\alpha x + \beta y) &= A\left(\sum_{i=1}^{n} \alpha a_iv_i + \sum_{i=1}^{n} \beta b_iv_i\right) \\
&= A\left(\sum_{i=1}^{n} (\alpha a_i + \beta b_i)v_i\right) \\
&= \sum_{i=1}^{n} (\alpha a_i + \beta b_i)w_i \\
&= \alpha \sum_{i=1}^{n} a_iw_i + \beta \sum_{i=1}^{n} b_iw_i \\
&= \alpha\left(A\left(\sum_{i=1}^{n} a_iv_i\right)\right) + \beta\left(A\left(\sum_{i=1}^{n} b_iv_i\right)\right) = \alpha Ax + \beta Ay
\end{aligned}$$

Damit ist $A \in \mathrm{Hom}(\mathbb{V},\mathbb{W})$.
Eindeutigkeit: Sei $\tilde{A} \in \mathrm{Hom}(\mathbb{V},\mathbb{W})$ mit $\tilde{A}v_i = w_i,\ i = 1(1)n$. Dann gilt:

$$\tilde{A}\left(\sum_{i=1}^{n} a_iv_i\right) = \sum_{i=1}^{n} a_i(\tilde{A}v_i) = \sum_{i=1}^{n} a_iw_i = \sum_{i=1}^{n} a_i(Av_i) = A\left(\sum_{i=1}^{n} a_iv_i\right)$$

$\Rightarrow A$ ist eindeutig. ■

Def.5.3.
Seien $\mathbb{V}_1,\mathbb{V}_2$ zwei $\mathbb{K}$-Vektorräume, $A, B \in \mathrm{Hom}(\mathbb{V}_1,\mathbb{V}_2)$. Wir definieren die Summe $A + B \in \mathrm{Hom}(\mathbb{V}_1,\mathbb{V}_2)$ durch $(A+B)v := Av + Bv,\ v \in \mathbb{V}_1$ und für $\lambda \in \mathbb{K}$, $\lambda A \in \mathrm{Hom}(\mathbb{V}_1,\mathbb{V}_2)$ durch $(\lambda A)v := \lambda(Av)$.

Satz 5.4.
Seien $\mathbb{V}_1,\mathbb{V}_2$ zwei $\mathbb{K}$-Vektorräume. Gemäß Def.5.3. wird die Menge der Abbildungen $\mathrm{Hom}(\mathbb{V}_1,\mathbb{V}_2)$ zu einem $\mathbb{K}$-Vektorraum.
Beweis: Man muß die Axiome aus Def.4.1. nachprüfen.
a) Seien $v, w \in \mathbb{V}_1,\ \alpha,\beta \in \mathbb{K}$. Dann ist

$$\begin{aligned}
(A+B)(\alpha v + \beta w) &= A(\alpha v + \beta w) + B(\alpha v + \beta w) \\
&= \alpha Av + \beta Aw + \alpha Bv + \beta Bw \\
&= \alpha(Av + Bv) + \beta(Aw + Bw) \\
&= \alpha(A+B)v + \beta(A+B)w.
\end{aligned}$$

b) Man zeigt $(\mathrm{Hom}(\mathbb{V}_1,\mathbb{V}_2),+)$ ist eine Gruppe.

c) $\lambda A \in \mathrm{Hom}(\mathbb{V}_1,\mathbb{V}_2), \lambda \in \mathbb{K}$. Wie in a) ist dann $\lambda A(\alpha v + \beta w) = \alpha(\lambda A)v + \beta(\lambda A)w$.

d) zu zeigen: Mit a)-c) ist $\mathrm{Hom}(\mathbb{V}_1,\mathbb{V}_2)$ ein $\mathbb{K}$-Vektorraum.
Seien $\lambda_1,\lambda_2 \in \mathbb{K},\ v \in \mathbb{V}_1$, dann $((\lambda_1\lambda_2)A)v = (\lambda_1\lambda_2)(Av) = \lambda_1((\lambda_2A)v)$.
Da v willkürlich war, so folgt $(\lambda_1\lambda_2)A = \lambda_1(\lambda_2A)$.

$((\lambda_1+\lambda_2)A)v = (\lambda_1+\lambda_2)(Av) = (\lambda_1 A + \lambda_2 A)v$. Wiederum v beliebig, also $(\lambda_1+\lambda_2)A = \lambda_1 A + \lambda_2 A$.
e) Für $v \in \mathbb{V}_1$ gilt: $(\mathbb{I}\cdot A)v = Av$, also $\mathbb{I}\cdot A = A$ und somit bilden die Abbildungen $\mathrm{Hom}(\mathbb{V}_1, \mathbb{V}_2)$ einen $\mathbb{K}$-Vektorraum. ■

Folgerung
1) Seien $\mathbb{V}_k,\ k = 1,2,3$ $\mathbb{K}$-Vektorräume, $A \in \mathrm{Hom}(\mathbb{V}_1, \mathbb{V}_2)$, $B \in \mathrm{Hom}(\mathbb{V}_2, \mathbb{V}_3)$, dann $(BA)v = B(Av)\ \forall\, v \in \mathbb{V}_1$ und $BA \in \mathrm{Hom}((\mathbb{V}_1, \mathbb{V}_3)$.
2) $\mathrm{Hom}(\mathbb{V}_1, \mathbb{V}_2)$ ist mit der Operatormultiplikation und Satz 5.4. ein Ring.

Wir geben einen Satz ohne Beweis an (siehe STROTH S.142).
Satz 5.5.
Seien $\mathbb{V}, \mathbb{W}$ zwei $\mathbb{K}$-Vektorräume und $\{v_1, \ldots, v_n\}$ eine Basis von $\mathbb{V}$, $\{w_1, \ldots, w_n\}$ eine Basis von $\mathbb{W}$. Wir setzen $L_{ij} \in \mathrm{Hom}(\mathbb{V}, \mathbb{W})$ gemäß $L_{ij}v_k := \begin{cases} 0, & k \neq i \\ w_j, & k = i \end{cases}$. Dann ist $\{L_{ij} \mid i = 1(1)n, j = 1(1)n\}$ eine Basis von $\mathrm{Hom}(\mathbb{V}, \mathbb{W})$. Insbesondere gilt $\dim \mathrm{Hom}(\mathbb{V}, \mathbb{W}) = \dim \mathbb{V} \cdot \dim \mathbb{W}$. ■

Mit diesen Aussagen können wir nun komfortabel das Matrizenproblem behandeln.

6 Matrizen und Determinanten

6.1 Definitionen, Eigenschaften

Seien $\mathbb{V}, \mathbb{W}$ zwei $\mathbb{K}$-Vektorräume, $A \in \mathrm{Hom}(\mathbb{V}, \mathbb{W})$. Nach Satz 5.5. kann man A darstellen als

$$A = \sum_{j=1}^{n}\sum_{k=1}^{m} c_{kj} L_{kj} \quad , \quad c_{kj} \in \mathbb{K}.$$

Man bezeichnet die Größen $(c_{11}, \ldots, c_{1n}, c_{21}, \ldots, c_{mn})$ als die Koordinaten von A.
Diese können wir in einem Rechteckschema anordnen $\begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & & & \vdots \\ c_{m1} & c_{m2} & \cdots & c_{mn} \end{pmatrix} = A.$

Bemerkung
Seien $\mathbb{V}, \mathbb{W}$ zwei $\mathbb{K}$-Vektorräume und $B_1 := \{v_1, \ldots, v_n\}$ eine Basis von $\mathbb{V}$, $B_2 := \{w_1, \ldots, w_m\}$ eine Basis von $\mathbb{W}$ und sei $A \in \mathrm{Hom}(\mathbb{V}, \mathbb{W})$. Dann ist $Av_i = \sum_{j=1}^{m} a_{ji} w_j,\ \ i = 1(1)n,\ a_{ji} \in \mathbb{K}$.
Die (a_{ji}) sind eindeutig bestimmt.

Def.6.1.

$$(a_{jk})_{j,k} := \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$$

(a_{jk}) heißt Matrix von A bzgl. B_1 und B_2, wir schreiben ${}_{B_1}A_{B_2}$.
(m, n) heißt der Typ der Matrix, wir schreiben auch $A \in M(m \times n)$. Wenn $m = n$, dann heißt A quadratisch.

Folgerung
Jeder linearen Abbildung ist eine Matrix zugeordnet. Diese Matrix hängt von den Koordinaten (a_{jk}) ab und von der Anordnung der Basiselemente in B_1 und B_2.

Beispiel Man beachte die Definition der Basistransformation.
$\mathbb{V} = \mathbb{R}^4,\ \mathbb{W} = \mathbb{R}^3,\ B_1 = (v_1, v_2, v_3, v_4),\ B_2 = (w_1, w_2, w_3)$.
Sei $A \in \mathrm{Hom}(\mathbb{V}, \mathbb{W})$ mit $\begin{array}{rcrrr} Av_1 &=& 2w_1 & -w_2 & +w_3 \\ Av_2 &=& -w_1 & +w_2 & -w_3 \\ Av_3 &=& w_1 & +2w_2 & +3w_3 \\ Av_4 &=& & w_2 & +w_3 \end{array} \Rightarrow A = \begin{pmatrix} 2 & -1 & 1 & 0 \\ -1 & 1 & 2 & 1 \\ 1 & -1 & 3 & 1 \end{pmatrix}$ bzgl. B_1 und B_2.
Wir motivieren unsere Transformationformel:
Sei $v \in \mathbb{V}$ und $v = \sum_{i=1}^{n} x_i v_i$. Wir rechnen:

$$Av = A(\sum_{i=1}^{n} x_i v_i) = \sum_{i=1}^{n} x_i (Av_i) = \sum_{i=1}^{n} x_i \left(\sum_{j=1}^{m} a_{ji} w_j\right) = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} a_{ji} x_i\right) w_j$$

und damit Av: $v_j = \sum_{j=1}^{m} a_{ji}x_i$ Transformation der Vektorkomponenten.

Nun untersuchen wir die Summe und das Produkt von Matrizen.

Satz 6.2.
1) $(\mathbb{V}, B_1),\ (\mathbb{W}, B_2)$ seien zwei $\mathbb{K}$-Vektorräume mit zug. Basen.
$A,\ B \in \mathrm{Hom}(\mathbb{V}, \mathbb{W}),\ A = (a_{ji}),\ B = (b_{ji})$ bzgl. B_1, B_2.
Dann ist $A + B$ die Matrix $(a_{ji} + b_{ji})_{j,i}$.
2) Seien $\mathbb{V}_k,\ k = 1, 2, 3$ $\mathbb{K}$-Vektorräume mit Basen B_k.
Sei $A \in \mathrm{Hom}(\mathbb{V}_1, \mathbb{V}_2),\ B \in \mathrm{Hom}(\mathbb{V}_2, \mathbb{V}_3),\ (a_{ji}) =_{B_1} A_{B_2},\ (b_{ji}) =_{B_2} B_{B_3}$.
Dann gehört zum Produkt BA bzgl. B_1 und B_3 die Matrix $\left(\sum_{k=1}^{\dim \mathbb{V}_2} b_{jk}a_{ki}\right)_{j,i}$.

Beweis: 1) $B_1 = \{v_k\}_1^n,\ B_2 = \{w_k\}_1^m$.
Dann folgt aufgrund der Linearität $(A + B)v_i = Av_i + Bv_i = \sum_{j=1}^{m} a_{ji}w_j + \sum_{j=1}^{m} b_{ji}w_j = \sum_{j=1}^{m}(a_{ji} + b_{ji})w_j \Rightarrow 1)$.
Sei $B_3 = \{t_k\}_1^r$. Dann ist

$$\begin{aligned}
(BA)v_i = B(Av_i) &= B\left(\sum_{k=1}^{m} a_{ki}w_k\right) \\
&= \sum_{k=1}^{m} a_{ki}(Bw_k) \\
&= \sum_{k=1}^{m} a_{ki}\left(\sum_{j=1}^{r} b_{jk}t_j\right) \\
&= \sum_{j=1}^{r}\left(\sum_{k=1}^{m} a_{ki}b_{jk}\right)t_j \\
&= \sum_{j=1}^{r}\left(\sum_{k=1}^{m} b_{jk}a_{ki}\right)t_j
\end{aligned}$$

■

Def.6.2.
1) $(a_{kj}),\ (b_{kj})$ seien Matrizen von gleichen Typ. Wir definieren $(a_{kj}) + (b_{kj}) = (a_{kj} + b_{kj})$.
2) Sei $\lambda \in \mathbb{K}$, (a_{kj}) eine Matrix, dann $\lambda(a_{kj}) = (\lambda a_{kj})$.
3) Ist (a_{kj}) vom Typ (m, n) und (b_{kj}) vom Typ (n, l), dann heißt die Matrix $(c_{kj}) = \left(\sum_{i=1}^{n} a_{ki}b_{ij}\right)$ vom Typ (m, l) das Produkt.

