Algebraische Grundlagen der Informatik

SoSe 2024

KAPITEL I: Komplexe Zahlen

1. Grundlagen

Dozentin: Prof. Dr. Agnes Radl

Email: agnes.radl@informatik.hs-fulda.de

Erinnerung: bisherige Zahlbereiche

- $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ „Menge der natürlichen Zahlen“
- $\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \ldots\}$ „Menge der ganzen Zahlen“
- $\mathbb{Q} = \left\{ \frac{m}{n} : m, n \in \mathbb{Z}, n \neq 0 \right\}$ „Menge der rationalen Zahlen“
- $\mathbb{R} =$ Menge aller Dezimalzahlen „Menge der reellen Zahlen“

Bemerkung

- Die Gleichung $x + 2 = 1$ ist nicht in $\mathbb{N}$ lösbar, aber in $\mathbb{Z}$.
- Die Gleichung $2x = 1$ ist nicht in $\mathbb{Z}$ lösbar, aber in $\mathbb{Q}$.
- Die Gleichung $x^2 = 2$ ist nicht in $\mathbb{Q}$ lösbar, aber in $\mathbb{R}$.
- Die Gleichung $x^2 = -1$ ist nicht in $\mathbb{R}$ lösbar.

Komplexe Zahlen

Definition

Unter der Menge der komplexen Zahlen $\mathbb{C}$ versteht man die Menge

$$\mathbb{C} := \mathbb{R} \times \mathbb{R}.$$

Die Addition „$+$“, Subtraktion „$-$“ und Multiplikation „$\cdot$“ zweier komplexer Zahlen (x, y) und (u, v) sind definiert durch

- $(x, y) + (u, v) := (x + u, y + v)$,
- $(x, y) - (u, v) := (x - u, y - v)$,
- $(x, y) \cdot (u, v) := (xu - yv, xv + yu)$.

Beobachtungen

- Addition, Multiplikation sind kommutativ. ($\to$ nachrechnen)
- Es gelten Assoziativ- und Distributivgesetz. ($\to$ nachrechnen)
- $(0, 0)$ ist das „Neutralelement“ der Addition, denn

$$(x, y) + (0, 0) = (x + 0, y + 0) = (x, y).$$

- $(1, 0)$ ist das „Neutralelement“ der Multiplikation, denn

$$(x, y) \cdot (1, 0) = (x \cdot 1 - y \cdot 0, x \cdot 0 + y \cdot 1) = (x, y).$$

Division in $\mathbb{C}$

Beobachtung

Falls $(x, y) \neq (0, 0)$, dann ist

$$\begin{aligned} &(x,y)\cdot\left(\frac{x}{x^2+y^2},\frac{-y}{x^2+y^2}\right) \\ =\ &\left(x\frac{x}{x^2+y^2}-y\frac{-y}{x^2+y^2},x\frac{-y}{x^2+y^2}+y\frac{x}{x^2+y^2}\right) \\ =\ &(1,0). \end{aligned}$$

Damit definiere nun die Division:

Definition

Falls $(u, v), (x, y) \in \mathbb{C}$ und $(x, y) \neq (0, 0)$, so definiert man

$$\frac{(u,v)}{(x,y)} := (u,v)\cdot\left(\frac{x}{x^2+y^2},\frac{-y}{x^2+y^2}\right).$$

Einbettung von $\mathbb{R}$ in $\mathbb{C}$

Beobachtung

Für alle $x_1, x_2 \in \mathbb{R}$ gilt:

- $(x_1, 0) + (x_2, 0) = (x_1 + x_2, 0)$
- $(x_1, 0) \cdot (x_2, 0) = (x_1 x_2, 0)$

Komplexe Zahlen der Form $(x, 0)$ werden also wie reelle Zahlen addiert und multipliziert.

Fazit

Jede reelle Zahl x kann also als komplexe Zahl $(x, 0)$ aufgefasst werden. In diesem Sinn ist

$$\mathbb{R} \subseteq \mathbb{C}.$$

Andere Notation für komplexe Zahlen

Wir verwenden meistens folgende Notation:

- x statt $(x, 0)$
- i statt $(0, 1)$

Wegen

$$(x, y) = (x, 0) + (0, y) = (x, 0) + (0, 1) \cdot (y, 0) = x + \mathrm{i}\, y$$

schreiben wir

- $x + \mathrm{i}\, y$ statt (x, y).

Beispiele

- $\mathrm{i}^2 = (0,1)\cdot(0,1) = (-1,0) = -1$
- $$\begin{aligned}(1+2\,\mathrm{i})(2+3\,\mathrm{i}) &\overset{\text{Distr.}}{=} 1\cdot(2+3\,\mathrm{i}) + 2\,\mathrm{i}\cdot(2+3\,\mathrm{i})\\ &= 2+3\,\mathrm{i}+4\,\mathrm{i}+6\,\mathrm{i}^2\\ &= -4+7\,\mathrm{i}\end{aligned}$$
- Darstellung von $\frac{1+2\,\mathrm{i}}{2-3\,\mathrm{i}}$ in der Form $x+\mathrm{i}\,y$, $x,y\in\mathbb{R}$:

$$\frac{1+2\,\mathrm{i}}{2-3\,\mathrm{i}} = \frac{1+2\,\mathrm{i}}{2-3\,\mathrm{i}}\cdot\frac{2+3\,\mathrm{i}}{2+3\,\mathrm{i}} = \frac{-4+7\,\mathrm{i}}{13} = -\frac{4}{13}+\frac{7}{13}\,\mathrm{i}\,.$$

wichtige Begriffe

Definition

Sei $z := x + \mathrm{i}\, y \in \mathbb{C}$, wobei $x, y \in \mathbb{R}$.

- $\operatorname{Re}(z) := x$ ist der Realteil von z.
- $\operatorname{Im}(z) := y$ ist der Imaginärteil von z.
- $\overline{z} := x - \mathrm{i}\, y$ ist die zu z konjugiert komplexe Zahl.
- $|z| := \sqrt{x^2 + y^2}$ ist der Betrag von z.

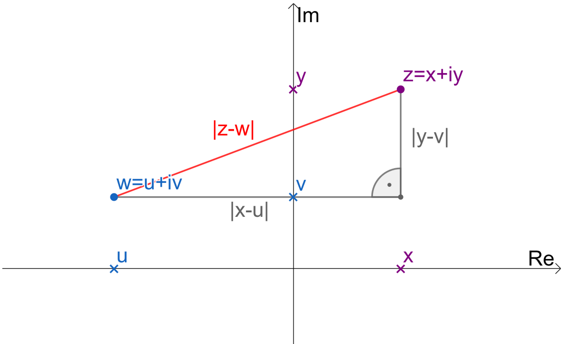
Abstand von z zu w

Bemerkung

Für $z = x + \mathrm{i}\, y$, $w = u + \mathrm{i}\, v$ mit $x, y, u, v \in \mathbb{R}$ wird $|z - w|$ interpretiert als der Abstand von z zu w, denn

$$|z - w| = \sqrt{(\mathrm{Re}(z - w))^2 + (\mathrm{Im}(z - w))^2} = \sqrt{(x - u)^2 + (y - v)^2}.$$

Skizze:



Rechenregeln

Für $z, w \in \mathbb{C}$ gelten:

1. $\overline{\overline{z}} = z$
2. $\overline{z + w} = \overline{z} + \overline{w}, \quad \overline{z \cdot w} = \overline{z} \cdot \overline{w}$
3. Ist $z = x + \mathrm{i}\, y$ mit $x, y \in \mathbb{R}$, so ist $|z|^2 = z \cdot \overline{z} = x^2 + y^2$.
4. Falls $z \neq 0$, dann ist $\frac{1}{z} = \frac{\overline{z}}{|z|^2}$.
5. $\mathrm{Re}(z) = \frac{1}{2}(z + \overline{z}), \quad \mathrm{Im}(z) = \frac{1}{2\,\mathrm{i}}(z - \overline{z})$
6. $|z| = |\overline{z}|$
7. $|\mathrm{Re}(z)| \leq |z|$, $|\mathrm{Im}(z)| \leq |z|$
8. $|z \cdot w| = |z| \cdot |w|, \quad \left|\frac{z}{w}\right| = \frac{|z|}{|w|}$ falls $w \neq 0$

Beweisidee:
1.–8. kann man direkt nachprüfen.

Dreiecksungleichung

Satz

Für alle $z, w \in \mathbb{C}$ gilt

$$|z + w| \leq |z| + |w| .$$

Algebraische Grundlagen der Informatik

SoSe 2024

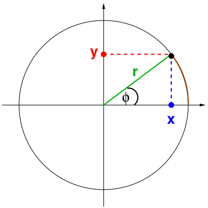
KAPITEL I: Komplexe Zahlen

2. Polardarstellung

Dozentin: Prof. Dr. Agnes Radl

Email: `agnes.radl@informatik.hs-fulda.de`

Erinnerung (WiSe 2023/2024): Sinus und Kosinus

- 

  $\varphi = \frac{\text{Länge des Kreisbogens}}{r}$

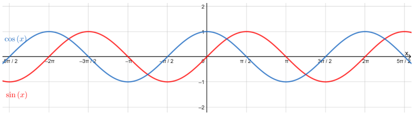
  $\sin(\varphi) = \frac{y}{r}$

  $\cos(\varphi) = \frac{x}{r}$

  Kreiszahl $\pi = 3,141...$

  Kreisumfang $2\pi r$

- $\sin : \mathbb{R} \to [-1,1]$ und $\cos : \mathbb{R} \to [-1,1]$ sind 2π-periodisch, das heißt, für alle $\varphi \in \mathbb{R}$ gilt:
  $\sin(\varphi + 2\pi) = \sin(\varphi)$ und $\cos(\varphi + 2\pi) = \cos(\varphi)$.



	0	$\frac{\pi}{2}$	π	$\frac{3\pi}{2}$	2π
sin	0	1	0	-1	0
cos	1	0	-1	0	1

- $\cos(-\varphi) = \cos(\varphi)$, $\sin(-\varphi) = -\sin(\varphi)$ für alle $\varphi \in \mathbb{R}$
- Trigonometrischer Pythagoras: $\sin^2(\varphi) + \cos^2(\varphi) = 1$ für alle $\varphi \in \mathbb{R}$.

Additionstheoreme

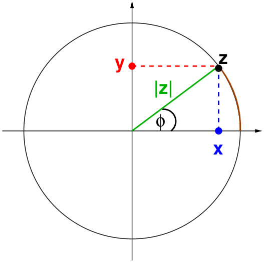
Für alle $\varphi, \psi \in \mathbb{R}$ gelten:

- $\sin(\varphi + \psi) = \sin(\varphi)\cos(\psi) + \cos(\varphi)\sin(\psi)$,
- $\cos(\varphi + \psi) = \cos(\varphi)\cos(\psi) - \sin(\varphi)\sin(\psi)$.

Trigonometrische Darstellung komplexer Zahlen

Eine komplexe Zahl $0 \neq z = x + \mathrm{i}\, y, x, y \in \mathbb{R}$ lässt sich nun schreiben als

$$\begin{aligned} z =& x + \mathrm{i}\, y \\ &= |z| \, \frac{x}{|z|} + \mathrm{i}\, |z| \, \frac{y}{|z|} \\ &= |z| \left(\frac{x}{|z|} + \mathrm{i}\, \frac{y}{|z|} \right) \\ &= |z| \left(\cos(\varphi) + \mathrm{i} \sin(\varphi) \right), \end{aligned}$$



wobei $\varphi \in \mathbb{R}$ bis auf Vielfache von 2π festgelegt ist. Oft fordert man $\varphi \in [0, 2\pi)$, um Eindeutigkeit zu erhalten.

Polardarstellung komplexer Zahlen

Definition

Für $\varphi \in \mathbb{R}$ definiere

$$e^{\mathrm{i}\varphi} := \cos(\varphi) + \mathrm{i}\sin(\varphi).$$

Bemerkung

Jedes $z \in \mathbb{C}$ besitzt eine Darstellung (die so genannte „Polardarstellung“) der Form

$$\boxed{z = re^{\mathrm{i}\varphi}} \qquad \text{mit } r \in [0, \infty) \text{ und } \varphi \in \mathbb{R}.$$

Dabei ist $r = |z|$.
Falls $z \neq 0$, dann wird φ als *ein* Argument von z bezeichnet und ist bis auf Addition von $2k\pi$, $k \in \mathbb{Z}$, eindeutig bestimmt.