Folgerung
1. Die Matrizen vom Typ (m, n) bilden einen $\mathbb{K}$-Vektorraum bzgl. der Operationen aus Def.6.2.
2. Die quadratischen Matrizen vom Typ (m, m) bilden einen Ring bzgl. der Operationen aus Def.6.2.
Mit abstrakten Matrizen kann man Abbildungen auf einem $\mathbb{K}$-Vektorraum beschreiben. Sei $(x_1, \ldots, x_n) \in \mathbb{V}$.
Dann sei $A = (a_{kj})$ und $y = Ax \Leftrightarrow y_k = \sum_{j=1}^{n} a_{kj}x_j,\ k = 1(1)n$.

Beispiel Sei $v = (1, 2, 1, 0)^{tr}$ und A wie oben, dann

$$Av = \begin{pmatrix} 2 & -1 & 1 & 0 \\ -1 & 1 & 2 & 1 \\ 1 & -1 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 2 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 3 \\ 2 \end{pmatrix} \Rightarrow Av = w_1 + 3w_2 + 2w_3.$$

Def.6.3.
Sei $(a_{kj}) \in M(m \times m)$. (a_{kj}) heißt regulär, falls ein $(b_{kj}) \in M(m \times m)$ existiert, so daß

$$(b_{ki})(a_{ij}) = \mathbb{I}_n = E_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix}.$$

$\mathbb{I}_n$ heißt n-dimensionale Einheitsmatrix.

Nun können wir einen Schluß ziehen: Die regulären Matrizen bilden eine Gruppe. Aus Satz 3.1. folgt: In einer Gruppe mit neutralem Element e folgt aus $a \circ b = e$, daß b eindeutig bestimmt ist. Also ist die in Def.6.3. eingeführte Matrix eindeutig.

Beispiel

$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$. $B \circ A = \mathbb{I}_2$, das heißt

$$\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} b_{11}a_{11} + b_{12}a_{21} & b_{11}a_{12} + b_{12}a_{22} \\ b_{21}a_{11} + b_{22}a_{21} & b_{21}a_{12} + b_{22}a_{22} \end{pmatrix}.$$

Hieraus erhält man $b_{11}a_{11} + b_{12}a_{21} = 1, \quad b_{11}a_{12} + b_{12}a_{22} = 0, \quad b_{21}a_{11} + b_{22}a_{21} = 0, \quad b_{21}a_{12} + b_{22}a_{22} = 1$

$$\Rightarrow b_{11} = -\frac{a_{22}}{a_{12}} b_{12}, \quad b_{22} = -\frac{a_{11}}{a_{21}} b_{21}, \quad (a_{12}, a_{21} \neq 0)$$

$$\Rightarrow b_{12}a_{21} - a_{11}\frac{a_{22}}{a_{12}} b_{12} = 1, \quad b_{21}a_{12} - a_{22}\frac{a_{11}}{a_{21}} b_{21} = 1$$

$$\Rightarrow b_{12}(a_{21}a_{12} - a_{11}a_{22}) = a_{12}, \quad b_{21}(a_{21}a_{12} - a_{11}a_{22}) = a_{21}.$$

Sei $D := a_{21}a_{12} - a_{11}a_{22} \neq 0$. Dann folgt

$$b_{12} = \frac{a_{12}}{D}, \quad b_{21} = \frac{a_{21}}{D}, \quad b_{22} = -\frac{a_{11}}{D}, \quad b_{11} = -\frac{a_{22}}{D}.$$

D heißt die Determinante von A und $D \neq 0$ ist hier eine Bedingung, daß die Inverse von A existiert. Wir kommen hierauf noch zurück.

Satz 6.3.

Sei $\mathbb{V}$ ein $\mathbb{K}$-Vektorraum und $\mathcal{B} := \{v_1, \ldots, v_n\}$ eine Basis von $\mathbb{V}$. Sei $(a_{jk}) \in M(n \times n)$. Wir definieren $w_k := \sum_{j=1}^{n} a_{jk} v_j$. Die w_k bilden genau dann eine Basis, wenn (a_{jk}) regulär ist.

Beweis: $A \in \mathrm{Hom}(\mathbb{V}, \mathbb{V})$ und $Av_k = w_k$. Ist $\{w_k\}_1^n$ eine Basis, dann A Isomorphismus und A regulär. Ist (a_{kj}) regulär, dann ist A ein Isomorphismus. Dann gibt aber die Zuordnung $w_k = Av_k$ eine Basis in $\mathbb{V}$, weil: Es gibt $B \in \mathrm{Hom}(\mathbb{V}, \mathbb{V})$ mit $B \cdot A = \mathbb{I}_n$. Ist $Bv_j = \sum_{k=1}^{n} b_{kj} v_k$, d.h. $(b_{kj}) =_{\mathcal{B}} B_{\mathcal{B}}$, dann ist $(b_{kj})(a_{ji}) = \mathbb{I}_n$. ■

Satz 6.4.

Seien $\mathbb{V}, \mathbb{W}$ zwei $\mathbb{K}$-Vektorräume und $B_1 := \{v_1, \ldots, v_n\}$ eine Basis von $\mathbb{V}$, $B_2 := \{w_1, \ldots, w_m\}$ eine Basis von $\mathbb{W}$ und sei $A \in \mathrm{Hom}(\mathbb{V}, \mathbb{W})$ mit $Av_k = \sum_{j=1}^{m} a_{jk} w_j, \ k = 1(1)n$ gegeben.

Sei $s_k = \begin{pmatrix} a_{1k} \\ \vdots \\ a_{mk} \end{pmatrix} \subset \mathbb{K}^m, \quad k = 1(1)n$. Dann ist $r(A) = \dim(s_1, \ldots, s_n)$.

($r(A)$ heißt Rang von A.)

Beweis: $w \in \mathbb{W}$, dann $w = \sum_{k=1}^{m} \lambda_k w_k, \ \lambda_k \in \mathbb{K}$.

Wir definieren $B : \mathbb{W} \to \mathbb{K}^m$ mittels $B\left(\sum_{k=1}^{m} \lambda_k w_k\right) = (\lambda_1, \ldots, \lambda_m)^{tr} \Rightarrow B$ Isomorphismus.

$r(A) = \dim \mathrm{Im}A = \dim B(\mathrm{Im}A) = \dim \mathrm{Im}(BA) = r(BA)$.

Da aber $(BA)v_k = B\left(\sum_{j=1}^{m} a_{jk} w_j\right) = (a_{1k}, \ldots, a_{mk})^{tr} = s_k$, somit ist $\mathrm{Im}(BA) = \langle s_1, \ldots, s_n \rangle$ Erzeugnis. ■

Def.6.4.

Sei (a_{kj}) Matrix vom Typ (m, n). Der Rang von (a_{kj}) wird durch $r((a_{kj})) := \dim\langle \begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix}, \ j = 1(1)n \rangle$ definiert. Man nennt dies auch Spaltenrang.

Folgerung

Seien $\mathbb{V}, \mathbb{W}$ zwei $\mathbb{K}$-Vektorräume und B_1 eine Basis von $\mathbb{V}$, B_2 eine Basis von $\mathbb{W}$ und sei $A \in \mathrm{Hom}(\mathbb{V}, \mathbb{W})$ mit $(a_{kj}) =_{B_1} A_{B_2}$. Dann:

1) $r(A) = r((a_{kj}))$.

2) Ist (a_{kj}) vom Typ (m,n) und sind (x_{il}), (y_{ls}) reguläre Matrizen vom Typ (m,m) bzw. (n,n), dann gilt

$$r((a_{kj})) = r((x_{kl})(a_{ls})(y_{sj})).$$

Beweis: 1) folgt aus Satz 6.4., 2) folgt aus Satz 6.3. ■

Def.6.5.
Sei (a_{kj}) vom Typ (m,n). $(a_{kj})^{tr}$ heißt transponierte Matrix und ist definiert durch $(a_{kj})^{tr} = (b_{kj})$, wobei $b_{kj} = a_{jk}\ \forall k = 1,\dots,m,\ j = 1,\dots,n$ (Spiegeln an der Diagonalen).

Beispiel: Zu $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ ist $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ die transponierte Matrix.

Durch einfaches Nachrechnen bestätigt man folgende Eigenschaften:
Seien (a_{kj}) und (b_{kj}) vom gleichen Typ.
1) $((a_{kj}) + (b_{kj}))^{tr} = (a_{kj})^{tr} + (b_{kj})^{tr}$;
2) $\lambda(a_{kj})^{tr} = (\lambda a_{kj})^{tr}$;
3) $((a_{kj})^{tr})^{tr} = (a_{kj})$;
4) Sei (a_{kj}) von Typ (n,m) und (b_{kj}) vom Typ (m,l), dann $((a_{kj})(b_{kj}))^{tr} = (a_{kj})^{tr} \cdot (b_{kj})^{tr}$.
Hieraus folgt dann aber: Ist $z_k = (a_{k1},\dots,a_{kn})$, $k = 1(1)m$, dann gilt $r((a_{kj})) = \dim\langle z_1,\dots,z_m\rangle$ und weiterhin $r((a_{kj})) = r((a_{kj})^{tr})$, d.h. Zeilenrang=Spaltenrang. (siehe STROTH S.160)

6.2 Lineare Gleichungssysteme

$$\text{(LG)} \qquad \sum_{k=1}^{n} a_{ik}x_k = y_i,\ i = 1(1)m \Leftrightarrow \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix}$$

Dies beschreibt eine lineare Abbildung $\mathbb{K}^n \xrightarrow{A} \mathbb{K}^m$. Dann bedeutet (LG): Ist $y \in \mathbb{K}^m$, so ist das Urbild von y die Menge aller $x \in \mathbb{K}^n$ mit $Ax = y$. Jedes derartige x heißt dann Lösung. Die Urbildmenge von y ist Lösungsmenge.
Fragen: Ist das Urbild von y leer oder nicht (Existenz)? Besteht das Urbild von y aus genau einem Vektor (Einzigkeit) ?
(LG) heißt homogen, falls $y_k = 0$ für $k = 1(1)m$, ansonsten inhomogen. Dann können wir sagen: Ist $y = 0$, dann ist $A^{-1}y \subseteq \ker(A)$.
Ist $y \neq 0$, dann kann das Urbild leer sein, oder es enthält einen Vektor $\bar{x}$.
Dann ist $A^{-1}y = \bar{x} + \ker(A)$. $\bar{x}$ heißt partikuläre Lösung von (LG).
(i) Ist $A^{-1}y \neq \emptyset$ für gegebenes $y \in \mathbb{K}^m$?
(ii) Ist $A^{-1}y \neq \emptyset$ für alle $y \in \mathbb{K}^m$?

Satz 6.5. (Existenz)
Sei $A \in \mathrm{Hom}(\mathbb{K}^n, \mathbb{K}^m)$, A vom Typ (m,n) bzgl. der Standardbasis mit den Spaltenvektoren $s_1,\dots,s_n$.
Sei $y \in \mathbb{K}^m$ und sei (A,y) sie sog. erweiterte Matrix von A.

(i) Dann sind die folgenden Aussagen äquivalent:
(a) $A^{-1}y \neq \emptyset$
(b) $y \in \mathrm{Im}(A)$
(c) $y \in \langle s_1,\dots,s_n\rangle$
(d) $r(A) = r((A,y))$,

(ii) Folgende Aussagen sind ebenfalls äquivalent:
(a) $A^{-1}y \neq \emptyset\ \forall\ y \in \mathbb{K}^m$
(b) A ist surjektiv
(c) $r(A) = m$.

Beweis: (i) (a)⇒(b) Das ist die Definition des Urbildes.
(b)⇒(c) Wenn $e_1,\dots,e_n$ Standardbasis in $\mathbb{K}^m$. Dann gilt $\mathrm{Im}(A) = \langle Ae_i \mid i = 1(1)n\rangle = \langle s_1,\dots,s_n\rangle$.
(c)⇒(d) Wegen $y \in \langle s_1,\dots,s_n\rangle$ folgt $\dim\langle s_1,\dots,s_n,y\rangle = \dim\langle s_1,\dots,s_n\rangle$. Dann ist aber $r(A) = r((A,y))$.
(d)⇒(a) Da y linear abhängig von $\{s_k\}_1^n$, so ist $A^{-1}y \neq \emptyset$.

(ii) (a)⇔(b) Definition der Surjektivität.
(b)⇔(c) $r(A) = \dim \mathrm{Im}(A) = m$ g.d.w. A surjektiv. ■

Satz 6.6. (Eindeutigkeit)
Vorauss. wie in Satz 6.5. . Sei $y \in \mathbb{K}^m$ und $A^{-1}y \neq \emptyset$.
Dann sind folgende Aussagen äquivalent:
(a) $Ax = y$ hat genau eine Lösung

(b) $Ax = 0$ hat nur die trivale Lösung $x = 0$
(c) $r(A) = n$.
Beweis: Sei $\bar{x}$ Lösung von $Ax = y$.
(a)⇒(b) Alle Lösungen von $Ax = y$ liegen in $\bar{x} + \ker(A)$. Dann $\ker(A) = \{0\}$.
(b)⇒(c) $\ker(A) = \{0\}$, d.h. A injektiv, somit $\mathrm{Im}(A) \cong \mathbb{K}^n$, d.h. $r(A) = n$.
(c)⇒(a) $r(A) = n$, so folgt $\dim \mathrm{Im}(A) = n$, somit $\mathrm{Im}(A) \cong \mathbb{K}^n$, $\mathrm{Im}(A) \cong \mathbb{K}^n / \ker(A) \cong \mathbb{K}^n$,
also $\ker(A) = \{0\}$, somit A injektiv. dann hat y genau ein Urbild. ■

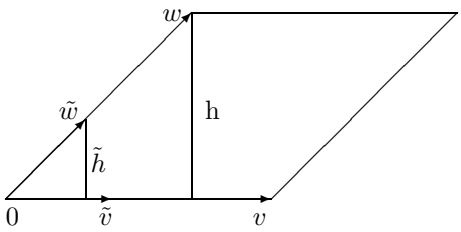
Folgerung
Gilt $m = n$ und ist eine Voraussetzung des Satzes 6.6. erfüllt, dann ist A eine Bijektion und invertierbar.

Satz 6.7.
Vorauss. wie in Satz 6.5. . $r(A) = k$.
Dann bilden die Lösungen von $Ax = 0$ einen (n-k)-dimensionalen Unterraum von $\mathbb{K}^n$.
Beweis: $A^{-1}(\{0\}) = \ker(A)$; $A : \mathbb{K}^n \to \mathbb{K}^m$ linear und $\mathrm{Im}(A) \cong \mathbb{K}^n / \ker(A)$, also folgt $k = r(A) = \dim \mathrm{Im}(A) = \dim(\mathbb{K}^n / \ker(A)) = \dim \mathbb{K}^n - \dim \ker(A) = n - \dim \ker(A) \Rightarrow \dim \ker(A) = n - k$. ■

6.3 Volumen und Determinante

Vorbemerkungen:
$$\begin{array}{ll} (1) & a_{11}x_1 + a_{12}x_2 = b_1 \quad | + a_{22} \cdot (1) - a_{12} \cdot (2) \\ (2) & a_{21}x_1 + a_{22}x_2 = b_2 \quad | + a_{11} \cdot (2) - a_{21} \cdot (1) \end{array}$$
$$\Rightarrow \begin{array}{l} (a_{11}a_{22} - a_{21}a_{12})x_1 = a_{22}b_1 - a_{12}b_2 \\ (a_{11}a_{22} - a_{21}a_{12})x_2 = a_{11}b_2 - a_{21}b_1 \end{array}.$$
Sei $D = a_{11}a_{22} - a_{21}a_{12} = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} \neq 0$.
Sei $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, dann sei mit $\begin{vmatrix} a & b \\ c & d \end{vmatrix} := ad - bc$ die zugehörige Determinante definiert.
Wir erhalten $x_1 = \dfrac{\begin{vmatrix} b_1 & a_{12} \\ b_2 & a_{22} \end{vmatrix}}{\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}}$, $x_2 = \dfrac{\begin{vmatrix} a_{11} & b_1 \\ a_{21} & b_2 \end{vmatrix}}{\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}}$. und
$\det A := \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}$ (CRAMERsche Regel für n=2) [13].
Ist $\det A = 0$ dann keine Lösung $\Leftrightarrow r(A) < 2$.

Beispiel



$v = (a_1, a_2)$, $w = (b_1, b_2)$.
Es existieren $\rho, \sigma \in \mathbb{R}$, $\rho, \sigma > 0$, $\alpha, \beta \in [0, 2\pi]$, so daß $\tilde{v} = \rho v$, $\tilde{w} = \sigma w$, $\tilde{v} = \rho(\cos\alpha, \sin\alpha), \tilde{w} = \sigma(\cos\alpha, \sin\alpha)$.
$F, \tilde{F}$ Fläche von $\mathrm{span}(v, w)$ bzw. $\mathrm{span}(\tilde{v}, \tilde{w})$.
Angenommen $0 \leq \beta - \alpha \leq \pi$. (Man kann immer auf diese Situation kommen.)

$$\tilde{h} = \sin(\beta - \alpha) = \cos\alpha \sin\beta - \cos\beta \sin\alpha = \begin{vmatrix} \cos\alpha & \sin\alpha \\ \cos\beta & \sin\beta \end{vmatrix}.$$
$$F = \rho\sigma\tilde{F} = \rho\sigma\tilde{h} = \begin{vmatrix} \rho\cos\alpha & \rho\sin\alpha \\ \sigma\cos\beta & \sigma\sin\beta \end{vmatrix} = \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix}$$

[13] benannt nach Gabriel CRAMER (1704-1752) schweiz. Mathematiker

$\Rightarrow$ Fläche des Parallelogramms= Determinante von $(\vec{a}, \vec{b})$.
Aus der Rechnung folgt noch: $\det \binom{\lambda v}{w} = \lambda \cdot \det \binom{v}{w}$, $\det \binom{\mu v}{w} = \mu \cdot \det \binom{v}{w}$, $\lambda, \mu \in \mathbb{R}$
Dies kann man verallgemeinern.

Def.6.6.
Seien $\mathbb{V}$ ein $\mathbb{K}$-Vektorraum, $\dim \mathbb{V} = n < \infty$. Eine Abbildung $V : \mathbb{V} \times \cdots \times \mathbb{V} \to \mathbb{K}$ heißt Volumen, falls gilt:
1) Für alle $i = 1(1)n$ und alle $v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n$ ist die Abbildung $v \mapsto V(v_1, \ldots, v_{i-1}, v, v_{i+1}, \ldots, v_n)$ linear,
2) Sind die $\{v_k\}_1^n$ linear abhängig, dann $V(v_1, \ldots, v_n) = 0$,
3) Es existieren immer $v_1, \ldots, v_n \in \mathbb{V}$, so daß $V(v_1, \ldots, v_n) \neq 0$.
V heißt auch alternierende multilineare Abbildung.

Lemma 6.1.
V sei Volumen auf dem $\mathbb{K}$-Vektorraum $\mathbb{V}$.
(1) Wenn $\{v_k\}_1^n \subset \mathbb{V}$, $\lambda \in \mathbb{K}$, so gilt für $i \neq j$: $V(v_1, \ldots, v_{i-1}, v_i + \lambda v_j, v_{i+1}, \ldots, v_n) = V(v_1, \ldots, v_n)$.
(2) Sei $\pi \in S_n$, so ist $V(v_{\pi(1)}, \ldots, v_{\pi(n)}) = \mathrm{sgn}\pi V(v_1, \ldots, v_n)$.
(3) $\{v_k\}_1^n \subset \mathbb{V}$, $w_k = \sum_{j=1}^{n} a_{jk} v_k$, $n = 1(1)n$, $a_{jk} \in \mathbb{K}$, dann

$$V(w_1, \ldots, w_n) = \left(\sum_{\pi \in S_n} (\mathrm{sgn}\pi) a_{1\pi(1)} \cdots a_{n\pi(n)}) \right) V(v_1, \ldots, v_n).$$

Beweis: (1) $V(v_1, \ldots, v_i + \lambda v_j, \ldots, v_n) = V(v_1, \ldots, v_n) + \lambda V(v_1, \ldots, v_{i-1}, v_j, v_{i+1}, \ldots, v_n) = V(v_1, \ldots, v_n)$.
(2) Sei $\tau = (i, j)$, $i < j$ eine Transposition=Inversion. Dann:

$$\begin{aligned}
V(v_1, \ldots, v_n) &= V(v_1, \ldots, v_{i-1}, v_i + v_j, v_{i+1}, \ldots, v_n) \\
&= V(v_1, \ldots, v_{i-1}, v_i + v_j, v_{i+1}, \ldots, v_{j-1}, v_j - (v_i + v_j), v_{j+1}, \ldots, v_n) \\
&= V(v_1, \ldots, v_{i-1} v_i + v_j, v_{i+1}, \ldots, v_{j-1}, -v_i, v_{j+1}, \ldots, v_n) \\
&= V(v_1, \ldots, v_{i-1}, v_j, v_{i+1}, \ldots, v_{j-1}, -v_i, v_{j+1}, \ldots, v_n) \\
&= (-1) V(v_{\tau(1)}, \ldots, v_{\tau(i)}, \ldots, v_{\tau(j)}, \ldots, v_{\tau(n)}) \\
\Leftrightarrow V(v_{\tau(1)}, \ldots, v_{\tau(n)}) &= \mathrm{sgn}\tau V(v_1, \ldots, v_n).
\end{aligned}$$

Da $\pi = \tau_1 \cdots \tau_k$ Produkt, so folgt durch Induktion:

$$\begin{aligned}
V(v_{\pi(1)}, \ldots, v_{\pi(n)}) &= V(v_{\tau_1(\tau_2 \cdots \tau_k)(1)}, \ldots, v_{\tau_1(\tau_2 \cdots \tau_k)(n)}) \\
&= (-1) V(v_{(\tau_2 \cdots \tau_k)(1)}, \ldots, v_{(\tau_2 \cdots \tau_k)(n)}) \\
&= -\mathrm{sgn}(\tau_2 \cdots \tau_k) V(v_1, \ldots, v_n) \\
&= \mathrm{sgn}\pi \cdot V(v_1, \ldots, v_n)
\end{aligned}$$

(3)

$$\begin{aligned}
V(w_1, \ldots, w_n) &= V(\sum_{j=1}^{n} a_{j1} v_j, \ldots, \sum_{j=1}^{n} a_{jn} v_j) \\
&= \sum_{j_1=1}^{n} \sum_{j_2=1}^{n} \cdots \sum_{j_n=1}^{n} a_{j_1 1} \cdots a_{j_n n} \underbrace{V(v_{j_1}, \ldots, v_{j_n})}_{=0, \text{wenn zwei } j_k \text{ gleich}} \\
&= \sum_{\pi \in S_n} \mathrm{sgn}\pi a_{\pi(1)1} \cdots a_{\pi(n)n} V(v_1, \ldots, v_n) \\
&= \left(\sum_{\pi \in S_n} (\mathrm{sgn}\pi) a_{\pi(1)1} \cdots a_{\pi(n)n} \right) V(v_1, \ldots, v_n) \\
&= \left(\sum_{\pi \in S_n} (\mathrm{sgn}\pi^{-1}) a_{1\pi(1)^{-1}} \cdots a_{n\pi(n)^{-1}} \right) V(v_1, \ldots, v_n) \\
&= \left(\sum_{\pi \in S_n} (\mathrm{sgn}\pi) a_{1\pi(1)} \cdots a_{n\pi(n)} \right) V(v_1, \ldots, v_n).
\end{aligned}$$

Dies gilt deshalb, weil π^{-1} ebenso ganz S_n durchläuft wie π selbst. ■

Folgerung
Sei $\mathbb{V}$ ein $\mathbb{K}$-Vektorraum, $\{v_1, \ldots, v_n\}$ eine Basis von $\mathbb{V}$, $0 \neq c \in \mathbb{K}$, $V : \mathbb{V} \times \cdots \times \mathbb{V} \to \mathbb{K}$ ein Volumen auf $\mathbb{V}$.

Beh.: Wenn $w_k = \sum_{j=1}^{n} a_{kj} v_j,\ k = 1(1)n,\ a_{kj} \in \mathbb{K}$, dann ist $V(w_1, \ldots, w_n) = \sum_{\pi \in S_n} (\mathrm{sgn}\pi) a_{1\pi(1)} \cdots a_{n\pi(n)} \cdot c$.
Beweis: siehe STROTH S.181 ■

Satz 6.8.
Sei $\mathbb{V}$ ein $\mathbb{K}$-Vektorraum, $\dim \mathbb{V} = n < \infty$, V sei Volumen auf $\mathbb{V}$.
Beh.: $\{v_1, \ldots, v_n\}$ linear unabhängig g.d.w. $V(v_1, \ldots, v_n) \neq 0$.