Beispiele zur Polardarstellung

- $\mathrm{i} = 1 \cdot e^{\mathrm{i}\,\pi/2} \quad (= \underbrace{\cos(\pi/2)}_{=0} + \mathrm{i}\,\underbrace{\sin(\pi/2)}_{=1})$
- $-1 = 1 \cdot e^{\mathrm{i}\,\pi} \quad (= \underbrace{\cos(\pi)}_{=-1} + \mathrm{i}\,\underbrace{\sin(\pi)}_{=0})$

Umrechnung: Polardarstellung $\to$ kartesische Form

Umrechnung von Polardarstellung in kartesische Form

Sei $z = re^{\mathrm{i}\varphi} \in \mathbb{C}$, wobei $r \in [0, \infty), \varphi \in \mathbb{R}$.

1.) $x = r\cos(\varphi)$

2.) $y = r\sin(\varphi)$

Kartesische Form von z: $\quad z = x + y\,\mathrm{i}$.

Umrechnung: kartesische Form $\rightarrow$ Polardarstellung

Umrechnung von kartesischer Form in Polardarstellung

Sei $z = x + y\,\mathrm{i} \in \mathbb{C} \setminus \{0\}$, wobei $x, y \in \mathbb{R}$.

1.) $r = |z| = \sqrt{x^2 + y^2}$

2.) $\varphi = \begin{cases} \arccos \frac{x}{|z|}, & \text{falls } y \geq 0 \\ 2\pi - \arccos \frac{x}{|z|}, & \text{falls } y < 0 \end{cases}$

Polardarstellung von z: $\quad z = re^{\mathrm{i}\,\varphi}$

Multiplikation komplexer Zahlen

Satz

Seien $z, w \in \mathbb{C}$ mit Polardarstellungen

$$z = r\,e^{\mathrm{i}\,\varphi}, w = s\,e^{\mathrm{i}\,\psi}, \qquad \text{wobei } r, s \in [0,\infty), \varphi, \psi \in \mathbb{R}.$$

Dann ist

$$z\,w = r\,s\,e^{\mathrm{i}(\varphi+\psi)}.$$

Bemerkung

Bei der Multiplikation komplexer Zahlen werden die Beträge multipliziert und die Argumente/Winkel addiert.

Beweis des Satzes.

$$\begin{aligned} z\,w =& r\,(\cos(\varphi) + \mathrm{i}\sin(\varphi))\,s\,(\cos(\psi) + \mathrm{i}\sin(\psi)) \\ =& rs(\underbrace{\cos(\varphi)\cos(\psi) - \sin(\varphi)\sin(\psi)}_{\overset{\text{Add.thm.}}{=}\cos(\varphi+\psi)} + \mathrm{i}(\underbrace{\sin(\varphi)\cos(\psi) + \cos(\varphi)\sin(\psi)}_{\overset{\text{Add.thm.}}{=}\sin(\varphi+\psi)})) \\ =& r\,s\,(\cos(\varphi+\psi) + \mathrm{i}\sin(\varphi+\psi)) = r\,s\,e^{\mathrm{i}(\varphi+\psi)} \end{aligned}$$

□

Algebraische Grundlagen der Informatik

SoSe 2024

KAPITEL I: Komplexe Zahlen

3. Komplexe Wurzeln

Dozentin: Prof. Dr. Agnes Radl

Email: agnes.radl@informatik.hs-fulda.de

Lösungen der Gleichung $z^n = w$

Problem

Für $w \in \mathbb{C} \setminus \{0\}$ und $n \in \mathbb{N}$, $n \geq 1$, finde alle $z \in \mathbb{C}$ mit

$$\boxed{z^n = w}.$$

Lösungen der Gleichung $z^n = w$

Seien $n \in \mathbb{N}, n \geq 1$, $r > 0$, $\varphi \in \mathbb{R}$ und $w = r \cdot e^{i\varphi}$. Dann gibt es n verschiedene komplexe Lösungen von

$$z^n = w,$$

nämlich

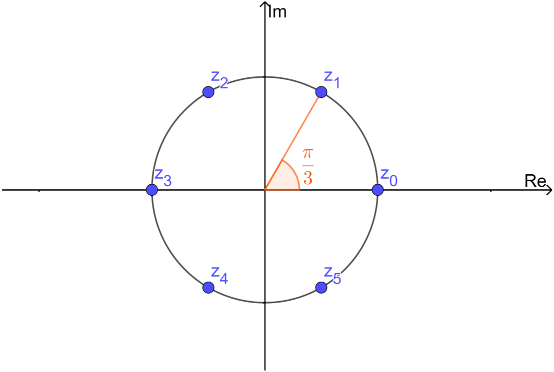
$$z_k = \sqrt[n]{r} e^{\mathrm{i}\left(\frac{\varphi}{n} + \frac{2k\pi}{n}\right)}, \quad k = 0, \ldots, n-1.$$

Einheitswurzeln

Speziell für $w = 1 = 1 \cdot e^{\mathrm{i}\cdot 0}$ erhält man die n-ten Einheitswurzeln

$$z_k = e^{\mathrm{i}\,\frac{2k\pi}{n}}, \quad k = 0, \ldots, n-1.$$

Beispiel: $(n = 6)$



$z_0 = 1, \quad z_1 = e^{\mathrm{i}\,\frac{\pi}{3}}, \quad z_2 = e^{\mathrm{i}\,\frac{2\pi}{3}}, \quad z_3 = -1, \quad z_4 = e^{\mathrm{i}\,\frac{4\pi}{3}}, \quad z_5 = e^{\mathrm{i}\,\frac{5\pi}{3}}$

Algebraische Grundlagen der Informatik

SoSe 2024

KAPITEL II: Relationen und algebraische Strukturen

1. Relationen

Dozentin: Prof. Dr. Agnes Radl

Email: agnes.radl@informatik.hs-fulda.de

Erinnerung (WiSe 2023/2024): Binäre Relationen

Erinnerung: Sind A und B Mengen und $R \subseteq A \times B$, so bezeichnet man R als binäre oder zweistellige Relation zwischen A und B.

Definition

Eine binäre Relation $R \subseteq A \times B$ heißt

- linkstotal, falls für alle $x \in A$ ein $y \in B$ existiert mit $(x, y) \in R$.
- rechtstotal, falls für alle $y \in B$ ein $x \in A$ existiert mit $(x, y) \in R$.
- linkseindeutig, falls für alle $x_1, x_2 \in A$ und für alle $y \in B$ aus $(x_1, y), (x_2, y) \in R$ folgt, dass $x_1 = x_2$.
- rechtseindeutig, falls für alle $x \in A$ und für alle $y_1, y_2 \in B$ aus $(x, y_1), (x, y_2) \in R$ folgt, dass $y_1 = y_2$.

Erinnerung (WiSe 2023/2024): Funktionen

Definition

Seien A und B Mengen. Eine Relation $R \subseteq A \times B$ ist eine Abbildung oder Funktion, falls sie

- linkstotal

und

- rechtseindeutig

ist.

Bemerkung

Das heißt, *jedem* Element in A wird *genau ein* Element in B zugeordnet.

weitere Sprechweisen

Bemerkung

- Eine partielle Funktion ist eine rechtseindeutige (und im Allgmeinen nicht linkstotale) Relation $R \subseteq A \times B$.
- Die Umkehrrelation einer Relation $R \subseteq A \times B$ ist die Relation

$$R^{-1} = \{(y, x) \in B \times A : (x, y) \in R\}.$$

Ist R eine bijektive Funktion, so ist R^{-1} gerade die Umkehrfunktion.

Relationen auf *einer* Menge

Definition

Sei M eine Menge. Eine Relation R auf M ist eine Teilmenge von $M \times M$, also $R \subseteq M \times M$.

Bemerkung

Andere Schreibweisen für „$(x, y) \in R$“ sind zum Beispiel:

- $x \, R \, y$,
- $x \sim_R y$,
- $x \sim y$.

Andere Schreibweisen für „$(x, y) \notin R$“ sind zum Beispiel:

- $x \not R \, y$,
- $x \not\sim_R y$,
- $x \not\sim y$.

Beispiele

(i) $M := \{2, 4, 5, 8\}, \quad R := \{(2, 2), (2, 4), (4, 2), (5, 8)\}$

(ii) $M := \mathbb{N}, \quad R_{\leq} := \{(x, y) \in M \times M : x \leq y\}$

(iii) $M := \mathbb{N}, \quad R_{<} := \{(x, y) \in M \times M : x < y\}$

(iv) $M := \mathbb{Z}, \quad R_3 := \{(x, y) \in M \times M : 3 \text{ teilt } y - x \text{ ohne Rest}\}$

(v) $M := \mathbb{N} \times \mathbb{N}, \quad R := \{((k, l), (m, n)) \in M \times M : k - l = m - n\}$

(vi) $\emptyset \neq K$ Menge, $M := \mathbb{P}(K)$, $R := \{(X, Y) \in M \times M : X \subseteq Y\}$

Eigenschaften von Relationen

Definition

Eine Relation R auf einer Menge M heißt

- reflexiv, falls für alle $x \in M$ gilt: $x \sim_R x$.
- irreflexiv, falls für alle $x \in M$ gilt: $x \not\sim_R x$.
- symmetrisch, falls für alle $x, y \in M$ gilt: Wenn $x \sim_R y$ gilt, dann gilt auch $y \sim_R x$.
- asymmetrisch, falls für alle $x, y \in M$ gilt: Aus $x \sim_R y$ folgt $y \not\sim_R x$.
- transitiv, falls für alle $x, y, z \in M$ gilt: Wenn $x \sim_R y$ und $y \sim_R z$ gelten, dann gilt auch $x \sim_R z$.
- antisymmetrisch, falls für alle $x, y \in M$ gilt: Aus $x \sim_R y$ und $y \sim_R x$ folgt $x = y$.

Beispiel von Seite 27

(i) $M := \{2, 4, 5, 8\}, \quad R := \{(2,2), (2,4), (4,2), (5,8)\}$

(ii) $M := \mathbb{N}, \quad R_{\leq} := \{(x, y) \in M \times M : x \leq y\}$

(iii) $M := \mathbb{N}, \quad R_{<} := \{(x, y) \in M \times M : x < y\}$

(iv) $M := \mathbb{Z}, \quad R_3 := \{(x, y) \in M \times M : 3 \text{ teilt } y - x \text{ ohne Rest}\}$

(v) $M := \mathbb{N} \times \mathbb{N}, \quad R := \{((k, l), (m, n)) \in M \times M : k - l = m - n\}$

(vi) $\emptyset \neq K$ Menge, $M := \mathbb{P}(K)$, $R := \{(X, Y) \in M \times M : X \subseteq Y\}$

	refl.	**irrefl.**	**symm.**	**asymm.**	**trans.**	**antisymm.**
(i)	–	–	–	–	–	–
(ii)	✓	–	–	–	✓	✓
(iii)	–	✓	–	✓	✓	✓
(iv)	✓	–	✓	–	✓	–
(v)	✓	–	✓	–	✓	–
(vi)	✓	–	–	–	✓	✓

Ordnungs- und Äquivalenzrelationen

Definition

Sei M eine Menge. $R \subseteq M \times M$ ist eine

(a) Ordungsrelation, falls R reflexiv, transitiv und antisymmetrisch ist.

Sind zwei beliebige Elemente $x, y \in M$ immer vergleichbar, das heißt, gilt für beliebige Elemente $x, y \in M$ immer $x \sim_R y$ oder $y \sim_R x$, so spricht man von einer totalen Ordnung. Ist dies nicht unbedingt der Fall, so spricht man von einer partiellen Ordnung.

(b) strikte Ordnungsrelation, falls R transitiv und asymmetrisch ist.

(c) Äquivalenzrelation, falls R reflexiv, symmetrisch und transitiv ist.