Beweis: Sei $\{v_k\}$ linear abhängig, dann $V(v_1, \ldots, v_n) = 0$ nach Def.6.6.(2).

Ist $\{v_1, \ldots, v_n\}$ Basis und $\{w_k\} \subset \mathbb{V}$ so, daß $V(w_1, \ldots, w_n) \neq 0$, dann ist $w_k = \sum_{j=1}^{n} b_{kj} v_j,\ b_{kj} \in \mathbb{K}$.

Dann gilt:

$0 \neq V(w_1, \ldots, w_n) = \left(\sum_{\pi \in S_n} (\mathrm{sgn}\pi)(b_{1\pi(1)} \cdots b_{n\pi(n)}) \right) V(v_1, \ldots, v_n)$ nach Lemma 6.1.(3).

Damit ist aber $V(v_1, \ldots, v_n) \neq 0$. ■

Folgerung
Sei $\mathbb{V}$ ein $\mathbb{K}$-Vektorraum, $\dim \mathbb{V} = n < \infty$, V_1, V_2 seien Volumina auf $\mathbb{V}$. Dann gibt es $0 \neq c \in \mathbb{K}$, so daß $V_2(v_1, \ldots, v_n) = c \cdot V_1(v_1, \ldots, v_n),\ v_i \in \mathbb{V},\ i = 1(1)n$.

Beweis: $\{w_k\}_1^n$ sei Basis von $\mathbb{V}$, $V_1(v_1, \ldots, v_n) \neq 0$. Sei $v_k = \sum_{j=1}^{n} a_{kj} w_j$.

Nach Lemma 6.1. ist $V_k(v_1, \ldots, v_n) = \left(\sum_{\pi \in S_n} (\mathrm{sgn}\pi) a_{1\pi(1)} \cdots a_{n\pi(n)} \right) V_k(w_1, \ldots, w_n),\ k = 1, 2$.

Definiere $c := \frac{V_2(w_1, \ldots, w_n)}{V_1(w_1, \ldots, w_n)}$. ■

Def.6.7.
Sei $\{v_1, \ldots, v_n\}$ Basis eines $\mathbb{K}$-Vektorraumes $\mathbb{V}$ und $A \in \mathrm{Hom}(\mathbb{V}, \mathbb{V})$.

$$\det A := \frac{V(Av_1, \ldots, Av_n)}{V(v_1, \ldots, v_n)} \quad \text{heißt die } \underline{\text{Determinante von A}}.$$

Satz 6.9.(!)
Sei $\{v_1, \ldots, v_n\}$ Basis eines $\mathbb{K}$-Vektorraumes $\mathbb{V}$ und $A \in \mathrm{Hom}(\mathbb{V}, \mathbb{V})$.
Dann: (1) $\det A$ ist unabhängig von der Wahl der Basis.
(2) $\det A \neq 0 \Leftrightarrow$ A ist invertierbar (d.h. Automorphismus).
Beweis: Aufgrund der Folgerung zu Satz 6.8. ist $\det A$ unabhängig von $\{v_k\}_1^n$. Wenn A kein Isomorphismus ist, dann ist $\{Av_k\}$ linear abhängig. Dann aber ist $V(Av_1, \ldots, Av_n) = 0$ und damit $\det A = 0$ basisunabhängig.
Sei nun A ein Isomorphismus. Sei $\tilde{V} : \mathbb{V} \times \cdots \times \mathbb{V} \to \mathbb{K}$ mit $\tilde{V}(w_1, \ldots, w_n) := V(Aw_1, \ldots, Aw_n)\ \forall w_k \in \mathbb{V}$.
z.z. $\tilde{V}$ ist Volumen.
Wir wissen nach Def. des Volumens, V ist linear im i-ten Argument, also auch $\tilde{V}$.
Wenn $\{w_k\} \subset \mathbb{V},\ \{\tilde{w}_k\} \subset \mathbb{V},\ \lambda \in \mathbb{K}$, so gilt:

$$\begin{aligned} \tilde{V}(w_1, \ldots, w_i + \lambda\tilde{w}_i, \ldots, w_n) &= V(Aw_1, \ldots, A(w_i + \lambda\tilde{w}_i), \ldots, Aw_n) \\ &= V(Aw_1, \ldots, Aw_n) + \lambda V(Aw_1, \ldots, A\tilde{w}_i, \ldots, Aw_n) \\ &= \tilde{V}(w_1, \ldots, w_n) + \lambda\tilde{V}(w_1, \ldots, \tilde{w}_i, \ldots, w_n) \end{aligned}$$

Sind $\{w_k\}$ linear abhängig, so auch $\{Aw_k\}$ und somit ist $V(Aw_1, \ldots, Aw_n) = 0$.
$\tilde{V}(v_1, \ldots, v_n) \neq 0$. A Isomorphismus, so ist auch $\{Av_1, \ldots, Av_n\}$ Basis von $\mathbb{V}$. Nach Satz 6.8. gilt dann $\tilde{V}(v_1, \ldots, v_n) = V(Av_1, \ldots, Av_n) \neq 0$ und damit ist $\tilde{V}$ Volumen auf $\mathbb{V}$.
Nach der Folgerung zu Satz 6.8. gilt $\tilde{V} = c \cdot V,\ 0 \neq c \in \mathbb{K}$.
Damit ist unabhängig von der Wahl der Basis $\det A = c = \frac{\tilde{V}(v_1, \ldots, v_n)}{V(v_1, \ldots, v_n)}$. ■

Folgerung (Übung)
Unter den Voraussetzungen von Satz 6.9. gilt:
(a) $\det(A \circ B) = \det A \cdot \det B$,
(b) $\det \mathbb{I}_n = 1$. Ist A invertierbar, dann ist $\det(A^{-1}) = (\det A)^{-1}$.

Def.6.8.

Sei $A = (a_{ij}) \in M(n,n)$.

$$A_{ij} := (-1)^{i+j} \begin{vmatrix} a_{11} & \cdots & a_{1,j-1} & a_{1,j+1} & \cdots & a_{1n} \\ \vdots & & & & & \vdots \\ a_{i1} & \cdots & a_{i,j-1} & a_{i,j+1} & \cdots & a_{in} \\ a_{i+1,1} & \cdots & a_{i+1,j-1} & a_{i+1,j+1} & \cdots & a_{i+1,n} \\ \vdots & & & & & \vdots \\ a_{n1} & \cdots & a_{n,j-1} & a_{n,j+1} & \cdots & a_{nn} \end{vmatrix}$$

A_{ij} heißt Adjunkte zu $a_{i,j}$ oder Minor zu (i,j) gehörig.
$\tilde{A} := (A_{ij})^{tr}$ heißt Adjunktenmatrix von A.

Beispiel
$\det A = \begin{vmatrix} 1 & 2 & 3 \\ -1 & -3 & -2 \\ 5 & 6 & 7 \end{vmatrix}$. Sei $i = j = 2 \Rightarrow A_{ij} = (-1)^4 \begin{vmatrix} 1 & 3 \\ 5 & 7 \end{vmatrix}$.

Satz 6.10. (Rechenregeln)
Sei $A = (a_{ij}) \in M(n,n)$, dann gilt:
(1) $A \cdot \tilde{A} = (\det A) \cdot \mathbb{I}_n$.
(2) Wenn $\det A \neq 0$, so $\det \tilde{A} = (\det A)^{n-1}$.
(3) Wenn $\det A \neq 0$, so $A^{-1} = (\det A)^{-1} \cdot \tilde{A}$.
(4) Laplace**scher Entwicklungssatz**
Entwicklung nach i-ter Zeile

$$\det A = \sum_{k=1}^{n} a_{ik} A_{ik},$$

Entwicklung nach j-ter Spalte

$$\det A = \sum_{k=1}^{n} a_{kj} A_{kj}.$$

Beweis:
(1) Sei $(c_{ij}) = A \cdot \tilde{A}$, $c_{ij} = \sum_{k=1}^{n} a_{ik} A_{jk} = \begin{cases} 0 & \text{für } i \neq j \\ \det A & \text{für } i = j \end{cases} \rightarrow A \cdot \tilde{A} = (\det A) \cdot \mathbb{I}_n$.
(2) Es ist $\det A \cdot \det \tilde{A} = \det(A \cdot \tilde{A}) = \det((\det A) \cdot \mathbb{I}_n) = (\det A)^n$. Wenn also $\det A \neq 0$, so $\det \tilde{A} = (\det A)^{n-1}$.
(3) Aus (1) folgt $A \cdot \left(\frac{1}{\det A} \tilde{A} \right) = \mathbb{I}_n \Rightarrow A^{-1} = \frac{1}{\det A} \tilde{A}$.
(4) Aus (1) folgt: $\det A = \sum_{k=1}^{n} a_{ik} A_{ik}$ für $i = 1(1)n$.
Es ist aber $A \cdot \tilde{A} = \tilde{A} \cdot A =: (d_{ij})$ und damit erhält man $d_{ij} = \sum_{k=1}^{n} A_{ki} a_{kj} = \begin{cases} 0 & \text{für } i \neq j \\ \det A & \text{für } i = j \end{cases}$. ■

Beispiel
Sei $A = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 2 & 3 \\ 1 & 1 & 1 \end{pmatrix}$, dann bedeutet der Entwicklungssatz für die 1.Zeile:

$$\begin{vmatrix} 0 & 1 & 0 \\ 1 & 2 & 3 \\ 1 & 1 & 1 \end{vmatrix} = 0 \cdot \begin{vmatrix} 2 & 3 \\ 1 & 1 \end{vmatrix} - 1 \begin{vmatrix} 1 & 3 \\ 1 & 1 \end{vmatrix} + 0 \cdot \begin{vmatrix} 1 & 2 \\ 1 & 1 \end{vmatrix} = 2.$$

Satz 6.11. (Cramersche Regel)
Sei $A = (a_{ij}) \in M(n,n)$, $\det A \neq 0$.
Wir betrachten $Ax = b \Leftrightarrow \sum_{k=1}^{n} a_{ik} x_k = b_i$, $i = 1(1)n$.
Dann hat das lineare Gleichungssystem genau eine Lösung und diese ist

$$x_j = \frac{1}{\det A} \sum_{k=1}^{n} A_{kj} b_k, \quad j = 1(1)n.$$

Beweis: Mit Satz 6.9. und Satz 6.6. folgt, es existiert genau eine Lösung.

Nach Satz 6.10.(3) ist

$$A^{-1} = \frac{1}{\det A}\tilde{A}$$

$$\Rightarrow x = A^{-1}b = \frac{1}{\det A}\tilde{A}b$$

$$\Rightarrow x_j = \frac{1}{\det A}\sum_{k=1}^{n} A_{kj}b_k.$$

■

7 Eigenwerte

7.1 Einführung

Wir betrachten zuerst spezielle Homomorphismen und beweisen den Kästchensatz.

Satz 7.1

1) Seien $\mathbb{V}$ ein $\mathbb{K}$-Vektorraum, $\dim \mathbb{V} < \infty,\ A \in \mathrm{Hom}(\mathbb{V},\mathbb{V})$, U Unterraum in $\mathbb{V}$ und $AU \subseteq U$. Sei $A_1 := A|_U$ und A_2 die Abbildung A auf $\mathbb{V}/U$, d.h. $A_2(v+U) := Av + U$.
Dann: $\det A = \det A_1 \cdot \det A_2$.