Beispiel von Seite 27

(i) $M := \{2, 4, 5, 8\}, \quad R := \{(2, 2), (2, 4), (4, 2), (5, 8)\}$

(ii) $M := \mathbb{N}, \quad R_{\leq} := \{(x, y) \in M \times M : x \leq y\}$

(iii) $M := \mathbb{N}, \quad R_{<} := \{(x, y) \in M \times M : x < y\}$

(iv) $M := \mathbb{Z}, \quad R_3 := \{(x, y) \in M \times M : 3 \text{ teilt } y - x \text{ ohne Rest}\}$

(v) $M := \mathbb{N} \times \mathbb{N}, \quad R := \{((k, l), (m, n)) \in M \times M : k + n = m + l\}$

(vi) $\emptyset \neq K$ Menge, $M := \mathbb{P}(K)$, $R := \{(X, Y) \in M \times M : X \subseteq Y\}$

Bemerkung

- (ii) und (vi) sind Ordnungsrelationen.
- (iii) ist eine strikte Ordnungsrelation.
- (iv) und (v) sind Äquivalenzrelationen.

Äquivalenzklassen

Definition

- Ist R eine Äquivalenzrelation auf der Menge M und ist $x \in M$, so ist die Menge

$$[x]_R := \{y \in M : x \sim_R y\}$$

die Äquivalenzklasse von x (bzgl. R).

Andere Notation: $[x]$ statt $[x]_R$.

- Ein Element aus $[x]$ heißt Vertreter dieser Äquivalenzklasse.
- $M/{\sim_R}$, beziehungsweise nur $M/{\sim}$, bezeichnet die Menge der Äquivalenzklassen bezüglich R, also

$$M/{\sim_R} = \{[x]_R : x \in M\}.$$

Zu Beispiel (iv) von Seite 27

Für $R_3 \subseteq \mathbb{Z} \times \mathbb{Z}$ mit

$$x \sim_{R_3} y, \text{ falls } 3|(y-x)$$

ist

- $[0] = \{y \in \mathbb{Z} : 0 \sim_{R_3} y\} = \{y \in \mathbb{Z} : 3|y\}$
  $= \{0, 3, -3, 6, -6, \dots\} = \{3z : z \in \mathbb{Z}\}$,
- $[1] = \{y \in \mathbb{Z} : 1 \sim_{R_3} y\} = \{y \in \mathbb{Z} : 3|(y-1)\}$
  $= \{1, 4, 7, \dots\} \cup \{-2, -5, -8, \dots\} = \{3z + 1 : z \in \mathbb{Z}\}$,
- $[2] = \{y \in \mathbb{Z} : 2 \sim_{R_3} y\} = \{y \in \mathbb{Z} : 3|(y-2)\}$
  $= \{2, 5, 8, \dots\} \cup \{-1, -4, -7, \dots\} = \{3z + 2 : z \in \mathbb{Z}\}$.

Desweiteren ist $[3] = [0], [4] = [1], [5] = [2], \dots$ und $[-1] = [2], [-2] = [1], [-3] = [0], \dots$. Wir haben also

$$\boxed{\mathbb{Z}/{\sim_{R_3}} = \{[0], [1], [2]\}.}$$

Restklassen

Allgemein:

Falls für $n \in \mathbb{N}, n \geq 2$, die Relation $R_n \subseteq \mathbb{Z} \times \mathbb{Z}$ definiert ist durch

$$x \sim_{R_n} y, \quad \text{falls} \quad n|(y-x),$$

so ist

$$\mathbb{Z}/\sim_{R_n} = \{[0], [1], [2], \ldots, [n-1]\} =: \mathbb{Z}_n,$$

wobei

$$[k] = \{k + nz : z \in \mathbb{Z}\}.$$

$[k]$ heißt Restklasse modulo n, da alle darin enthaltenen Zahlen bei Division durch n den gleichen Rest lassen.

Zu Beispiel (v) von Seite 27

Sei $M := \mathbb{N} \times \mathbb{N}$, wobei $(k, l) \sim (m, n)$ falls $k - l = m - n$.

Beobachtung

- In einer Äquivalenzklasse sind genau die Zahlenpaare, deren Differenzen gleich sind.
- Die Abbildung

  $$f : \mathbb{N} \times \mathbb{N}/\sim \to \mathbb{Z}, \quad [(n, m)] \mapsto n - m,$$

  ist also bijektiv. Insbesondere gilt für $n \in \mathbb{N}$

  $$f([(n + 1, 1)]) = n, \quad f([(1, n + 1)]) = -n.$$

Partition einer Menge durch Äquivalenzrelation

Satz

Sei R eine Äquivalenzrelation auf M und $x_1, x_2 \in M$. Dann gelten:

(a) Ist $x_1 \sim_R x_2$, so ist $[x_1]_R = [x_2]_R$.

(b) Ist $x_1 \not\sim_R x_2$, so ist $[x_1]_R \cap [x_2]_R = \emptyset$.

(c) $\bigcup_{x \in M} [x]_R = M$

Verknüpfung von Relationen

Definition

- Sind A, B, C Mengen und $R \subseteq A \times B$, $S \subseteq B \times C$, so ist die Verkettung oder Verknüpfung der Relationen S und R gegeben durch

  $$S \circ R = \{(a, c) \in A \times C : \exists b \in B \text{ so dass } (a, b) \in R \text{ und } (b, c) \in S\}.$$

- Ist R eine Relation auf einer Menge M, so definiert man

  $$R^{n+1} = R \circ R^n, \quad n \geq 1.$$

Reflexive, transitive und symmetrische Hülle einer Relation

Definition

Sei M eine Menge und $R \subseteq M \times M$ eine Relation.

- Die reflexive Hülle von R ist
$$R \cup \{(x, x) : x \in M\}.$$
- Die symmetrische Hülle von R ist
$$R \cup R^{-1}.$$
- Die transitive Hülle von R ist
$$\bigcup_{n \geq 1} R^n.$$

Aus einer Relation eine Äquivalenzrelation gewinnen

Bemerkung

Ist R eine Relation auf einer Menge M und bildet man zunächst die

- reflexive Hülle R_r von R,

dann die

- symmetrische Hülle $(R_r)_s$ von R_r

und schließlich die

- transitive Hülle $((R_r)_s)_t$ von $(R_r)_s$,

so erhält man die kleinste Äquivalenzrelation, die R enthält.

Algebraische Grundlagen der Informatik

SoSe 2024

KAPITEL II: Relationen und algebraische Strukturen

2. Erinnerung: Euklidischer Algorithmus

Dozentin: Prof. Dr. Agnes Radl

Email: agnes.radl@informatik.hs-fulda.de

Teilbarkeit

Definition

1. $a \in \mathbb{Z}$ heißt durch $b \in \mathbb{Z}$ teilbar, beziehungsweise b teilt a, falls es ein $z \in \mathbb{Z}$ gibt mit $a = z \cdot b$.

   Notation: $\begin{cases} b \mid a, & \text{falls } a \text{ durch } b \text{ teilbar,} \\ b \nmid a, & \text{sonst.} \end{cases}$

2. Seien $a, b \in \mathbb{Z}$. Es sind a und b kongruent modulo $m \in \mathbb{N}^*$, wenn gilt: $m|(b-a)$.

   Notation: $a \equiv b \bmod m$ oder $a \equiv b \pmod{m}$.

Division mit Rest

Bemerkung

- Sind $a \in \mathbb{Z}$ und $m \in \mathbb{N}^*$, so gibt es eindeutig bestimmte Zahlen $q \in \mathbb{Z}$ und $r \in \{0, \ldots, m-1\}$, so dass

  $$a = q \cdot m + r.$$

  Dabei ist r der Rest.

  Notation: $r = a \bmod m$
- Beachten Sie, dass der Rest nicht negativ ist!
- Falls $b \in \mathbb{Z}$ und $a \equiv b \bmod m$ gilt, so lassen a und b bei Division durch m den gleichen Rest r:

  $$r = a \bmod m = b \bmod m.$$

größter gemeinsamer Teiler

Definition

Seien $a, b \in \mathbb{Z}$ und a und b nicht beide $= 0$.

(a) Der größte gemeinsame Teiler $\mathrm{ggT}(a, b)$ von a und b ist die größte Zahl $k \in \mathbb{N}$ mit $k|a$ und $k|b$.

(b) Ist $\mathrm{ggT}(a, b) = 1$, so heißen a und b teilerfremd.

Bemerkung

- $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, a)$
- $\mathrm{ggT}(a, b) = \mathrm{ggT}(|a|, |b|)$

Euklidischer Algorithmus

Satz

Seien $a, b \in \mathbb{Z} \setminus \{0\}$. Folgendes Verfahren endet nach einer endlichen Anzahl von Schritten und liefert $\mathrm{ggT}(a, b)$:

Schritt 0:

$$\begin{cases} a_0 := |a|, \quad a_1 := |b|, & \text{falls } |a| > |b|; \\ a_0 := |b|, \quad a_1 := |a|, & \text{sonst.} \end{cases}$$

Schritt $k, k \geq 1$:

(„Führe so lange Division mit Rest aus, bis Rest 0 auftaucht.“)

- Bestimme $q_{k-1} \in \mathbb{N}, a_{k+1} \in \mathbb{N}$ mit $0 \leq a_k$, so dass $a_{k-1} = q_{k-1} a_k + a_{k+1}$.
- Ist $a_{k+1} = 0$, dann ist $\mathrm{ggT}(a, b) = a_k$ und das Verfahren endet.
- Ist $a_{k+1} \neq 0$, dann weiter mit Schritt $k + 1$.

Darstellung des ggT

Korollar

Seien $a, b \in \mathbb{Z} \setminus \{0\}$. Dann gibt es $s, t \in \mathbb{Z}$, so dass

$$\mathrm{ggT}(a, b) = sa + tb.$$

Algebraische Grundlagen der Informatik

SoSe 2024

KAPITEL II: Relationen und algebraische Strukturen

3. Gruppen, Ringe, Körper

Dozentin: Prof. Dr. Agnes Radl

Email: agnes.radl@informatik.hs-fulda.de

Verknüpfungen

Definition

Eine Abbildung $*: M \times M \to M$ heißt Verknüpfung auf M.

Notation: Statt $*((x, y))$ schreibt man $x * y$. Zum Beispiel $3 + 7$ statt $+((3, 7))$.

Beispiel

- „$+$“ und „$\cdot$“ sind Verknüpfungen auf $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.
- „$-$“ ist eine Verknüpfung auf $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, nicht aber auf $\mathbb{N}$.

Gruppen

Definition

Sei $G \neq \emptyset$ und $* : G \times G \to G$ eine Verknüpfung auf G. Dann heißt $(G, *)$ oder kurz G Gruppe, falls

1. $*$ assoziativ ist, das heißt für alle $a, b, c \in G$ gilt $a * (b * c) = (a * b) * c$; ($\to$ Klammern können weggelassen werden)
2. es ein Neutralelement $e \in G$ gibt, das heißt, es existiert ein $e \in G$, so dass für alle $a \in G$ gilt: $a * e = e * a = a$;
3. jedes $a \in G$ ein inverses Element besitzt, das heißt, zu jedem $a \in G$ existiert ein $b \in G$, so dass $a * b = b * a = e$. Notation für das Inverse: a^{-1} oder $-a$.

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

Beispiele

- $(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+)$, $(\mathbb{C},+)$ sind Gruppen.
- $(\mathbb{N},\cdot),(\mathbb{Z},\cdot)$ sind keine Gruppen.
- $(\mathbb{Q}\setminus\{0\},\cdot),(\mathbb{R}\setminus\{0\},\cdot),(\mathbb{C}\setminus\{0\},\cdot)$ sind Gruppen.
- X eine beliebige nicht-leere Menge und

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

Dann ist $(G,\circ)$ eine Gruppe.

Ist $n \in \mathbb{N}^*$, $X := \{1,\dots,n\}$ und

$$S_n := \{f : X \to X \mid f \text{ bijektiv}\},$$

so heißt die Gruppe $(S_n,\circ)$ symmetrische Gruppe. Die Elemente dieser Gruppe nennt man auch Permutationen.

Eigenschaften von Gruppen

Satz

Sei $(G, *)$ eine Gruppe. Dann gelten:

(a) Das Neutralelement ist eindeutig.

(b) Zu jedem $a \in G$ gibt es genau ein inverses Element.

(c) Seien $a, x, y \in G$. Dann gelten folgende Kürzungsregeln:

- $a * x = a * y \quad \Rightarrow \quad x = y$,
- $x * a = y * a \quad \Rightarrow \quad x = y$.