2) Es gilt

$$\begin{vmatrix} a_{11} & \cdots & a_{1n} & & & \\ \vdots & & \vdots & & * & \\ a_{n1} & \cdots & a_{nn} & & & \\ 0 & \cdots & 0 & b_{11} & \cdots & b_{1m} \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & b_{m1} & \cdots & b_{mm} \end{vmatrix} = \det(a_{jk}) \cdot \det(b_{jk}).$$

Beweis: 1) Sei A kein Isomorphismus, dann A kein Monomorphismus und $v \in \ker(A),\ v \neq 0$ existiert. Dann $A_2(v+U) = Av + U = U$, also $v + U \in \ker(A_2)$. Wenn A_2 Isomorphismus, $v \in U$, d.h. $\ker(A_1) \neq 0$. Dann gilt: A_1 oder A_2 kein Isomorphismus und nach Satz 6.9. folgt $0 = \det A = \det A_1 \cdot \det A_2$.
Sei A ein Isomorphismus $\Rightarrow \ker(A) = \{0\}$. Dann A_1 Monomorphismus, sogar Isom.; A_2 Epimorphismus und somit auch Isomorphismus.
Sei $\{u_1, \ldots, u_m\}$ Basis von U, $\{u_1, \ldots, u_m, v_1, \ldots, v_n\}$ Basis von $\mathbb{V}$ und V sei ein Volumen. Dann gilt nach Def. 6.7.

$$\det A = \frac{V(Au_1, \ldots, Au_m, Av_1, \ldots, Av_n)}{V(u_1, \ldots, u_m, v_1, \ldots, v_n)}.$$

(1) z.zg. $\{u_1, \ldots, u_m, Av_1, \ldots, Av_n\}$ Basis von $\mathbb{V}$:
Sei $\sum_{k=1}^{m} c_k u_k + \sum_{k=1}^{n} d_k(Av_k) = 0,\ c_k, d_k \in \mathbb{K}$. Dann ist aber $\sum_{k=1}^{n} d_k(Av_k) + u = U \Leftrightarrow \sum_{k=1}^{n} d_k a(v_k + U) = U$.
Somit bilden die $\{v_k + U \mid k = 1(1)n\}$ Basis in $\mathbb{V}/U$.

Da A_2 isomorph, so auch $\{A_2(v_k + U)\}$ Basis in $\mathbb{V}/U$. Damit $d_1 = \cdots = d_n = 0 \Rightarrow \sum_{k=1}^{m} c_k u_k = 0$. Da $\{u_1, \ldots, u_m\}$ Basis in $U \Rightarrow c_1 = \cdots = c_m = 0$, d.h. $\{u_1, \ldots, Av_n\}$ in 1) linear unabhängig, $n + m = \dim \mathbb{V}$ und $\{u_1, \ldots, Av_n\}$ Basis.

(2) z.zg. $\det A_1 = \frac{V(Au_1,\ldots,Au_m,Av_1,\ldots,Av_n)}{V(u_1,\ldots,u_m,Av_1,\ldots,Av_n)}$:
Wir definieren $\phi : \underbrace{U \times \cdots \times U}_{m} \to \mathbb{K}$ durch $\phi(w_1, \ldots, w_m) := V(w_1, \ldots, w_m, Av_1, \ldots, Av_n),\ w_1, \ldots, w_m \in U$.

Beh.: ϕ ist ein Volumen auf U. Aufgrund der Def. ist V im k-ten Argument linear, somit auch ϕ. Ist $\{w_k\}$ linear abhängig, dann auch $\{w_1, \ldots, w_m, Av_1, \ldots, Av_n\}$ und $\phi(w_1, \ldots, w_m) = 0$. Nach 1) ist aber $\phi(u_1, \ldots, u_m) \neq 0 \Rightarrow \phi$ ist Volumen auf U. Nach Satz 6.8. $\det A = \frac{\phi(Au_1,\ldots,Au_m)}{\phi(u_1,\ldots,u_m)}$

(3) z.zg. $\det A_2 = \frac{V(u_1,\ldots,u_m,Av_1,\ldots,Av_n)}{V(u_1,\ldots,u_m,v_1,\ldots,v_n)}$:
Wir definieren $\psi : \underbrace{U \times \cdots \times U}_{n} \to \mathbb{K}$ durch $\psi(w_1 + U, \ldots, w_m + U) := V(u_1, \ldots, u_m, w_1, \ldots, w_n)$.

z.zg. ψ ist Abbildung:

Sei $w_i + U = \tilde{w}_i + U \Leftrightarrow \tilde{w}_i - w_i \in U$(Äquivalenzklasse) $\Rightarrow \tilde{w}_i - w_i = \sum_{j=1}^{n} c_{ji}u_j,\ c_{ji} \in \mathbb{K}$. Wir rechnen

$$\begin{aligned}\psi(w_1+U,\dots,\tilde{w}_i+U,\dots,w_n+U) &= V(u_1,\dots,u_m,w_1,\dots,\tilde{w}_i,\dots,w_n)\\ &= V(u_1,\dots,u_m,w_1,\dots,w_i+\sum_{j=1}^{n}c_{ji}u_j,\dots,w_n)\\ &= V(u_1,\dots,u_m,w_1,\dots,w_m)\\ &= \psi(w_1+U,\dots,w_i+U,\dots,w_n+U)\end{aligned}$$

Also ist ψ eine Abbildung. Nach Definition ist ψ auch Volumen. Nach 6.7. folgt dann

$$\det A_2 = \frac{A_2(v_1+U),\dots,A_2(v_n+U))}{\psi(v_1+U,\dots,v_n+U)} = \frac{V(u_1,\dots,u_m,Av_1,\dots,Av_n)}{V(u_1,\dots,u_m,v_1,\dots,v_n)}.$$

Dann kann man bilden $\det A_1 \cdot \det A_2 = \det A$.
2) folgt aus einer Übungsaufgabe $\det(AB) = \det A \cdot \det B$. ■.

Beispiele
1) Wir betrachten sog. schiefsymmetrische Matrizen, für die gilt $a_{kj} = -a_{jk},\ k = 1(1)n$.
Dann $\det(a_{kj}) = \det(-a_{jk}) = (-1)^n \det(a_{kj})$.
Wenn n ungerade und char$\mathbb{K} \neq 2$ (bei uns $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ ist char$\mathbb{K} = 0$), dann $\det(a_{kj}) = 0$.

2) Ist $a_{kj} = 0$ für $k > j$ (Dreiecksmatrix), dann $\det(a_{kj}) = \prod_{k=1}^{n} a_{kk}$.

3) $b_1,\dots,b_n \in \mathbb{K},\ a_{kj} = b_k^{j-1},\ k,j = 1(1)n$.

Dann $(a_{kj}) := \begin{pmatrix} 1 & b_1 & b_1^2 & \cdots & b_1^{n-1} \\ \vdots & & & & \vdots \\ 1 & b_n & b_n^2 & \cdots & b_n^{n-1} \end{pmatrix}$ VANDERMONDEsche Determinante [14]

$$\det(a_{kj}) = \begin{vmatrix} 1 & b_1 & b_1^2 & \cdots & b_1^{n-1} \\ \vdots & & & & \vdots \\ 1 & b_n & b_n^2 & \cdots & b_n^{n-1} \end{vmatrix}$$

$$= \begin{vmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & b_2-b_1 & b_2^2-b_2b_1 & \cdots & b_2^{n-1}-b_1b_1^{n-2} \\ \vdots & & & & \vdots \\ 1 & b_n-b_1 & \cdots & \cdots & b_n^{n-1}-b_1b_n^{n-2} \end{vmatrix}$$ (Mult. der Spalte $m-1$ mit b_1 und Subt. von m-ter Spalte)

$m = n, n-1, \dots, 2$

$$= \begin{vmatrix} b_2-b_1 & b_2^2-b_2b_1 & \cdots & b_2^{n-1}-b_1b_1^{n-2} \\ \vdots & & & \vdots \\ b_n-b_1 & \cdots & \cdots & b_n^{n-1}-b_1b_n^{n-2} \end{vmatrix}$$ (Ausklammern von $(b_i - b_1)$)

$$= \prod_{k=2}^{n}(b_k-b_1) \begin{vmatrix} 1 & b_2 & \cdots & b_2^{n-2} \\ \vdots & & & \vdots \\ 1 & b_n & \cdots & b_n^{n-2} \end{vmatrix}$$ (Induktion)

$$= \prod_{k>j}(b_k-b_j).$$ ■

Sei $\dim \mathbb{V} < \infty$ und $A : \mathbb{V} \to \mathbb{V}$ Endomorphismus. Ist $\{v_1,\dots,v_n\}$ Basis von $\mathbb{V}$, dann sind die Einträge von A angebbar, d.h. $\det(A)$ ist definiert.

Def.7.1.
1) Seien $\mathbb{V}$ ein $\mathbb{K}$-Vektorraum, $\dim \mathbb{V} < \infty,\ A \in \mathrm{Aut}(\mathbb{V},\mathbb{V})$. A heißt orientierungstreu , falls $\det A > 0$, orientierungsuntreu, wenn $\det a < 0$.
2) Seien $B_1 = \{v_1,\dots,v_n\}, B_2 = \{w_1,\dots,w_n\}$ Basen in $\mathbb{V}$. Sei $w_k = A(v_k)$. B_1 und B_2 heißen gleichorientiert, wenn $\det A > 0$.

Beispiel $\mathrm{GL}(n,\mathbb{R}) = \{A \in \mathrm{Gl}(n,\mathbb{R}) \mid \det A > 0\} \cup \{A \in \mathrm{Gl}(n,\mathbb{R}) \mid \det A < 0\}$ disjunkte Zerlegung.

Def.7.2.
Seien $A_1, A_2 \in \mathrm{Gl}(n,\mathbb{R})$.

[14] Alexandre Théophile VANDERMONDE (1735-1796) franz. Mathematiker

$\varphi : I \to \mathrm{Gl}(n,\mathbb{R}),\ t \mapsto \varphi(t) = (\varphi_{ij}(t)),\ I = [a,b] \subset \mathbb{R}$ ein Intervall mit $\varphi(a) = A_1,\ \varphi(b) = A_2$. Dann heißt φ ein Weg von A_1 nach A_2. (Für alle t müssen die Matrizen $= (\varphi_{ij}(t))$ invertierbar sein.)

Beispiel

$$(\varphi_{ij}(t)) = \begin{pmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{pmatrix},\ t \in [0, \frac{\pi}{2}].$$

$$A_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ A_2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

$\det(\varphi_{ij}(t)) = \cos^2 t + \sin^2 t = 1$ unabhängig von t, d.h. invertierbar für alle t.
$\Rightarrow$ Ist $\varphi : I \to \mathrm{Gl}(n,\mathbb{R})$ ein Weg von A_1 nach A_2, dann hat $\det A_1$ das selbe Vorzeichen wie $\det A_2$ (z.B. Möbiusband).

7.2 Definitionen und Beispiele

Def.7.3
Sei A ein Endomorphismus des $\mathbb{K}$-Vektorraumes $\mathbb{V}$. $\lambda \in \mathbb{K}$ heißt Eigenwert von A, wenn es ein $v \in \mathbb{V},\ v \neq 0$ gibt, so daß $Av = \lambda v$ gilt. v heißt Eigenvektor zum Eigenwert λ.

Beispiel
Sei $\mathbb{V}$ ein $\mathbb{K}$-Vektorraum, $\dim \mathbb{V} = 2$.
Sei $A = \begin{pmatrix} \cos\alpha & \sin\alpha \\ \sin\alpha & -\cos\alpha \end{pmatrix}$ und es gelte für ein $v \in \mathbb{V}$ und $\lambda \in \mathbb{K}$: $Av = \lambda v$.
Damit gilt $0 = Av - \lambda v = (A - \lambda \mathbb{I}_2)v$, d.h. $\begin{pmatrix} \cos\alpha - \lambda & \sin\alpha \\ \sin\alpha & -\cos\alpha - \lambda \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = 0 \Rightarrow \det(A - \lambda \mathbb{I}_2) = 0$
$\Rightarrow -(\cos\alpha - \lambda)(\cos\alpha + \lambda) - \sin^2\alpha = 0 \Leftrightarrow \lambda^2 = 1 \Leftrightarrow \lambda_1 = 1,\ \lambda_2 = -1.$
Wir lösen nun das Gleichungssystem für $\lambda_1 = 1$: $\begin{pmatrix} \cos\alpha - 1 & \sin\alpha \\ \sin\alpha & -\cos\alpha - 1 \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = 0$
$\Rightarrow v_1(\cos\alpha - 1) + v_2 \sin\alpha = 0$ und $v_1 \sin\alpha - v_2(\cos\alpha + 1) = 0$.
Sei $\sin\alpha \neq 0$. Da beide Gleichungen linear abhängig, reicht es aus, die Gleichung $(\cos\alpha - 1)v_1 + \sin\alpha v_2 = 0$ zu betrachten. Dies ist äquivalent zu $v_1 = \frac{\sin\alpha}{1-\cos\alpha} v_2 = \frac{2\sin\frac{\alpha}{2}\cos\frac{\alpha}{2}}{2\sin\frac{\alpha}{2}} v_2 = \frac{\cos\frac{\alpha}{2}}{\sin\frac{\alpha}{2}} v_1$.
Ein Eigenvektor ist also $(v_1, v_2) = \left(\cos\frac{\alpha}{2}, \sin\frac{\alpha}{2}\right)$. Dies gilt aber auch, wenn $\sin\alpha = 0$. ■

Def.7.4.
1) Ein Endomorphismus heißt diagonalisierbar, wenn es eine Basis von Eigenvektoren gibt.
Ist $\dim \mathbb{V} = n < \infty$, dann $A \in \mathrm{End}(\mathbb{V},\mathbb{V})$ diagonalisierbar, wenn eine Basis B von $\mathbb{V}$ existiert und die hiervon erzeugte Matrix für $A = M_B(A)$ diagonal ist, d.h. nur Einträge auf der Hauptdiagonalen besitzt und die restlichen Einträge gleich Null sind.
2) Sei $A_1, A_2 \in M(m \times n, \mathbb{K})$.
$A_1 \sim A_2$, wenn es ein $S \in \mathrm{GL}(m,\mathbb{K})$ und ein $T \in \mathrm{GL}(n,\mathbb{K})$ gibt, so daß $A_2 = SA_1T^{-1}$.
Ist $m = n$, dann heißen A_1 und A_2 ähnlich, d.h. $A_2 = SA_1S^{-1}$.