Kongruenzrelationen

Definition

Sei M eine Menge, auf der eine Verknüpfung „$*$“ definiert ist, und sei R eine Äquivalenzrelation auf M. Gilt für alle $a_1, a_2, b_1, b_2 \in M$ mit $a_1 \sim a_2$ und $b_1 \sim b_2$ auch

$$a_1 * b_1 \sim a_2 * b_2,$$

so bezeichnet man R als Kongruenzrelation.

Beispiel

Die Teilbarkeitsrelation R_n (von Seite 34) ist eine Kongruenzrelation auf $\mathbb{Z}$ bezüglich „$+$“ und „$\cdot$“.

Addition und Multiplikation mit Restklassen

Erinnerung: Für $n \in \mathbb{N}, n \geq 2$, ist

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

wobei $[k] = \{k + nz : z \in \mathbb{Z}\}$.

Definiere Verknüpfungen „$+$“ und „$\cdot$“ auf $\mathbb{Z}_n$ durch

- $[a] + [b] := [a + b]$,
- $[a] \cdot [b] := [a \cdot b]$.

Bemerkung

Die Verknüpfungen sind „wohldefiniert“, das heißt unabhängig von dem jeweiligen Vertreter der Äquivalenzklasse, da die Teilbarkeitsrelation R_n (von Seite 34) eine Kongruenzrelation auf $\mathbb{Z}$ bezüglich „$+$“ und „$\cdot$“ ist.

Verknüpfungstafeln von $(\mathbb{Z}_4, +)$ und $(\mathbb{Z}_4, \cdot)$

$+$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

$\cdot$	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

Beobachtung

- $(\mathbb{Z}_4, +)$ ist eine (kommutative) Gruppe. (Neutralelement: [0], Inverses zu $[a]$: $[-a]$)
- $(\mathbb{Z}_4, \cdot)$ ist keine Gruppe.
- Die invertierbaren Elemente in $(\mathbb{Z}_4, \cdot)$ sind [1] und [3].
- $(\{[1], [3]\}, \cdot)$ ist eine Gruppe, wobei die Verknüpfungstafel gegeben ist durch

$\cdot$	[1]	[3]
[1]	[1]	[3]
[3]	[3]	[1]

Gruppeneigenschaft von $(\mathbb{Z}_n, +)$

Beobachtung

Allgemein gilt:

Für jedes $n \in \mathbb{N}, n \geq 2$, ist $(\mathbb{Z}_n, +)$ eine kommutative Gruppe.

Dabei ist jeweils

- $[0]$ das Neutralelement.
- $[-k]$ das Inverse zu $[k]$ für $k \in \mathbb{Z}$.

Invertierbarkeit in $(\mathbb{Z}_n, \cdot)$

Satz

Sei $n \in \mathbb{N}, n \geq 2$. Dann ist $[k] \in \mathbb{Z}_n$ genau dann invertierbar bezüglich „$\cdot$“, wenn $\mathrm{ggT}(k, n) = 1$.

Prime Restklassengruppe modulo n

Definition

Für $n \in \mathbb{N}$, $n \geq 2$, heißt

$$\mathbb{Z}_n^* := \{[k] \in \mathbb{Z}_n : \text{ggT}(k, n) = 1\}$$

prime Restklassengruppe modulo n.

Beispiel

- $\mathbb{Z}_4^* = \{[1], [3]\}$
- Ist p eine Primzahl, so ist $\mathbb{Z}_p^* = \{[1], [2], \ldots, [p-1]\}$.

Satz

Sei $n \in \mathbb{N}, n \geq 2$. Dann ist $(\mathbb{Z}_n^*, \cdot)$ eine kommutative Gruppe.

Ringe

Definition

Sei $R \neq \emptyset$ eine Menge, auf der zwei Verknüpfungen $+ : R \times R \to R$ und $\cdot : R \times R \to R$ definiert sind. Dann heißt $(R, +, \cdot)$ oder kurz R Ring, falls

(i) $(R, +)$ eine abelsche Gruppe ist,

(ii) für alle $a, b, c \in R$ gilt:

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \text{(Assoziativgesetz)},$$

(iii) für alle $a, b, c \in R$ gilt:
$a \cdot (b + c) = a \cdot b + a \cdot c$ und $(a + b) \cdot c = a \cdot c + b \cdot c$
(Distributivgesetze).

Ist die Verknüpfung „$\cdot$“ kommutativ, so heißt der Ring kommutativ. Gibt es zusätzlich noch ein neutrales Element bezüglich „$\cdot$“, also ein Element $1 \in R$ mit $a \cdot 1 = 1 \cdot a = 1$ für alle $a \in R$, so ist $(R, +, \cdot)$ ein kommutativer Ring mit Eins.

Beispiele

- $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sind kommutative Ringe mit Eins.
- $(\mathbb{Z}_n, +, \cdot)$ ist für $n \in \mathbb{N}, n \geq 2$, ein kommutativer Ring mit Eins.
- Später lernen wir noch den Ring der $n \times n$-Matrizen kennen.

Eigenschaften von Ringen

Satz

Sei $(R, +, \cdot)$ ein Ring, wobei 0 das Neutralelement bezüglich „$+$“ bezeichnet.

(a) Für alle $a \in R$ gilt

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

(b) Ist R ein Ring mit 1, $a \in R$ invertierbar und $a \cdot b = 0$ oder $b \cdot a = 0$, dann ist $b = 0$.

Bemerkung

Ein Element $a \in R \setminus \{0\}$ ist ein Nullteiler, falls ein $b \in R \setminus \{0\}$ existiert mit $a \cdot b = 0$ oder $b \cdot a = 0$. Teil (b) des Satzes besagt, dass invertierbare Elemente eines Rings mit 1 keine Nullteiler sein können.

Körper

Definition

Sei $K \neq \emptyset$ eine Menge, auf der zwei Verknüpfungen $+ : K \times K \to K$ und $\cdot : K \times K \to K$ definiert sind. Dann heißt $(K, +, \cdot)$ oder kurz K Körper, falls

(i) $(K, +)$ eine abelsche Gruppe ist,

(ii) $(K \setminus \{0\}, \cdot)$ eine abelsche Gruppe ist und

(iii) für alle $a, b, c \in K$ gilt:
$a \cdot (b + c) = a \cdot b + a \cdot c$ und $(a + b) \cdot c = a \cdot c + b \cdot c$
(Distributivgesetze).

Bemerkung

Zumeist wird das Neutralelement bezüglich „$+$“ mit 0 bezeichnet und das Neutralelement bezüglich „$\cdot$“ mit 1.

Beispiele

- $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sind Körper.
- $(\mathbb{Z}, +, \cdot)$ ist kein Körper.
- $(\mathbb{Z}_p, +, \cdot)$, p Primzahl, ist ein Körper.
- $(\mathbb{Z}_n, +, \cdot)$ ist kein Körper, falls n keine Primzahl, (denn nicht alle Elemente besitzen Inverses bezüglich Multiplikation).
- Jeder Körper ist ein kommutativer Ring mit Eins, aber die Umkehrung gilt im Allgemeinen nicht.

  Beispiel: $(\mathbb{Z}, +, \cdot)$ ist kein Körper, jedoch ein kommutativer Ring mit Eins.

Eigenschaften von Körpern

Satz

Sei $(K, +, \cdot)$ ein Körper, wobei 0 das Neutralelement bezüglich „$+$" und 1 das Neutralelement bezüglich „$\cdot$" bezeichnet.

(a) Für alle $a \in K$ gilt $a \cdot 0 = 0 \cdot a = 0$.

(b) Aus $a, b \in K$, $a \cdot b = 0$ folgt $a = 0$ oder $b = 0$.
(„nullteilerfrei")

Anwendung: Prüfziffern

Aufbau ISBN-Nummer:

$$x_{10} - x_9 x_8 x_7 - x_6 x_5 x_4 x_3 x_2 - x_1,$$

wobei $x_2 \,..., x_{10} \in \{0, \dots, 9\}$, $x_1 \in \{0, \dots, 9, 10\}$.

x_1 ist die sogenannte Prüfziffer und wird so gewählt, dass

$$\sum_{k=1}^{10} k \cdot x_k \equiv 0 \mod 11,$$

das heißt, in $\mathbb{Z}_{11}$ gilt

$$\left[\sum_{k=1}^{10} k \cdot x_k\right] = [0] \quad \text{bzw.} \quad [x_1] = \left[-\sum_{k=2}^{10} k \cdot x_k\right].$$

Beispiel

ISBN-Nummer: 3-519-32079-?

Wir berechnen

$$\sum_{k=1}^{10} k \cdot x_k = 1 \cdot x_1 + 2 \cdot 9 + 3 \cdot 7 + \ldots + 10 \cdot 3 = 213 + x_1.$$

Für $x_1 = 7$ ist $\sum_{k=1}^{10} k \cdot x_k = 220$, und es gilt $220 \mod 11 = 0$.

Welche Fehler werden bei ISBN-Nummern erkannt?

Behauptung

Folgende Fehler werden immer erkannt:

- Eingabe genau einer falschen Ziffer.
- Vertauschung von genau zwei Ziffern.

Erstellung von Prüfziffernverfahren

- Sollen Ziffern zwischen 0 und 9 verwendet werden, so muss man in $\mathbb{Z}_n$, $n \geq 10$, arbeiten, um diese unterscheiden zu können.
- Die Prüfziffer $P(x_r \cdots x_2) \in \{0, \dots, n-1\}$ einer Ziffernfolge $x_r \cdots x_2$ mit $x_i \in \{0, \dots, n-1\}$ wird so berechnet, dass

$$[P(x_r \cdots x_2)] = \left[-\sum_{k=2}^{r} g_k x_k\right]$$

gilt, wobei $g_j \in \{0, \dots, n-1\}$ „Gewichte“ sind.

Erstellung von Prüfziffernverfahren – Einzelfehler

- Enthält $y_r \cdots y_2$ genau eine falsche Eingabe an Position l verglichen mit $x_r \cdots x_2$, so ist

$$[P(y_r \cdots y_2) - P(x_r \cdots x_2)] = [g_l] \underbrace{[y_l - x_l]}_{\neq [0]}.$$

  Ist $[g_l]$ invertierbar, so ist $[g_l]\,[y_l - x_l] \neq [0]$, und der Fehler wird erkannt.

- Um genau eine falsche Eingabe an Position l zu erkennen, wähle das Gewicht g_l also so, dass $[g_l]$ invertierbar in $\mathbb{Z}_n$ ist.

Erstellung von Prüfziffernverfahren – Vertauschungsfehler

- Enthält $y_r \cdots y_2$ genau eine Vertauschung von Positionen l und m verglichen mit $x_r \cdots x_2$, so ist

$$[P(y_r \cdots y_2) - P(x_r \cdots x_2)] = [g_l - g_m] \underbrace{[x_m - x_l]}_{\neq [0]}.$$

  Ist $[g_l]$ invertierbar, so ist $[g_l - g_m] [x_m - x_l] \neq [0]$, und der Fehler wird erkannt.

- Um einen Vertauschungsfehler von Positionen l und m zu erkennen, wähle die Gewichte g_l und g_m also so, dass $[g_l - g_m]$ invertierbar in $\mathbb{Z}_n$ ist.

Algebraische Grundlagen der Informatik

SoSe 2024

KAPITEL III: Lineare Gleichungssysteme

1. Lineare Gleichungssysteme

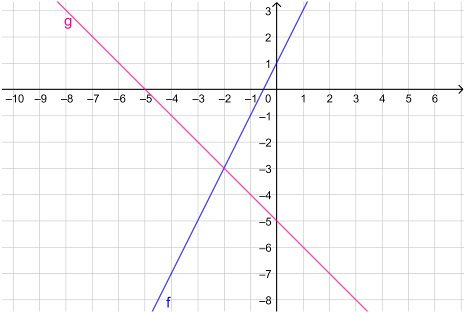
Dozentin: Prof. Dr. Agnes Radl

Email: agnes.radl@informatik.hs-fulda.de

Beispiel

Betrachten Sie die Geraden

$$f : \mathbb{R} \to \mathbb{R}, \quad f(t) := 2t + 1,$$
$$g : \mathbb{R} \to \mathbb{R}, \quad g(t) := -t - 5.$$



- Schneiden sich die Geraden?
- Wenn ja, wo?

Beispiel – Fortsetzung

Gesucht ist also ein Punkt (x, y), der

$$\begin{aligned} 2x + 1 &= y \qquad (i) \\ -x - 5 &= y \qquad (ii) \end{aligned}$$

erfüllt.
Man erhält also ein lineares Gleichungssystem mit zwei Gleichungen und zwei Unbekannten.

Beispiel Schnitt zweier Geraden

Erinnerung voriges Beispiel:

$$\begin{aligned} 2x+1 &= y \qquad (i) \\ -x-5 &= y \qquad (ii) \end{aligned}$$

Durch Umformen erhält man

$$\begin{aligned} \underbrace{2}_{a_{11}}\underbrace{x}_{x_1} + \underbrace{(-1)}_{a_{12}}\cdot\underbrace{y}_{x_2} &= \underbrace{-1}_{b_1} \qquad (i) \\ \underbrace{(-1)}_{a_{21}}\cdot\underbrace{x}_{x_1} + \underbrace{(-1)}_{a_{22}}\cdot\underbrace{y}_{x_2} &= \underbrace{5}_{b_2} \qquad (ii) \end{aligned}$$

Es ist also von der Form

$$\left.\begin{aligned} a_{11}x_1 + a_{12}x_2 &= b_1 \\ a_{21}x_1 + a_{22}x_2 &= b_2 \end{aligned}\right\}(G)$$

Lineare Gleichungssysteme

Definition

Ein reelles lineares Gleichungssystem (kurz: LGS) mit m Gleichungen und n Unbekannten hat die Form

$$\left.\begin{array}{ccccccc} a_{11}x_1 & + & \cdots & + & a_{1n}x_n & = & b_1 \\ \vdots & & & & & & \vdots \\ a_{m1}x_1 & + & \cdots & + & a_{mn}x_n & = & b_m \end{array}\right\} (G)$$

wobei $a_{ij} \in \mathbb{R}, i = 1, \ldots, m,\ j = 1, \ldots, n$, die Koeffizienten sind, $x_1, \ldots, x_n$ die Unbekannten und $b_i \in \mathbb{R}$, $i = 1, \ldots, m$ die „rechte Seite".

Bemerkung

Gesucht sind $x_1, \ldots, x_n \in \mathbb{R}$, so dass (G) erfüllt ist.

Bezeichnungen und Kurznotation bei LGS

- $\mathbb{R}^n := \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} : x_1, \ldots, x_n \in \mathbb{R} \right\} \quad (n \in \mathbb{N}^*)$
- $A := \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$ heißt Koeffizientenmatrix.
- Für das LGS (G) schreibt man kurz $\boxed{Ax = b}$, wobei A die Koeffizientenmatrix ist, $b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \in \mathbb{R}^m$ die rechte Seite enthält und in $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{R}^n$ die Unbekannten stehen.
- Ist $b_1 = \ldots = b_m = 0$, so heißt das LGS homogen.

Lineare Gleichungssysteme

Definition

- Die Lösungsmenge des LGS (G) ist

$$L(G) := \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{R}^n : \begin{array}{l} a_{k1}x_1 + \cdots + a_{kn}x_n = b_k \\ \text{für jedes } k \in \{1, \ldots, m\} \end{array} \right\}.$$

- $(A|b) := \left(\begin{array}{ccc|c} a_{11} & \cdots & a_{1n} & b_1 \\ \vdots & & \vdots & \vdots \\ a_{m1} & \cdots & a_{mn} & b_m \end{array}\right)$ heißt erweiterte Koeffizientenmatrix.
- Oft schreibt man dann $L(A|b)$ statt $L(G)$, um die Lösungsmenge zu bezeichnen.

Fragen

- Existieren Lösungen von (G)?
- Wenn ja, wie viele?
- Wie findet man die Lösungen?

Auffinden von Lösungen

Beobachtung

Folgende Umformungen an (G) ändern nichts an $L(G)$:

(Z_1) Vertauschen zweier Zeilen.

(Z_2) Multiplikation einer Zeile mit $\lambda \in \mathbb{R}, \lambda \neq 0$.

(Z_3) Addition eines Vielfachen einer Zeile zu einer *anderen* Zeile.

Idee

Forme (G) mit Hilfe der „elementaren Zeilenumformungen“ $(Z_1), (Z_2)$ und (Z_3) so lange um, bis die Lösungsmenge $L(G)$ ablesbar ist.

Bemerkung

Um Schreibarbeit zu sparen, führt man diese Umformungen nur an der erweiterten Koeffizientenmatrix $(A|b)$ durch, nicht an (G).

Zeilenstufenform einer Matrix

Definition

Eine Matrix ist in Zeilenstufenform, falls

- je tiefer die Zeile, desto weiter rechts der Zeilenkopf (d. h. erster Nicht-Nulleintrag der Zeile).

  (Damit sind automatisch unterhalb eines Zeilenkopfes nur Nullen - außer in der letzten Zeile.)

- Nullzeilen (falls vorhanden) ganz unten sind.

Bemerkung

Hat man die erweiterte Koeffizientenmatrix eines LGS in Zeilenstufenform überführt, so kann man daraus die Lösung ablesen.

Gauß[1]-Verfahren zum Auffinden von Lösungen

Betrachte die erweiterte Koeffizientenmatrix $(A|b)$ des LGS.

1. Besitzt die Koeffizientenmatrix „führende Nullspalten“, so streiche diese in Gedanken und wende das Verfahren auf das verkürzte System an.
2. Eintrag links oben muss $\neq 0$ sein. (Dies ist mit (Z_1) erreichbar.)
3. Mit (Z_3) sukzessive Nullspalte unterhalb des Eintrags links oben erzeugen.
4. Schritt 2. und 3. für verkürztes System (das heißt, oberste Zeile und „führende Nullspalten“ gestrichen) wiederholen usw. bis Matrix in Zeilenstufenform.

[1] Genaues Verfahren u. Begriffe in G. Fischer, *Lineare Algebra*, Abschnitt 0.4.

Gauß-Verfahren zum Auffinden von Lösungen

Ablesen der Lösungsmenge aus der Zeilenstufenform:

1. Freie Variablen[1] – falls vorhanden – umbenennen und das zur Zeilenstufenform gehörende LGS aufschreiben.
2. Gleichungen von unten nach oben der Reihe nach nach den gebundenen Variablen[1] auflösen und das Ergebnis jeweils in die darüber liegenden Gleichungen einsetzen.
3. Angabe der Lösungsmenge $L(A|b)$.

[1] „gebundene Variablen" gehören zu den Zeilenköpfen; die anderen Variablen sind „freie Variablen"

Rang einer Matrix

Definition

Sei A die Koeffizientenmatrix und $(A|b)$ die erweiterte Koeffizientenmatrix eines linearen Gleichungssystems. Angenommen, daraus ergibt sich durch Umformen die Matrix $(\tilde{A}|\tilde{b})$ in Zeilenstufenform. Dann ist daran der Rang von A bzw. $(A|b)$ ablesbar:

- $\text{Rang}(A) := \#$ Nicht-Nullzeilen in $\tilde{A}$
- $\text{Rang}(A|b) := \#$ Nicht-Nullzeilen in $(\tilde{A}|\tilde{b})$

Bemerkung

Es gilt für ein LGS mit n Unbekannten:

- $\#$ gebundene Variablen $= \text{Rang}(A)$
- $\#$ freie Variablen $= n - \text{Rang}(A)$

Lösungen von LGS mit n Unbekannten

Beobachtung

- LGS lösbar $\quad\Leftrightarrow\quad \text{Rang}(A) = \text{Rang}(A|b)$.
- Falls das LGS lösbar ist, dann gelten:
  - $\text{Rang}(A) = n \quad\Rightarrow\quad$ genau eine Lösung vorhanden
  - $\text{Rang}(A) < n \quad\Rightarrow\quad$ unendlich viele Lösungen vorhanden

Normierte Zeilenstufenform

Definition

Eine Matrix ist in normierter Zeilenstufenform, falls sie

- in Zeilenstufenform ist,
- jeder Zeilenkopf (d.h. erster Nicht-Nulleintrag) gleich 1 ist und
- über jedem Zeilenkopf (außer in Zeile 1) stehen nur Nullen.

Bemerkung

Jede Matrix A kann in normierte Zeilenstufenform gebracht werden durch:

1. Umformen von A in Zeilenstufenform.
2. Division der nicht-Nullzeilen durch den jeweiligen Zeilenkopf ($\rightarrow$ Zeilenköpfe werden zu 1.)
3. Für jeden Zeilenkopf: Subtrahiere von den *darüberliegenden* Zeilen jeweils ein geeignetes Vielfaches der Zeile mit dem betrachteten Zeilenkopf, so dass darüber nur noch Nullen stehen.

Algebraische Grundlagen der Informatik

SoSe 2024

KAPITEL III: Lineare Gleichungssysteme

2. Determinanten

Dozentin: Prof. Dr. Agnes Radl

Email: `agnes.radl@informatik.hs-fulda.de`

LGS mit „quadratischer“ Koeffizientenmatrix

In diesem Abschnitt betrachten wir lineare Gleichungssysteme mit genauso vielen Gleichungen wie Unbekannten, also

- n Gleichungen und
- n Unbekannten.

Die Koeffizientenmatrix ist dann „quadratisch“, das heißt, sie besitzt genauso viele Zeilen wie Spalten, also

- n Zeilen und
- n Spalten.

Eindeutige Lösbarkeit bei 1 Gl. und 1 Unb.

Frage:
Wie erkennt man an der Koeffizientenmatrix, ob ein LGS mit n Gleichungen und n Unbekannten eindeutig lösbar ist, das heißt, ob $|L(G)| = 1$ gilt?

Beispiel ($n = 1$)

$$\boxed{a_{11}x_1 = b_1 \quad (G)}$$

- $a_{11} \neq 0 \quad \Rightarrow \quad L(G) = \left\{ \frac{b_1}{a_{11}} \right\}$
- $a_{11} = 0, b_1 \neq 0 \quad \Rightarrow \quad L(G) = \emptyset$
- $a_{11} = 0, b_1 = 0 \quad \Rightarrow \quad L(G) = \mathbb{R}$ (unendlich viele Lösungen)

Fazit

$$\boxed{|L(G)| = 1 \quad \Leftrightarrow \quad a_{11} \neq 0}$$

Eindeutige Lösbarkeit von LGS, 2 Gl. und 2 Unb.

Beispiel $(n = 2)$

$$\boxed{\left.\begin{array}{ccccc} a_{11}x_1 & + & a_{12}x_2 & = & b_1 \\ a_{21}x_1 & + & a_{22}x_2 & = & b_2 \end{array}\right\} (G)}$$

- $a_{11} \neq 0$:
$$\left(\begin{array}{cc|c} a_{11} & a_{12} & b_1 \\ a_{21} & a_{22} & b_2 \end{array}\right) \xrightarrow{(ii)-\frac{a_{21}}{a_{11}}(i)} \left(\begin{array}{cc|c} a_{11} & a_{12} & b_1 \\ 0 & a_{22} - \frac{a_{21}}{a_{11}}a_{12} & b_2 - \frac{a_{21}}{a_{11}}b_1 \end{array}\right)$$

$$\begin{aligned} |L(G)| = 1 \quad &\Leftrightarrow \quad \mathrm{Rang}(A) = 2 \quad \Leftrightarrow \quad a_{22} - \frac{a_{21}}{a_{11}}a_{12} \neq 0 \\ &\Leftrightarrow \quad a_{11}a_{22} - a_{21}a_{12} \neq 0 \end{aligned}$$

- Ähnlich überlegt man sich den Fall $a_{11} = 0$.

Fazit

$$\boxed{|L(G)| = 1 \quad \Leftrightarrow \quad a_{11}a_{22} - a_{21}a_{12} \neq 0}$$

Definition der Determinante

Sei $n \in \mathbb{N}^*$ und $A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}$. Die Determinante von A ist

$$\boxed{\det A := \begin{cases} a_{11}, & n = 1, \\ \displaystyle\sum_{k=1}^{n} (-1)^{k+1} a_{k1} \det A_{k1}, & n \geq 2, \end{cases}}$$

wobei A_{k1} aus A durch Streichung von Zeile k und Spalte 1 entsteht:

$$A_{k1} = \begin{pmatrix} a_{11} & \cdots & \cdots & a_{1n} \\ \vdots & & & \vdots \\ a_{k1} & \cdots & \cdots & a_{kn} \\ \vdots & & & \vdots \\ a_{n1} & \cdots & \cdots & a_{nn} \end{pmatrix}$$

Eindeutige Lösbarkeit von LGS mit n Gl. und n Unb.