Folgerung
1. $A \in M(n \times n, \mathbb{K})$ diagonalisierbar g.d.w. $\exists\ S \in \mathrm{GL}(n,\mathbb{K})$ mit $SAS^{-1} = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$.
2. Seien $(\lambda_k, v_k),\ k = 1(1)m,\ m \leq \dim \mathbb{V}$ paarweise verschiedene Eigenwerte und dazugehörige Eigenvektoren. Dann sind die $v_1, \ldots, v_m$ linear unabhängig.
Beweis mittels vollständiger Induktion:
$m = 1 \Rightarrow v_1 \neq 0$ nach Definition.
Sei $m \geq 2$ und die Aussage für $m - 1$ wahr.

$$\text{Sei } \sum_{k=1}^{m} c_k v_k = 0 \Rightarrow \begin{cases} 0 = A\left(\sum\limits_{k=1}^{m} c_k v_k\right) = & c_1\lambda_1 v_1 + c_2\lambda_2 v_2 + \cdots + c_m\lambda_m v_m \\ 0 = \lambda_m \cdot \sum\limits_{k=1}^{m} c_k v_k = & c_1\lambda_m v_1 + c_2\lambda_m v_2 + \cdots + c_m\lambda_m v_m \end{cases}$$

$\Rightarrow c_1(\lambda_1 - \lambda_m)v_1 + \cdots + c_{m-1}(\lambda_{m-1} - \lambda_m)v_{m-1} = 0.$
Da $v_1, \ldots, v_{m-1}$ linear unabhängig nach Ind.voraussetzung und die $\lambda_k \neq \lambda_j$ für $k \neq j$, folgt $c_1 = \cdots = c_{m-1} = 0$ und damit $c_1 v_1 = 0$. Da $v_1 \neq 0 \Rightarrow c_1 = 0$.
3. Aus 2. folgt direkt: Es gibt höchstens $n = \dim \mathbb{V}$ Eigenwerte.
4. Sei $A \in \mathrm{End}(\mathbb{V})$. A habe paarweise verschiedene Eigenwerte $\lambda_1, \ldots, \lambda_n,\ n = \dim \mathbb{V}$.
Dann ist A diagonalisierbar.

Dies ist richtig, da zu jedem λ_k mindestens ein $v_k \neq 0$ existiert und diese nach 2. linear unabhängig sind. ■

Def.7.5.
Sei $A \in \mathrm{End}(\mathbb{V}),\ \lambda \in \mathbb{K}$. Mit $\mathrm{Eig}(A,\lambda) := \{v \in \mathbb{V} \mid Av = \lambda v\}$ bezeichnen wir den Eigenraum von A bzgl. λ.

Folgerung
1. $\mathrm{Eig}(A,\lambda) \subset \mathbb{V}$ ist ein Unterraum.
2. λ ist Eigenwert von A g.d.w. $\mathrm{Eig}(A,\lambda) \neq \{0\}$.
3. $\mathrm{Eig}(A,\lambda) \setminus \{0\}$ ist die Menge der zu λ gehörigen Eigenvektoren von A.
4. $\mathrm{Eig}(A,\lambda) = \ker(A - \lambda\mathbb{I}_n)$.
5. Sind $\lambda_1, \lambda_2 \in \mathbb{K},\ \lambda_1 \neq \lambda_2$, dann $\mathrm{Eig}(A,\lambda_1) \cap \mathrm{Eig}(A,\lambda_2) = \{0\}$.
Beweis von 5.: Sei $v \in \mathrm{Eig}(A,\lambda_1) \cap \mathrm{Eig}(A,\lambda_2) \Rightarrow \lambda_1 v = Av = \lambda_2 v \Rightarrow (\lambda_1 - \lambda_2)v = 0 \Rightarrow v = 0$. ■

7.3 Charakteristisches Polynom

Lemma 7.1.
Sei $A \in \mathrm{End}(\mathbb{V}),\ \lambda \in \mathbb{K}$. Dann gilt:
λ ist Eigenwert von $A \Leftrightarrow \det(A - \lambda\mathbb{I}_n) = 0$.
Beweis: λ ist Eigenwert $\Leftrightarrow \exists\ v \neq 0 : Av = \lambda v \Leftrightarrow Av - \lambda v = 0 \Leftrightarrow (A - \lambda\mathbb{I}_n)v = 0 \Leftrightarrow \ker(A - \lambda\mathbb{I}_n) \neq \{0\} \Leftrightarrow \mathrm{Im}(A - \lambda\mathbb{I}_n) \neq \mathbb{V} \Leftrightarrow \mathrm{rang}(A - \lambda\mathbb{I}_n) < \dim \mathbb{V} \Leftrightarrow \det(A - \lambda\mathbb{I}_n) = 0$. ■

Folgerung
Suchen wir Eigenwerte von A, dann müssen wir die Nullstellen von $P_A : \mathbb{K} \to \mathbb{K}$ mit $\lambda \mapsto \det(A - \lambda\mathbb{I}_n)$ suchen. Die so definierte Funktion P_A ist ein Polynom.
Beweis: Sei B Basis von $\mathbb{V}$ und $A = (a_{ij}) \in M_B(n \times n)$.

$$P_A(\lambda) = \det(A - \lambda\mathbb{I}_n) = \begin{vmatrix} a_{11} - \lambda & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} - \lambda & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} - \lambda \end{vmatrix}.$$

Mit Hilfe des Laplaceschen Entwicklungssatzes erhalten wir

$$P_A(\lambda) = \alpha_n\lambda^n + \alpha_{n-1}\lambda^{n-1} + \cdots + \alpha_1\lambda + \alpha_0,$$

wobei $\alpha_n = (-1)^n,\ \alpha_{n-1} = (-1)^{n-1}(a_{11} + \cdots + a_{nn}),\ \alpha_0 = \det A$. ■

Bezeichung
Die Funktion P_A wird als charakteristisches Polynom bezeichnet.
Die Funktion $\mathrm{Tr}(A) := a_{11} + \cdots + a_{nn}$ heißt Spur von A.

Beispiel

$$\begin{aligned} A = \begin{pmatrix} -1 & 6 \\ -1 & 4 \end{pmatrix} \Rightarrow \det(A - \lambda\mathbb{I}_2) &= \begin{vmatrix} -1-\lambda & 6 \\ -1 & 4-\lambda \end{vmatrix} \\ &= (-1-\lambda)(4-\lambda) + 6 \\ &= \lambda^2 - 3\lambda + 2 = (\lambda-1)(\lambda-2) \Rightarrow \\ \Rightarrow P_A(\lambda) &= (\lambda-1)(\lambda-2). \end{aligned}$$

Die Eigenwerte sind somit $\lambda_1 = 1$ und $\lambda_2 = 2$.
Lösen wir die zugehörigen Gleichungssysteme

$$\begin{pmatrix} -2 & 6 \\ -1 & 3 \end{pmatrix} \cdot v_1 = 0 \text{ und } \begin{pmatrix} -3 & 6 \\ -1 & 2 \end{pmatrix} \cdot v_2 = 0$$

so erhalten wir die zugehörigen Eigenvektoren $v_1 = \begin{pmatrix} 3 \\ 1 \end{pmatrix}$ und $v_2 = \begin{pmatrix} 2 \\ 1 \end{pmatrix}$. ■

Bemerkung
Seien $A \sim B$ zwei ähnliche Matrizen mit $B = SAS^{-1},\ S \in \mathrm{GL}(n,\mathbb{K})$. Dann haben A und B das gleiche charakteristische Polynom.

Beweis:

$$\begin{aligned}\det(B-\lambda\mathbb{I}_n) &= \det(SAS^{-1}-\lambda\mathbb{I}_n)\\ &= \det(SAS^{-1}-\lambda S\mathbb{I}_n S^{-1})\\ &= \det(S(A-\lambda\mathbb{I}_n)S^{-1})\\ &= \det(S)\cdot\det(A-\lambda\mathbb{I}_n)\cdot\det(S^{-1})\\ &= \det(A-\lambda\mathbb{I}_n)\end{aligned}$$

■

Folgerung
Das charakteristische Polynom eines Endomorphismus auf $\mathbb{V}$ ist unabhängig von der darstellenden Basis.

Zusammenfassend können wir folgenden Satz formulieren:
Satz 7.2.
Seien $\mathbb{V}$ ein $\mathbb{K}$-Vektorraum, $\dim\mathbb{V}<\infty,\ A\in\mathrm{End}(\mathbb{V})$. Das charakteristische Polynom $P_A(t)\in K[t]$ hat folgende Eigenschaften:
1. deg P_A =grad $P_A\le n$.
2. Die Nullstellen von P_A sind die Eigenwerte von A.
3. Sei λ ein Eigenwert von A. Dann erhält man $\mathrm{Eig}(A,\lambda)$ als Lösung des homogenen Gleichungssystems $(A-\lambda\mathbb{I}_n)x=0$. ■

Bemerkung zur Ähnlichkeit
A sei diagonalisierbar, dann existiert ein $S\in\mathrm{GL}(n\mathbb{K})$ mit $SAS^{-1}=\begin{pmatrix}\lambda_1 & & 0\\ & \ddots & \\ 0 & & \lambda_n\end{pmatrix}$.
Es gilt $(SAS^{-1}-\lambda\mathbb{I}_n)x=0\Leftrightarrow(SAS^{-1}-\lambda S\mathbb{I}_nS^{-1})x=0\Leftrightarrow AS^{-1}x=\lambda S^{-1}\mathbb{I}_nx\Leftrightarrow AS^{-1}x=\lambda S^{-1}x$.
Setzten wir nun $y:=S^{-1}x$ so erhalten wir $Ay=\lambda y$, d.h. die Spalten von S^{-1} bilden eine Basis von Eigenvektoren.

Beispiel
Es war $A=\begin{pmatrix}-1 & 6\\ -1 & 4\end{pmatrix}$ und $x_1=\begin{pmatrix}3\\1\end{pmatrix}$ und $x_2=\begin{pmatrix}2\\1\end{pmatrix}$ die Eigenvektoren.
Wählen wir $S^{-1}=(x_1,x_2)=\begin{pmatrix}3 & 2\\ 1 & 1\end{pmatrix}$ ergibt sich $S=\begin{pmatrix}1 & -2\\ -1 & 3\end{pmatrix}$.
Somit ist $SAS^{-1}=\begin{pmatrix}1 & -2\\ -1 & 3\end{pmatrix}\begin{pmatrix}-1 & 6\\ -1 & 4\end{pmatrix}\begin{pmatrix}3 & 2\\ 1 & 1\end{pmatrix}=\begin{pmatrix}1 & 0\\ 0 & 2\end{pmatrix}$.
In der Hauptdiagonalen stehen die Eigenwerte. ■

7.4 Diagonalisierung, Tridiagonalisierung

1) Sei $\dim\mathbb{V}=n, A\in\mathrm{End}(\mathbb{V})$ und diagonalisierbar, dann

$$A=\begin{pmatrix}\lambda_1 & & 0\\ & \ddots & \\ 0 & & \lambda_n\end{pmatrix}\Rightarrow\det(A-t\mathbb{I}_n)=\begin{vmatrix}\lambda_1-t & & 0\\ & \ddots & \\ 0 & & \lambda_n-t\end{vmatrix}=P_A(t)=(\lambda_1-t)\cdots(\lambda_n-t).$$

Umgekehrt, wenn $P_A(t)=\pm(\lambda_1-t)\cdots(\lambda_n-t)$, dann ist A diagonalisierbar, $\lambda_k\neq\lambda_j,\ k\neq j$.
Damit ist der Fall einfacher Nullstellen von P_A geklärt.
Nun nehmen wir an, P_A habe mehrfache Nullstellen, d.h. $P_A(t)=\pm(t-\lambda_1)^{r_1}\cdots(t-\lambda_k)^{r_k},\ \lambda_i\neq\lambda_j,\ i\neq j,\ 1\le r_j\le n,\ i=1(1)k,\ r_1+r_2+\cdots+r_k=n$.
r_i heißt Vielfachheit von λ_i, Bezeichnung $\mu(P_A,\lambda_i):=r_i$.