Satz

Ein LGS (G) mit n Gleichungen und n Unbekannten und Koeffizientenmatrix A ist genau dann eindeutig lösbar, wenn $\det A \neq 0$ gilt, das heißt:

$$|L(G)| = 1 \quad \Leftrightarrow \quad \det A \neq 0.$$

Bemerkung

Die Aussage wird später klar, wenn wir uns die Änderung der Determinante unter elementaren Zeilenumformungen überlegen.

Determinantenberechnung für $n = 2$

$$\det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \sum_{k=1}^{2} (-1)^{k+1} a_{k1} \det A_{k1}$$

$$= a_{11} \det A_{11} - a_{21} \det A_{21}$$

$$= a_{11} \det \begin{pmatrix} \cancel{a_{11}} & \cancel{a_{12}} \\ \cancel{a_{21}} & a_{22} \end{pmatrix} - a_{21} \det \begin{pmatrix} \cancel{a_{11}} & a_{12} \\ \cancel{a_{21}} & \cancel{a_{22}} \end{pmatrix}$$

$$= a_{11} a_{22} - a_{21} a_{12}$$

Determinantenberechnung für $n = 3$

$$\det\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = \sum_{k=1}^{3} (-1)^{k+1} a_{k1} \det A_{k1}$$

$$= a_{11} \det A_{11} - a_{21} \det A_{21} + a_{31} \det A_{31}$$

$$= a_{11} \det\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} - a_{21} \det\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$

$$+ a_{31} \det\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$

$$= a_{11}(a_{22}a_{33} - a_{32}a_{23}) - a_{21}(a_{12}a_{33} - a_{32}a_{13}) + a_{31}(a_{12}a_{23} - a_{22}a_{13})$$

$$= a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{31}a_{22}a_{13} - a_{32}a_{23}a_{11} - a_{33}a_{21}a_{12}$$

Determinantenberechnung für $n = 3$

$$\det\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$

$$= a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{31}a_{22}a_{13} - a_{32}a_{23}a_{11} - a_{33}a_{21}a_{12}$$

Merkregel (Regel von Sarrus)

$$\begin{array}{ccccc} + & + & + & & \\ \left(\begin{matrix} a_{11} \\ a_{21} \\ a_{31} \end{matrix}\right. & \begin{matrix} a_{12} \\ a_{22} \\ a_{32} \end{matrix} & \left.\begin{matrix} a_{13} \\ a_{23} \\ a_{33} \end{matrix}\right) & \begin{matrix} a_{11} \\ a_{21} \\ a_{31} \end{matrix} & \begin{matrix} a_{12} \\ a_{22} \\ a_{32} \end{matrix} \\ - & - & - & & \end{array}$$

Achtung: Dieses Schema funktioniert nur für $n = 3$.

Determinantenberechnung von „oberen Dreiecksmatrizen“

$$\det \begin{pmatrix} a_{11} & \cdots & \cdots & a_{1n} \\ 0 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & a_{nn} \end{pmatrix} = a_{11} \cdot a_{22} \cdot \ldots \cdot a_{nn} = \prod_{k=1}^{n} a_{kk}$$

Laplacescher Entwicklungssatz

Satz (ohne Beweis)

Sei A eine Matrix mit n Zeilen und n Spalten.

- Für jedes $l \in \{1, \ldots, n\}$ gilt:

$$\det A = \sum_{k=1}^{n} (-1)^{k+l} a_{kl} \det A_{kl}.$$

(„Entwicklung nach Spalte l“)

- Für jedes $k \in \{1, \ldots, n\}$ gilt:

$$\det A = \sum_{l=1}^{n} (-1)^{k+l} a_{kl} \det A_{kl}.$$

(„Entwicklung nach Zeile k“)

Bemerkung

- Enthält A eine *Nullzeile* oder *Nullspalte*, so ist

$$\det A = 0.$$

- Ist $A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$, so ist die Transponierte A^T von A gegeben durch

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

Ist A eine quadratische Matrix, so ist

$$\det(A) = \det(A^T).$$

Änderung von det unter elementaren Zeilenumformungen

Man kann zeigen, dass sich die Determinante einer Matrix unter elementaren Zeilenumformungen wie folgt verhält:

(Z_1) Die Determinante ändert ihr Vorzeichen bei Vertauschung zweier Zeilen.

(Z_2) Die Determinante wird mit λ multipliziert bei Multiplikation einer Zeile mit $\lambda \neq 0$.

(Z_3) Die Determinante ändert sich nicht, addiert man das Vielfache einer Zeile zu einer anderen.

Bemerkung

Die Determinante wird 0 bei Multiplikation einer Zeile mit 0. (Dies ist jedoch keine elementare Zeilenumformung.)

Änderung von det unter elementaren Spaltenumformungen

Entsprechendes gilt auch für Spaltenumformungen:

(S_1) Die Determinante ändert ihr Vorzeichen bei Vertauschung zweier Spalten.

(S_2) Die Determinante wird mit λ multipliziert bei Multiplikation einer Spalte mit $\lambda \neq 0$.

(S_3) Die Determinante ändert sich nicht, addiert man das Vielfache einer Spalte zu einer anderen.

Bemerkung

Die Determinante wird 0 bei Multiplikation einer Spalte mit 0. (Dies ist jedoch keine elementare Spaltenumformung.)

Algebraische Grundlagen der Informatik

SoSe 2024

KAPITEL IV: Der Vektorraum $\mathbb{R}^n$ und lineare Abbildungen

1. Der Vektorraum $\mathbb{R}^n$

Dozentin: Prof. Dr. Agnes Radl

Email: `agnes.radl@informatik.hs-fulda.de`

Der Vektorraum $\mathbb{R}^n$

Definition

- Unter dem Vektorraum $\mathbb{R}^n$ verstehen wir die Menge $\mathbb{R}^n$ (siehe Kap. III, S. 71) zusammen mit der Addition

$$+ : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n, \quad \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} := \begin{pmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{pmatrix}$$

  und der Skalarmultiplikation

$$\cdot : \mathbb{R} \times \mathbb{R}^n \to \mathbb{R}^n, \quad \lambda \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} := \begin{pmatrix} \lambda x_1 \\ \vdots \\ \lambda x_n \end{pmatrix}.$$

  (Der Malpunkt „·“ wird meistens weggelassen.)
- Die Elemente von $\mathbb{R}^n$ werden als Vektoren bezeichnet.

Der Vektorraum $\mathbb{R}^n$

Definition (Fortsetzung)

Außerdem definieren wir

- $-\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} := \begin{pmatrix} -x_1 \\ \vdots \\ -x_n \end{pmatrix}$
- $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} - \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} := \begin{pmatrix} x_1 - y_1 \\ \vdots \\ x_n - y_n \end{pmatrix}$
- $0_{\mathbb{R}^n} := \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$ „Nullvektor“

  (Oft schreibt man auch nur 0 statt $0_{\mathbb{R}^n}$.)

Rechenregeln in $\mathbb{R}^n$

Man prüft leicht nach, dass für $\lambda \in \mathbb{R}$ und $x \in \mathbb{R}^n$ folgende Rechenregeln gelten:

(a) $0 \cdot x = 0_{\mathbb{R}^n}$,

(b) $\lambda \cdot 0_{\mathbb{R}^n} = 0_{\mathbb{R}^n}$,

(c) $\lambda \cdot x = 0_{\mathbb{R}^n} \quad \Rightarrow \quad \lambda = 0$ oder $x = 0_{\mathbb{R}^n}$,

(d) $(-1) \cdot x = -x$.

Vektorräume – allgemein

Eine Menge V zusammen mit einer Addition

$$+ : V \times V \to V, \quad (v, w) \mapsto v + w$$

und einer Skalarmultiplikation

$$\cdot : \mathbb{R} \times V \to V, \quad (\lambda, v) \mapsto \lambda \cdot v$$

heißt $\mathbb{R}$-Vektorraum oder Vektorraum (VR) über $\mathbb{R}$ falls:

(V1) $(V, +)$ ist eine kommutative Gruppe.

(V2) Für alle $\lambda, \mu \in \mathbb{R}$, $v, w \in V$ gelten:

- $(\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot v$
- $\lambda \cdot (v + w) = \lambda \cdot v + \lambda \cdot w$
- $\lambda \cdot (\mu \cdot v) = (\lambda \cdot \mu) \cdot v$
- $1 \cdot v = v$

Ein Element $v \in V$ heißt Vektor.

(Ersetzt man $\mathbb{R}$ durch $\mathbb{C}$, so erhält man einen $\mathbb{C}$-Vektorraum.)

Beispiele für Vektorräume

Natürlich ist $\mathbb{R}^n$ mit der zu Beginn eingeführten Addition und Skalarmultiplikation ein Vektorraum über $\mathbb{R}$.

Es gibt aber noch andere Vektorräume, zum Beispiel:

$$V := \text{ Menge der Funktionen von } \mathbb{R} \text{ nach } \mathbb{R},$$

wobei für $f, g \in V, \lambda \in \mathbb{R}$

$$f + g : \mathbb{R} \to \mathbb{R}, \quad x \mapsto f(x) + g(x)$$

und

$$\lambda \cdot f : \mathbb{R} \to \mathbb{R}, \quad x \mapsto \lambda f(x).$$

Untervektorräume

Definition

$U \subseteq V$ ist ein Untervektorraum (UVR) des Vektorraumes V, falls

(i) $U \neq \emptyset$

und falls für alle $u, v \in U$ und alle $\lambda \in \mathbb{R}$ gelten

(ii) $u + v \in U$, („abgeschlossen bezüglich Addition“)

(iii) $\lambda u \in U$. („abgeschlossen bezüglich Skalarmultiplikation“)

Beispiele

- $\mathbb{R}^n$ und $\{0_{\mathbb{R}^n}\}$ sind UVR von $\mathbb{R}^n$.
- Man prüft leicht nach, dass die Lösungsmenge eines *homogenen* LGS mit n Unbekannten ein UVR von $\mathbb{R}^n$ ist.
- Es ist

  $$U := \{p : \mathbb{R} \to \mathbb{R} | p \text{ Polynom}\}$$

  ein Untervektorraum des Vektorraums der Funktionen von $\mathbb{R}$ nach $\mathbb{R}$.

Lineare Hülle

Definition

Sei $k \in \mathbb{N}^*$ und seien $v_1, \ldots, v_k \in \mathbb{R}^n$.

Die lineare Hülle von $v_1, \ldots, v_k$ ist die Menge aller Linearkombinationen

$$\operatorname{lin}\{v_1, \ldots, v_k\} := \{\lambda_1 v_1 + \cdots + \lambda_k v_k : \lambda_1, \ldots, \lambda_k \in \mathbb{R}\}.$$

Außerdem definiert man

$$\operatorname{lin} \emptyset := \{0_{\mathbb{R}^n}\}.$$

Bemerkung

Seien $v_1, \ldots, v_k \in \mathbb{R}^n$.

- Es ist $\operatorname{lin}\{v_1, \ldots, v_k\}$ ein UVR von $\mathbb{R}^n$.
- Sind $w_1, \ldots, w_m \in \operatorname{lin}\{v_1, \ldots, v_k\}$, so gilt

$$\operatorname{lin}\{w_1, \ldots, w_m\} \subseteq \operatorname{lin}\{v_1, \ldots, v_k\}.$$

Lineare Unabhängigkeit

Definition

Die Vektoren $v_1, \ldots, v_k \in \mathbb{R}^n$ heißen linear unabhängig, falls aus

$$\lambda_1 v_1 + \cdots + \lambda_k v_k = 0_{\mathbb{R}^n} \quad \text{mit } \lambda_1, \ldots, \lambda_k \in \mathbb{R}$$

stets folgt, dass

$$\lambda_1 = \ldots = \lambda_k = 0.$$

Andernfalls heißen $v_1, \ldots, v_k$ linear abhängig.

Test auf lineare Unabhängigkeit im $\mathbb{R}^n$

Bemerkung

- Der Test auf lineare Unabhängigkeit von k Vektoren $v_1 = \begin{pmatrix} v_{1,1} \\ \vdots \\ v_{1,n} \end{pmatrix}, \ldots, v_k = \begin{pmatrix} v_{k,1} \\ \vdots \\ v_{k,n} \end{pmatrix}$ im $\mathbb{R}^n$ führt auf ein LGS (G) mit n Gleichungen und k Unbekannten $\lambda_1, \ldots, \lambda_k$:

$$\left.\begin{array}{ccccccc} v_{1,1}\lambda_1 & + & \cdots & + & v_{k,1}\lambda_k & = & 0 \\ \vdots & & & & & & \vdots \\ v_{1,n}\lambda_1 & + & \cdots & + & v_{k,n}\lambda_k & = & 0 \end{array}\right\} (G)$$

- Die Vektoren sind genau dann linear unabhängig, wenn $L(G) = \{0_{\mathbb{R}^n}\}$ gilt.

Anleitung zum Test auf lineare Unabhängigkeit im $\mathbb{R}^n$

Test auf lineare Unabhängigkeit der Vektoren $v_1, \dots, v_k \in \mathbb{R}^n$:

- Schreibe die Vektoren $v_1, \dots v_k$ als Spalten in eine Matrix A.
- Bestimme Rang(A).
- Ist
$$\text{Rang}(A) = \text{Anzahl Spalten von } A,$$
so sind die Vektoren linear unabhängig, andernfalls linear abhängig.

Ist $k = n$, so kann man auch die Determinante verwenden:

- Schreibe die Vektoren $v_1, \dots, v_n$ als Spalten in eine Matrix A.
- Bestimme $\det A$.
- Ist
$$\det A \neq 0,$$
so sind die Vektoren linear unabhängig, andernfalls linear abhängig.

Basis und Dimension

Definition

- Sei U ein UVR von $\mathbb{R}^n$, wobei $U \neq \{0_{\mathbb{R}^n}\}$, und seien $b_1, \dots, b_k \in U$.

  Es ist $\{b_1, \dots, b_k\}$ eine Basis von U, falls

  1. $b_1, \dots, b_k$ linear unabhängig sind,
  2. $\operatorname{lin}\{b_1, \dots, b_k\} = U$ gilt.

  Es ist dann k die Dimension des UVR.

  Notation: $\dim U = k$.

- Ist $U = \{0_{\mathbb{R}^n}\}$, so setzt man als Basis die leere Menge und $\dim U = 0$.

Kanonische Basis im $\mathbb{R}^n$

Beispiel

Für $k \in \{1, \dots, n\}$ sei

$$e_k := \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \leftarrow \text{Position } k.$$

Dann ist

$$\{e_1, \dots, e_n\}$$

eine Basis von $\mathbb{R}^n$, die sogenannte kanonische Basis.

Bemerkung (ohne Beweis)

- Jeder UVR U des $\mathbb{R}^n$ besitzt eine Basis.

- Jeder UVR $U \neq \{0_{\mathbb{R}^n}\}$ des $\mathbb{R}^n$ besitzt unendlich viele verschiedene Basen. Unterschiedliche Basen eines UVR haben jedoch immer gleich viele Basisvektoren. (Sonst würde die Definition der *Dimension* keinen Sinn ergeben.)

- Ist U ein UVR mit $\dim U = n$ und sind $v_1, \ldots, v_{n+1} \in U$, dann sind $v_1, \ldots, v_{n+1}$ linear abhängig.

- Ist U ein UVR mit $\dim U = n$ und sind $b_1, \ldots, b_n \in U$ linear unabhängig, dann ist $\{b_1, \ldots, b_n\}$ bereits eine Basis von U.

Sämtliche Untervektorräume des $\mathbb{R}^2$

- 0-dimensional: $U = \{0_{\mathbb{R}^2}\}$
- 1-dimensional: $U_v = \text{lin}\{v\}$ für $v \in \mathbb{R}^2, v \neq 0$
  Anschaulich: Ursprungsgerade durch v
- 2-dimensional: $\mathbb{R}^2$

Sämtliche Untervektorräume des $\mathbb{R}^3$

- 0-dimensional: $U = \{0_{\mathbb{R}^3}\}$
- 1-dimensional: $U_v = \text{lin}\{v\}$ für $v \in \mathbb{R}^3, v \neq 0$

  Anschaulich: Ursprungsgerade durch v
- 2-dimensional: $U_{v,w} = \text{lin}\{v, w\}$ für linear unabhängige $v, w \in \mathbb{R}^3$

  Anschaulich: Von v und w aufgespannte Ebene, die $0_{\mathbb{R}^3}$ enthält.
- 3-dimensional: $\mathbb{R}^3$

Eindeutigkeit der Darstellung bezüglich einer Basis

Satz

Sei V ein UVR von $\mathbb{R}^n$ mit Basis $\mathcal{B} = \{b_1, \ldots, b_k\}$. Dann gibt es zu jedem $v \in V$ *eindeutig* bestimmte Koeffizienten $\lambda_1, \ldots, \lambda_k \in \mathbb{R}$ mit

$$v = \lambda_1 b_1 + \cdots + \lambda_k b_k.$$

Definition

$\lambda_1, \ldots, \lambda_k$ sind die Koordinaten von v bezüglich der Basis $\mathcal{B}$.

Koordinatenabbildung

Bemerkung

- Sei $\mathcal{B} = \{b_1, \dots, b_m\}$ eine Basis eines m-dimensionalen Untervektorraums V von $\mathbb{R}^n$. Die Koordinatenabbildung

$$K_{\mathcal{B}} : V \to \mathbb{R}^m, \quad v = \sum_{k=1}^{m} \lambda_k b_k \mapsto \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_m \end{pmatrix}$$

  ordnet jedem Vektor $v \in V$ seine Koordinaten bezüglich der Basis $\mathcal{B}$ zu.
- Die Koordinatenabbildung ist bijektiv.

Beispiel

$\mathcal{B}_1 := \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\}$ und $\mathcal{B}_2 := \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \right\}$ sind Basen des UVR $V := \left\{ \begin{pmatrix} x_1 \\ x_2 \\ 0 \end{pmatrix} : x_1, x_2 \in \mathbb{R} \right\}$ des $\mathbb{R}^3$.
Für $v = \begin{pmatrix} 3 \\ -1 \\ 0 \end{pmatrix} \in V$ gilt nun

$$v = 3 \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} - 1 \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = 4 \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} - 1 \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}.$$

Somit sind

- 3 und -1 die Koordinaten von v bezüglich $\mathcal{B}_1$, also $K_{\mathcal{B}_1}(v) = \begin{pmatrix} 3 \\ -1 \end{pmatrix}$.
- 4 und -1 die Koordinaten von v bezüglich $\mathcal{B}_2$, also $K_{\mathcal{B}_2}(v) = \begin{pmatrix} 4 \\ -1 \end{pmatrix}$.

Algebraische Grundlagen der Informatik

SoSe 2024

KAPITEL IV: Der Vektorraum $\mathbb{R}^n$ und lineare Abbildungen

2. Lineare Abbildungen und Matrizen

Dozentin: Prof. Dr. Agnes Radl

Email: `agnes.radl@informatik.hs-fulda.de`

Lineare Abbildungen

Definition

Seien $U \subseteq \mathbb{R}^n$ und $V \subseteq \mathbb{R}^m$ UVR. Eine Abbildung

$$f : U \to V$$

heißt linear, falls für alle $x, y \in U$ und $\lambda \in \mathbb{R}$ gilt:

(L1) $f(\lambda x) = \lambda f(x)$,

(L2) $f(x + y) = f(x) + f(y)$.

Bemerkung

Es gilt

$$f(0_U) = f(0 \cdot 0_U) \overset{(L1)}{=} 0 \cdot f(0_U) = 0_V.$$

Beispiele für lineare Abbildungen

1. $\mathbb{R}^n \to \mathbb{R}^m, \quad x \mapsto 0_{\mathbb{R}^m}$ ist linear.

2. $\mathbb{R}^n \to \mathbb{R}^n, \quad x \mapsto \alpha x$ ist für jedes $\alpha \in \mathbb{R}$ linear.

3. $P : \mathbb{R}^n \to \mathbb{R}, \quad \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto x_1$ ist linear.

4. $S : \mathbb{R}^2 \to \mathbb{R}^2, \quad \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} -x_1 \\ x_2 \end{pmatrix}$ ist linear.
   („Spiegelung an der y-Achse“)

5. $f : \mathbb{R}^2 \to \mathbb{R}^3, \quad \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} x_1+x_2 \\ 2x_1 \\ 4x_1+2x_2 \end{pmatrix}$ ist linear.

6. $D_\alpha : \mathbb{R}^2 \to \mathbb{R}^2, \quad \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \mapsto \begin{pmatrix} \cos(\alpha)x_1 - \sin(\alpha)x_2 \\ \sin(\alpha)x_1 + \cos(\alpha)x_2 \end{pmatrix}$ ist für jedes $\alpha \in \mathbb{R}$ linear.
   („Drehung um den Winkel α“)

Wie erkennt man lineare Abbildungen auf einen Blick?

Bemerkung

Abbildungen der Form

$$f : \mathbb{R}^n \to \mathbb{R}^m, \quad \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} a_{11}x_1 + \ldots + a_{1n}x_n \\ \vdots \\ a_{m1}x_1 + \ldots + a_{mn}x_n \end{pmatrix}$$

mit $a_{ij} \in \mathbb{R}$, $i = 1, \ldots, m, j = 1, \ldots, n$, sind linear und umgekehrt ist jede lineare Abbildung von dieser Form.

Beispiele für Abbildungen, die nicht linear sind

7. $f : \mathbb{R} \to \mathbb{R}, \quad x \mapsto x + 1$ ist nicht linear.
8. $\tilde{f} : \mathbb{R}^3 \to \mathbb{R}^3, \quad x \mapsto x + \begin{pmatrix} 1 \\ -3 \\ 2 \end{pmatrix}$ ist nicht linear.
9. $g : \mathbb{R}_+ \to \mathbb{R}, \quad x \mapsto \sqrt{x}$ ist nicht linear.
10. $h : \mathbb{R} \to \mathbb{R}, \quad x \mapsto x^2$ ist nicht linear.
11. $\cos, \sin, \tan$ sind nicht linear.

Darstellende Matrizen

Beobachtung und Definition

- Sei $\{e_1, \ldots, e_n\}$ die kanonische Basis des $\mathbb{R}^n$. Ist $f : \mathbb{R}^n \to \mathbb{R}^m$ linear und ist $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{R}^n$, so ist

$$f(x) = f(x_1 e_1 + \ldots + x_n e_n) \overset{f \text{ linear}}{=} x_1 f(e_1) + \ldots + x_n f(e_n) \quad (\in \mathbb{R}^m).$$

- Um $f(x)$ zu berechnen, muss also nur $f(e_1), \ldots, f(e_n)$ bekannt sein.
- Schreibe $f(e_1), \ldots, f(e_n)$ als Spalten einer Matrix A_f.
  A_f hat dann m Zeilen und n Spalten.
  Sprechweise: A_f ist eine $m \times n$-Matrix.
- $\mathbb{R}^{m \times n} :=$ Menge aller $m \times n$-Matrizen.
- A_f heißt darstellende Matrix der linearen Abbildung f.

Beispiele (darstellende Matrizen zu S. 114)

1. $\begin{pmatrix} 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix} \in \mathbb{R}^{m \times n}$
2. $\begin{pmatrix} \alpha & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \alpha \end{pmatrix} \in \mathbb{R}^{n \times n}$
3. $\begin{pmatrix} 1 & 0 & \cdots & 0 \end{pmatrix} \in \mathbb{R}^{1 \times n}$
4. $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$
5. $\begin{pmatrix} 1 & 1 \\ 2 & 0 \\ 4 & 2 \end{pmatrix}$
6. $\begin{pmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{pmatrix}$

Multiplikation „Matrix · Vektor“

Idee:

„Matrix · Vektor“ soll so definiert werden, dass

$$\boxed{A_f \cdot x = f(x)}$$

gilt, wenn A_f die darstellende Matrix für die lineare Abbildung f ist und x im Definitionsbereich von f liegt.