Bemerkung
Sei λ ein Eigenwert zu A. Es gilt: $1\le\dim\mathrm{Eig}(A,\lambda)\le\mu(P_A,\lambda)$.
Beweis: Sei $\{v_1,\ldots,v_s\}$ eine Basis in $\mathrm{Eig}(A,\lambda)$. Da λ Eigenwert ist, folgt $1\le s$. Wir ergänzen zu einer Basis von $\mathbb{V}$: $B=(v_1,\ldots,v_s,v_{s+1},\ldots,v_n)$.
Wir stellen den Endomorphismus A als Matrix bzgl. B dar:

$$A=\left(\begin{array}{ccc|c}\lambda & & 0 & \\ & \ddots & & * \\ 0 & & \lambda & \\ \hline & 0 & & \tilde{A}\end{array}\right).$$

Dann folgt aber $P_A(t) = (t-\lambda)^s \cdot P_{\tilde{A}}(t)$. Aus diesem Grund ist $\dim \mathrm{Eig}(A,\lambda) \leq \mu(P_A,\lambda)$. ■

Hauptsatz 7.3.
Seien $\mathbb{V}$ ein $\mathbb{K}$-Vektorraum, $\dim \mathbb{V} < \infty,\ A \in \mathrm{End}(\mathbb{V})$. Dann sind folgende Aussagen äquivalent:
(i) A ist diagonalisierbar.
(ii) $P_A(t)$ zerfällt in Linearfaktoren und $\dim \mathrm{Eig}(A,\lambda) = \mu(P_A,\lambda)$ für alle Eigenwerte von A.
(iii) Seien $\lambda_1,\ldots,\lambda_k$ Eigenwerte von A, $\lambda_i \neq \lambda_j,\ i \neq j$. Dann ist $\mathbb{V} = \mathrm{Eig}(A,\lambda_1) \oplus \cdots \oplus \mathrm{Eig}(A,\lambda_k)$.
Beweis:
(i)⇒(ii)
Da A diagonalisierbar ist, so erzeugen wir aus den Basen der Eigenräume die Basis für $\mathbb{V}$:
$\lambda_1,\ldots,\lambda_k$ seien die Eigenwerte von A. Sei $\{v_1^{(i)},\ldots,v_{s_i}^{(i)}\}$ Basis von $\mathrm{Eig}(A,\lambda_i)$ für $i = 1(1)k$.
Mit $r_i = \mu(P_A,\lambda_i)$ gilt: $s_1 + \cdots + s_k = n,\ v_1 + \cdots + r_k = n$ und $s_i \leq r_i$.
Dies ist nur möglich für $s_i = r_i$, also (ii).
(ii)⇒(iii)
Nach Definition der direkten Summe (Elemente aus $\mathrm{Eig}(A,\lambda_i)$ sind voneinander linear unabhängig) folgt:
$\dim(\mathrm{Eig}(A,\lambda_1) \oplus \cdots \oplus \mathrm{Eig}(A,\lambda_k)) = r_1 + \cdots + r_k = n \Rightarrow$ (iii).
(iii)⇒(i)
Für jedes $i \in \{1,\ldots,k\}$ sei $B_i = \{v_1^{(i)},\ldots,v_{s_i}^{(i)}\}$ Basis von $\mathrm{Eig}(A,\lambda_i)$. Vereinigt man alle B_i, d.h. $B = \{v_1^{(1)},\ldots,v_{s_1}^{(1)},\ldots,v_1^{(k)},\ldots,v_{s_k}^{(k)}\}$, dann hat man eine Basis von $\mathbb{V}$. Diese besteht aus Eigenvektoren, somit ist A diagonalisierbar $s_i = r_i,\ \forall\, i$. Dann ist $A \in M_B(n \times n, \mathbb{K})$ und

$$A = \begin{pmatrix} \lambda_1 & & & & & & & & \\ & \ddots & & & & & & & \\ & & \lambda_1 & & & & 0 & & \\ & & & \lambda_2 & & & & & \\ & & & & \ddots & & & & \\ & & & & & \lambda_2 & & & \\ & & & & & & \ddots & & \\ & & & & & & & \lambda_k & \\ & & & & & & & & \ddots \\ & & 0 & & & & & & \lambda_k \end{pmatrix}.$$

■

7.5 Endomorphismuspotenzen, Nilpotenz, JORDANsche Normalform

Betrachte $P(t) \in \mathbb{K}[t]:\ P(t) := \alpha_r t^r + \cdots + \alpha_1 t + \alpha_0$.
$A \in \mathrm{End}(\mathbb{V}),\ A^2 := A \circ A$, allg. $A^n := \underbrace{A \circ \cdots \circ A}_{n-\text{mal}}$.
Wir betrachten $P(A) := \alpha_r A^r + \cdots + \alpha_1 A + \alpha_0$.
Wenn $0 \neq v \in \ker(P(A)) \Leftrightarrow \alpha_r A(v)^r + \cdots + \alpha_1 A(v) + \alpha_0 = 0 \Rightarrow \{v, Av, \ldots, A^r(v)\}$ sind linear unabhängig für $P \neq 0$. Wenn $\alpha_r \neq 0 \Rightarrow W := \mathrm{span}(v, A(v), \ldots, A^{r-1}(V)\} \subset \mathbb{V}$. $1 \leq \dim W \leq r$.

Satz von CAYLEY-HAMILTON [15]
Sei $\mathbb{V}$ ein $\mathbb{K}$-Vektorraum, $\dim \mathbb{V} = n < \infty,\ A \in \mathrm{End}(\mathbb{V}),\ P_A \in \mathbb{K}[t]$.
Dann $P_A(A) = \mathfrak{O} \in \mathrm{End}(\mathbb{V})$.
($\mathfrak{O}$ bezeichnet den Endomorphismus, der $\mathbb{V}$ auf 0_n abbildet.)
Beweis: FISCHER S.241ff

Def. $A \in \mathrm{End}(\mathbb{V})$ heißt <u>nilpotent</u>, wenn $\exists\ k \in \mathbb{N}:\ A^k = \mathfrak{O}$.

Beispiel

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},\ \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \Rightarrow k = 2.$$

Bezeichnung $\mathrm{Hau}(A,\lambda) := \ker(A - \lambda\mathbb{I}_n)^r$ ist der <u>Hauptraum</u> oder <u>verallg. Eigenraum</u> von A zu r.

Es gilt: $\mathrm{Eig}(A,\lambda) = \ker(A - \lambda\mathbb{I}_n) \subset \ker(A - \lambda\mathbb{I}_n)^r = \mathrm{Hau}(A,\lambda)$.

[15] Arthur CAYLEY (1821-1895) engl.Mathematiker, William Rowan HAMILTON (1805-1865) irischer Mathematiker

Satz über die Hauptraumzerlegung
Sei $A \in \mathrm{End}(\mathbb{V}),\ P_A(t) = \pm(t-\lambda_1)^{r_1}\cdots(t-\lambda_k)^{r_k},\ \lambda_i \neq \lambda_j,\ i \neq j.$
$\mathbb{V}_i := \mathrm{Hau}(A, \lambda_i) \subset \mathbb{V}$ für jedes $i = 1(1)k$. Dann gilt:
(1) $A(\mathbb{V}_i) \subset \mathbb{V}_i$ und $\dim \mathbb{V}_i = r_i,\ i = 1(1)k.$
(2) $\mathbb{V} = \mathbb{V}_1 \oplus \cdots \oplus \mathbb{V}_k.$
(3) $A = A_D + A_N$ Zerlegung von A mit A_D diagonalisierbar und A_N nilpotent, $A_D \circ A_N = A_N \circ A_D.$

Folgerung
$A \in M(n \times n, \mathbb{K}),\ P_A$ wie oben. Dann gibt es ein $S \in \mathrm{GL}(n, \mathbb{K})$, so daß

$$SAS^{-1} = \begin{pmatrix} \lambda_1 \mathbb{I}_{r_1} + N_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_k \mathbb{I}_{r_k} + N_k \end{pmatrix} =: \hat{A},$$

dabei ist $\lambda_j \mathbb{I}_{r_j} + N_j = \begin{pmatrix} \lambda_j & & * \\ & \ddots & \\ 0 & & \lambda_j \end{pmatrix} \in M(r_j \times r_j, \mathbb{K})$. N ist dann nilpotent.
Dann erhält man das Ergebnis:
Sei $A \in \mathrm{End}(\mathbb{V}),\ P_A(t) = \pm(t-\lambda_1)^{r_1}\cdots(t-\lambda_k)^{r_k},\ \lambda_i \neq \lambda_j,\ i \neq j.$
Dann gibt es Basen von $\mathbb{V}$ so, daß $M_B(A) = \hat{A}$ und $N_j = \begin{pmatrix} 0 & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & 0 \end{pmatrix} \in M(r_k \times r_k, \mathbb{K}).$

Allgemein gilt der **Satz über die Jordansche Normalform**[16]
Sei $\mathbb{V}$ ein $\mathbb{K}$-Vektorraum, $\dim \mathbb{V} = n < \infty$.
Sei $A \in \mathrm{End}(\mathbb{V}),\ P_A(t) = \pm(t-\lambda_1)\cdots(t-\lambda_n)(\lambda_i$ ggf. nicht paarweise verschieden).
Dann gibt es $B \subset \mathbb{V}$, so daß

$${}_BA_B = \begin{pmatrix} \lambda_1 & 1 & & 0 & & & & & & & & & \\ & \ddots & \ddots & & & & & & & & & & \\ & & \ddots & 1 & & & & & & & & & \\ 0 & & & \lambda_1 & & & & & & & & & \\ & & & & \lambda_2 & 1 & & 0 & & & & & \\ & & & & & \ddots & \ddots & & & & & & \\ & & & & & & \ddots & 1 & & & & & \\ & & & & 0 & & & \lambda_2 & & & & & \\ & & & & & & & & \ddots & & & & \\ & & & & & & & & & \lambda_n & 1 & & 0 \\ & & & & & & & & & & \ddots & \ddots & \\ & & 0 & & & & & & & & & \ddots & 1 \\ & & & & & & & & & 0 & & & \lambda_n \end{pmatrix}.$$

Beweis: Stroht S.296-312

8 Orthogonalität

8.1 Innere Produkte

Def.8.1.
Sei $\mathbb{V}$ ein $\mathbb{R}$-Vektorraum, $\dim \mathbb{V} = n < \infty$. Dann sei $\langle \cdot, \cdot \rangle : \mathbb{V} \times \mathbb{V} \to \mathbb{R}^+$ eine Abbildung, wobei gelten soll:
(1) $\forall\ u, v \in \mathbb{V}\ \ \langle u, v \rangle = \langle v, u \rangle,$
(2) $\forall\ u, v, w \in \mathbb{V}\ \ \langle u + v, w \rangle = \langle u, w \rangle + \langle v, w \rangle,$
(3) $\forall\ u, v \in \mathbb{V}\ \forall\ \lambda \in \mathbb{R}\ \ \langle \lambda u, v \rangle = \lambda \langle u, v \rangle,$
(4) $\langle v, v \rangle = 0 \Leftrightarrow v = 0.$

[16] Marie Ennemond Camille Jordan (1838-1922) franz.Mathematiker

Eine solche Abbildung heißt inneres Produkt oder Skalarprodukt.

Beispiel Seien $u = (u_1, \ldots, u_n),\ v = (v_1, \ldots, v_n) \in \mathbb{V}$. Dann ist mit $\langle u, v\rangle := \sum_{k=1}^{n} u_k v_k$ ein inneres Produkt definiert, das sog. EUKLIDische Skalarprodukt.
Man kann dies verallgemeinern: Sei $A \in \mathrm{GL}(n, \mathbb{R})$. Man definiert dann das gewichtete innere Produkt durch
$\langle u, v\rangle_A := \langle u, Av\rangle = \langle u, \left(\sum_{j=1}^{n} a_{kj} v_j\right)\rangle = \sum_{k=1}^{n}\sum_{j=1}^{n} u_k a_{kj} v_j.$

Man definiert durch $\|v\|^2 := \langle v, v\rangle$ eine Norm auf $\mathbb{V}$. Für Normen $\|\cdot\| : \mathbb{V} \to \mathbb{R}^+$ gilt allgemein:

(1) $\|v\| \geq 0$ und $\|v\| = 0 \Leftrightarrow v = 0$,
(2) $\|\lambda v\| = |\lambda|\|v\|$,
(3) $\|u + v\| \leq \|u\| + \|v\|$ (Dreiecksungleichung).

Mit Hilfe der Norm kann man eine Metrik (Abstand) $\rho(u, v) : \mathbb{V} \times \mathbb{V} \to \mathbb{R}$ in $\mathbb{V}$ definieren. Wir setzten dabei $\rho(u, v) := \|u - v\|$.

Die Metrik hat folgende Eigenschaften:
(1) $\rho(u, v) \geq 0$ und $\rho(u, v) = 0 \Leftrightarrow u = v$,
(2) $\rho(u, v) = \rho(v, u)$,
(3) $\rho(u, v) \leq \rho(u, w) + \rho(w, v)$ (Dreiecksungleichung).

Beispiel EUKLIDischer Abstand (Metrik) $\rho(u, v) = \sqrt{(u_1 - v_1)^2 + \cdots + (u_n - v_n)^2}$.

Betrachten wir das gewichtete innere Skalarprodukt und setzten $A = \mathbb{I}_n$, so erhalten wir mittels

$$\rho(u, v) = \|u - v\| = \sqrt{\langle u - v, \mathbb{I}_n(u - v)\rangle} = \sqrt{\langle u - v, u - v\rangle} = \sqrt{(u_1 - v_1)^2 + \cdots + (u_n - v_n)^2}$$

den euklidischen Abstand.

Beispiel Setzen wir $n = 4$ und $A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$ die MINKOWSKI-Matrix und $\rho(u, v)$ ist der MINKOWSKI-Abstand, d.h. $\rho(u, v) = \sqrt{(u_1 - v_1)^2 - (u_2 - v_2)^2 - (u_3 - v_3)^2 - (u_4 - v_4)^2}$.
Dann kann $\rho(u, v) = 0$ sein, auch wenn $u \neq v$. (Anwendung in der spez. Relativitätstheorie, Lichtgeodäten)

Lemma 8.1. (CAUCHY-SCHWARZsche Ungleichung)
Sei $\mathbb{V}$ ein $\mathbb{R}$-Vektorraum, $\dim \mathbb{V} = n < \infty$. Seien $u, v \in \mathbb{V}$. Dann gilt:

$$\langle u, v\rangle^2 \leq \langle u, u\rangle\langle v, v\rangle.$$

Beweis: Wenn $u = 0$ oder $v = 0$, dann ist $\langle u, v\rangle = 0$ und wir sind fertig.
Also seien $u \neq 0$ und $v \neq 0$. $a := \langle u, u\rangle,\ b := 2\langle u, v\rangle,\ c := \langle v, v\rangle,\ t \in \mathbb{R}$.
Wir betrachten $0 \leq \langle (tu + v), (tu + v)\rangle = \langle u, u\rangle t^2 + 2\langle u, v\rangle t + \langle v, v\rangle = at^2 + bt + c$.
Nullstellen zu $t^2 + \frac{b}{a}t + \frac{c}{a} = 0$ sind $t_1, t_2 = -\frac{1}{2}\frac{b}{a} \pm \sqrt{\frac{b^2}{4a^2} - \frac{c}{a}} = -\frac{1}{2}\frac{b}{a} \pm \frac{1}{2a}\sqrt{b^2 - 4ac}$.
Sollen keinen reellen Wurzeln mehrfach auftreten, dann

$$b^2 - 4ac \leq 0 \Leftrightarrow 4\langle u, v\rangle - 4\langle u, u\rangle\langle v, v\rangle \leq 0 \Leftrightarrow \langle u, v\rangle^2 \leq \langle u, u\rangle\langle v, v\rangle.$$

■

Folgerung

$$\langle u, v\rangle^2 \leq \langle u, u\rangle\langle v, v\rangle \Leftrightarrow \langle u, v\rangle^2 \leq \|u\|^2 \cdot \|v\|^2 \Leftrightarrow |\langle u, v\rangle| \leq \|u\| \cdot \|v\|.$$

Anwendung
$|u_1 v_1 + \cdots + u_n v_n| \leq (u_1^2 + \cdots + u_n^2)^{\frac{1}{2}}(v_1^2 + \cdots + v_n^2)^{\frac{1}{2}}$.
Betrachte $\left(\frac{\langle u, v\rangle}{\|u\|\|v\|}\right)^2 \leq 1 \Leftrightarrow -1 \leq \frac{\langle u, v\rangle}{\|u\|\|v\|} \leq 1$.
Damit kann man einen Winkel definieren: $\cos\theta = \cos(u, v) := \frac{\langle u, v\rangle}{\|u\|\|v\|}$.
z.B. $u = (4, 3, 1, -2),\ v = (-2, 1, 2, 3)$. Dann

$$\|u\| = \sqrt{30},\ \|v\| = \sqrt{18},\ \langle u, v\rangle = -9,\ \cos\theta = -\frac{9}{\sqrt{30}\sqrt{18}} = -\frac{3}{2\sqrt{15}}.$$

Speziell für $\mathbb{V} = \mathbb{R}^2$: $\|u\| = a,\ \|v\| = b \Rightarrow \langle \vec{a}, \vec{b}\rangle = a \cdot b \cdot \cos(a, b)$ bekannt aus der Schule.

8.2 Orthogonalbasis, GRAM-SCHMIDT-Verfahren

Def.8.2.
Seien $u, v \in \mathbb{V},\ u \neq 0,\ v \neq 0$. Dann heißen u, v orthogonal, wenn $\langle u, v\rangle = 0$ (Symbol $u \perp v$).

Folgerung Seien $u \perp v$.
Dann $\|u+v\|^2 = \langle u+v, u+v\rangle = \|u\|^2 + 2\langle u, v\rangle + \|v\|^2 = \|u\|^2 + \|v\|^2$ (Verallgemeinerter PYTHAGORAS).

Seien $M_1, M_2 \subset \mathbb{V}$ Mengen in $\mathbb{V}$ für die gilt: $\forall\ u \in M_1,\ \forall\ v \in M_2\ \langle u, v\rangle = 0$. Dann schreibt man $M_1 \perp M_2$.

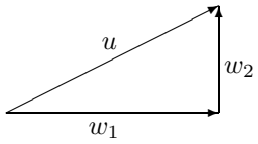
Normierung von Vektoren
Sei $v = (1,2,3) \Rightarrow \|v\| = \sqrt{14}$.
Wir betrachten $u = \frac{v}{\|v\|}$. Damit ist $u = (\frac{1}{\sqrt{14}}, \frac{2}{\sqrt{14}}, \frac{3}{\sqrt{14}}) \Rightarrow \|u\|^2 = \frac{1}{14} + \frac{2}{14} + \frac{3}{14} = 1 \Rightarrow \|u\| = 1$.

Allgemein: Sei $v \in \mathbb{V}$. Dann ist $u \in \mathbb{V}$ mit $u = \frac{v}{\|v\|}$ ein Einheitsvektor, d.h. $\|u\| = 1$.

Bedeutung: Sei $\{v_1, \ldots, v_n\}$ eine sog. Orthonormalbasis (ONB) in $\mathbb{V}$, d.h. $\langle v_i, v_j\rangle = \delta_{ij} := \begin{cases} 0 & i \neq j \\ 1 & i = j \end{cases}$
$u = c_1 v_1 + \cdots + c_n v_n$. Wie berechnet man die c_k?
Bilde Skalarprodukt mit $v_k \Rightarrow \langle u, v_k\rangle = c_k \Rightarrow u = \langle u, v_1\rangle v_1 + \cdots + \langle u, v_n\rangle v_n$.

Standard-ONB: $\{e_k\}_{k=1}^n,\ e_k := (0, \ldots, 0, \underbrace{1}_{\uparrow k}, 0, \ldots, 0)$.

Projektionen



$u = w_1 + w_2,\ P : u \mapsto w_1,\ P^\perp : u \mapsto w_2$.

Allgemein: Sei $\mathbb{V}_1$ ein endlich dimensionaler Unterraum in $\mathbb{V}$. Auf $\mathbb{V}$ sei ein Skalarprodukt $\langle \cdot, \cdot\rangle$ definiert. Dann $\forall\ u \in \mathbb{V}:\ u = w_1 + w_2$ und $w_1 \in \mathbb{V}_1$, wobei $w_2 \perp w_1$. Wir formulieren dies noch als Satz:

Satz 8.1.
Jeder endlich dimensionale Vektorraum mit innerem Produkt hat eine ONB.
Beweis: Sei $\mathbb{V} \neq \{0\}$, $\{u_1, \ldots, u_n\}$ eine beliebige Basis von $\mathbb{V}$. Wir geben dann ein solches Verfahren an, daß man aus $\{u_1, \ldots, u_n\}$ eine ONB $\{v_{1_o}, \ldots, v_{n_o}\}$ machen kann.
GRAM-SCHMIDT-Verfahren:
Schritt I: Setze $v_1 := \frac{u_1}{\|u_1\|}$.
Schritt II: Setze $v_2 \perp v_1$ vermittels $v_2 := u_2 - \frac{\langle v_1, u_2\rangle}{\|v_1\|^2} v_1$.
$v_2 \perp v_1$ denn: $\langle v_2, v_1\rangle = \langle u_2 - \frac{\langle v_1, u_2\rangle}{\|v_1\|^2} v_1, v_1\rangle = \langle u_2, v_1\rangle - \frac{\langle v_1, u_2\rangle\langle v_1, v_1\rangle}{\|v_1\|^2} = \langle u_2, v_1\rangle - \frac{\langle u_2, v_1\rangle\|v_1\|^2}{\|v_1\|^2} = 0$.
Schritt III: $v_3 := u_3 - \frac{\langle v_1, u_3\rangle}{\|v_1\|^2} v_1 - \frac{\langle v_2, u_3\rangle}{\|v_2\|^2} v_2$.
Dann ist $v_1 \perp v_3$ und $v_2 \perp v_3$.
allgemein k-ter Schritt:

$$v_k = u_k - \frac{\langle v_1, u_k\rangle}{\|v_1\|^2} v_1 - \frac{\langle v_2, u_k\rangle}{\|v_2\|^2} v_2 - \cdots - \frac{\langle v_{k-1}, u_k\rangle}{\|v_{k-1}\|^2} v_{k-1}.$$

Dies wird fortgesetzt bis $k = n$.
Man erhält eine Folge orthogonaler Vektoren $\{v_1, \ldots, v_n\}$, wenn man diese normiert, dann hat man eine ONB. ■

Beispiel
$u_1 = (1,0,0),\ u_2 = (3,7,-2),\ u_3 = (0,4,1)$.
1. Wir setzen $v_1 := u_1$, da $\|u_1\| = 1$ setzen wir $v_{1_o} := v_1$.
2. $v_2 := u_2 - \frac{\langle v_1, u_2\rangle}{\|v_1\|^2} v_1 = (3,7,-2) - \frac{3}{1}(1,0,0) = (0,7,-2)$
$\|v_2\| = \sqrt{49+4} = \sqrt{53} \Rightarrow v_{2_o} := \frac{1}{\sqrt{53}}(0,7,-2)$.
3. $v_3 := u_3 - \frac{\langle v_1, u_3\rangle}{\|v_1\|^2} v_1 - \frac{\langle v_2, u_3\rangle}{\|v_2\|^2} v_2 = (0,4,1) - 0 - \frac{\langle (0,7,-2), (0,4,1)\rangle}{53}(0,7,-2) = (0,4,1) - \frac{26}{53}(0,7,-2) = (0, \frac{30}{53}, \frac{105}{53})$

$\|v_3\| = \sqrt{\left(\frac{30}{53}\right)^2 + \left(\frac{105}{53}\right)^2} = \frac{1}{53}\sqrt{11925} \Rightarrow v_{3_o} := \frac{53}{\sqrt{11925}}(0, \frac{30}{53}, \frac{105}{53})$. ■

Dokument zuletzt geändert am 22.06.2002. Hinweise auf Fehler bitte an mrw@mathematik.hu-berlin.de