Multiplikation „Matrix · Vektor"

Definition

Ist $A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \in \mathbb{R}^{m \times n}$

(Kurznotation: $A = (a_{ij}) \in \mathbb{R}^{m \times n}$)

und $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{R}^n$, so definiert man

$$Ax := x_1 \begin{pmatrix} a_{11} \\ \vdots \\ a_{m1} \end{pmatrix} + \ldots + x_n \begin{pmatrix} a_{1n} \\ \vdots \\ a_{mn} \end{pmatrix}.$$

Bemerkung

Es ist $Ax \in \mathbb{R}^m$ und

$$Ax = \begin{pmatrix} a_{11}x_1 + \ldots + a_{1n}x_n \\ \vdots \\ a_{m1}x_1 + \ldots + a_{mn}x_n \end{pmatrix} = \begin{pmatrix} \sum_{k=1}^n a_{1k}x_k \\ \vdots \\ \sum_{k=1}^n a_{mk}x_k \end{pmatrix}.$$

Beispiele

- $$\underbrace{\begin{pmatrix} 3 & -2 \\ 2 & 0 \\ 1 & 4 \end{pmatrix}}_{\in \mathbb{R}^{3\times 2}} \underbrace{\begin{pmatrix} 1 \\ 2 \end{pmatrix}}_{\in \mathbb{R}^{2}} = \begin{pmatrix} 3\cdot 1 - 2\cdot 2 \\ 2\cdot 1 + 0\cdot 2 \\ 1\cdot 1 + 4\cdot 2 \end{pmatrix} = \begin{pmatrix} -1 \\ 2 \\ 9 \end{pmatrix} \in \mathbb{R}^3$$
- $$\underbrace{\begin{pmatrix} 1 & -2 & 0 & 4 \\ -3 & -1 & 2 & 1 \end{pmatrix}}_{\in \mathbb{R}^{2\times 4}} \underbrace{\begin{pmatrix} 1 \\ 0 \\ -1 \\ 2 \end{pmatrix}}_{\in \mathbb{R}^{4}} =$$
  $$\begin{pmatrix} 1\cdot 1 - 2\cdot 0 + 0\cdot(-1) + 4\cdot 2 \\ -3\cdot 1 - 1\cdot 0 + 2\cdot(-1) + 1\cdot 2 \end{pmatrix} = \begin{pmatrix} 9 \\ -3 \end{pmatrix} \in \mathbb{R}^2$$

Beispiele (Fortsetzung)

- $$\underbrace{\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}}_{\in\mathbb{R}^{2\times 2}} \underbrace{\begin{pmatrix} 5 \\ 6 \end{pmatrix}}_{\in\mathbb{R}^{2}} = \begin{pmatrix} 1\cdot 5 + 2\cdot 6 \\ 3\cdot 5 + 4\cdot 6 \end{pmatrix} = \begin{pmatrix} 17 \\ 39 \end{pmatrix} \in \mathbb{R}^2$$
- $$\underbrace{\begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix}}_{\in\mathbb{R}^{3\times 2}} \underbrace{\begin{pmatrix} 7 \\ 8 \\ 9 \end{pmatrix}}_{\in\mathbb{R}^{3}}$$

  Rote Zahlen stimmen nicht überein – ist also nicht definiert!

Bemerkung

- Für $A \in \mathbb{R}^{m \times n}$ ist die Abbildung

$$\mathbb{R}^n \to \mathbb{R}^m, \quad x \mapsto Ax$$

  linear.
- Ist (G) ein LGS mit Koeffizientenmatrix $A \in \mathbb{R}^{m \times n}$ und rechter Seite $b \in \mathbb{R}^m$, so ist

$$L(G) = \{x \in \mathbb{R}^n : Ax = b\}.$$

Beobachtung (ohne Beweis)

- Sind $f : \mathbb{R}^n \to \mathbb{R}^m$ und $g : \mathbb{R}^n \to \mathbb{R}^m$ lineare Abbildungen und ist $\lambda \in \mathbb{R}$, so sind auch
  - $f + g : \mathbb{R}^n \to \mathbb{R}^m, \quad x \mapsto f(x) + g(x)$,
  - $\lambda f : \mathbb{R}^n \to \mathbb{R}^m, \quad x \mapsto \lambda f(x)$

  lineare Abbildungen.
- Sind $f : \mathbb{R}^n \to \mathbb{R}^r$ und $g : \mathbb{R}^r \to \mathbb{R}^m$ linear, so ist auch
  - $g \circ f : \mathbb{R}^n \to \mathbb{R}^m$

  linear.

Frage

Wie sehen die darstellenden Matrizen $A_{f+g}, A_{\lambda f}$ und $A_{g \circ f}$ aus?

Addition/ Skalarmultiplikation von Matrizen und Matrizenprodukt

Definition

- Sind $A = (a_{ij})$ und $B = (b_{ij})$ beide in $\mathbb{R}^{m \times n}$, so definiert man

$$A + B := (a_{ij} + b_{ij}) \in \mathbb{R}^{m \times n}.$$

Ist $\lambda \in \mathbb{R}$, so definiert man

$$\lambda A := (\lambda a_{ij}) \in \mathbb{R}^{m \times n}.$$

- Ist $A = (a_{ij}) \in \mathbb{R}^{m \times r}$ und $B = (b_{ij}) \in \mathbb{R}^{r \times n}$, so definiert man

$$A \cdot B := (c_{ij}) \in \mathbb{R}^{m \times n},$$

wobei

$$c_{ij} = \sum_{k=1}^{r} a_{ik} b_{kj}.$$

Darstellende Matrizen für Addition, Skalarmultiplikation, Komposition

Beobachtung (ohne Beweis)

- Sind $f : \mathbb{R}^n \to \mathbb{R}^m$ und $g : \mathbb{R}^n \to \mathbb{R}^m$ lineare Abbildungen und ist $\lambda \in \mathbb{R}$, so gilt für die darstellenden Matrizen
  - $\boxed{A_{f+g} = A_f + A_g}$,
  - $\boxed{A_{\lambda f} = \lambda A_f}$.
- Sind $f : \mathbb{R}^n \to \mathbb{R}^r$ und $g : \mathbb{R}^r \to \mathbb{R}^m$ linear, so gilt für die darstellenden Matrizen
  - $\boxed{A_{g \circ f} = A_g A_f}$.

Beispiele

- $$\underbrace{\begin{pmatrix} 3 & 2 \\ 4 & 1 \\ 0 & -6 \end{pmatrix}}_{\in \mathbb{R}^{3\times 2}} \underbrace{\begin{pmatrix} 1 & 0 \\ 2 & -1 \end{pmatrix}}_{\in \mathbb{R}^{2\times 2}} = \begin{pmatrix} 3\cdot 1 + 2\cdot 2 & 3\cdot 0 + 2\cdot(-1) \\ 4\cdot 1 + 1\cdot 2 & 4\cdot 0 + 1\cdot(-1) \\ 0\cdot 1 - 6\cdot 2 & 0\cdot 0 - 6\cdot(-1) \end{pmatrix} = \underbrace{\begin{pmatrix} 7 & -2 \\ 6 & -1 \\ -12 & 6 \end{pmatrix}}_{\in \mathbb{R}^{3\times 2}}$$

- $$\underbrace{\begin{pmatrix} 3 & 2 \\ 4 & 1 \\ 0 & -6 \end{pmatrix}}_{\in \mathbb{R}^{3\times 2}} \underbrace{\begin{pmatrix} 3 & 2 \\ 4 & 1 \\ 0 & -6 \end{pmatrix}}_{\in \mathbb{R}^{3\times 2}}$$ Rote Zahlen stimmen nicht überein – ist also nicht definiert!

Beispiele (Fortsetzung)

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

  $$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

  Beachte: Das Matrizenprodukt ist i. A. nicht kommutativ!

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

  Beachte: Das Produkt ist die „Nullmatrix“, obwohl keine der Matrizen die Nullmatrix ist.

Rechenregeln für Matrizen

Bemerkung

Sind A, B und C Matrizen (mit passender Dimension für nachfolgende Operationen) und ist $\lambda \in \mathbb{R}$, so gelten:

- $(\lambda A)B = \lambda(AB) = A(\lambda B)$
- Assoziativgesetz: $(AB)C = A(BC)$
- Distributivgesetze:
  - $(A + B)C = AC + BC$
  - $A(B + C) = AB + AC$

Kern und Bild

Definition

Sei $A \in \mathbb{R}^{m \times n}$.

- Der Kern von A ist
$$\ker A := \{x \in \mathbb{R}^n : Ax = 0_{\mathbb{R}^m}\}.$$
- Das Bild von A ist
$$\operatorname{im} A := \{Ax : x \in \mathbb{R}^n\}.$$

Bemerkung

Es ist

- $\ker A$ ein Untervektorraum von $\mathbb{R}^n$,
- $\operatorname{im} A$ ein Untervektorraum von $\mathbb{R}^m$.

Rangsatz

Satz (ohne Beweis)

Sei $A \in \mathbb{R}^{m \times n}$. Dann gilt:

$$\boxed{\dim \ker(A) + \dim \operatorname{im}(A) = n.}$$

Bemerkung (ohne Beweis)

Es ist

$$\dim \operatorname{im}(A) = \operatorname{Rang}(A).$$

Zusammenhang Rang(A) und Injektivität, Surjektivität, Bijektivität der zugehörigen linearen Abbildung

Bemerkung (ohne Beweis)

Sei $A \in \mathbb{R}^{m \times n}$. Die lineare Abbildung $f : \mathbb{R}^n \to \mathbb{R}^m, x \mapsto Ax$ ist

- injektiv $\Leftrightarrow \ker(A) = \{0_{\mathbb{R}^n}\}$
  $\Leftrightarrow \text{Rang}(A) = n$,
- surjektiv $\Leftrightarrow \dim \text{im}(A) = m$
  $\Leftrightarrow \text{Rang}(A) = m$,
- bijektiv $\Leftrightarrow m = n$ und $\text{Rang}(A) = n$
  $\Leftrightarrow m = n$ und $\det(A) \neq 0$.

Darstellende Matrix für Umkehrabbildung

Beobachtung (ohne Beweis)

Ist $f : \mathbb{R}^n \to \mathbb{R}^n$ linear und bijektiv, so ist auch die Umkehrabbildung $f^{-1} : \mathbb{R}^n \to \mathbb{R}^n$ linear.

Frage

Wie sieht die darstellenden Matrix $A_{f^{-1}}$ aus?

Überlegung

Da

$$f^{-1} \circ f = \mathrm{id}_{\mathbb{R}^n} = f \circ f^{-1},$$

muss also gelten

$$A_{f^{-1}} A_f = A_{\mathrm{id}_{\mathbb{R}^n}} = A_f A_{f^{-1}}.$$

Definition

- Mit I oder I_n wird die Einheitsmatrix

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix} \in \mathbb{R}^{n \times n}$$

  bezeichnet.
- Ist $A \in \mathbb{R}^{n \times n}$, und gibt es eine Matrix $A^{-1} \in \mathbb{R}^{n \times n}$ mit

$$AA^{-1} = A^{-1}A = I_n,$$

  so nennt man A invertierbar, und A^{-1} ist die zu A inverse Matrix.

Bemerkung (ohne Beweis)

- Für alle $A \in \mathbb{R}^{n\times n}$ gilt $AI_n = I_nA = A$.
- Ist $f : \mathbb{R}^n \to \mathbb{R}^n$ linear und bijektiv, so ist A_f invertierbar und

$$\boxed{(A_f)^{-1} = A_{f^{-1}}.}$$

- Es gilt für $A \in \mathbb{R}^{n\times n}$:

$$\boxed{A \text{ invertierbar} \quad \Leftrightarrow \quad \det A \neq 0 \quad \Leftrightarrow \quad \operatorname{Rang}(A) = n.}$$

- Ist $A \in \mathbb{R}^{n\times n}$ invertierbar und gilt $AB = I$ oder $BA = I$ für ein $B \in \mathbb{R}^{n\times n}$, so ist $B = A^{-1}$.
- Die Inverse zu einer invertierbaren Matrix ist eindeutig bestimmt.
- Ist $A \in \mathbb{R}^{n\times n}$ invertierbar und $b \in \mathbb{R}^n$, so ist $x = A^{-1}b$ die Lösung für das LGS $Ax = b$.

Berechnung von A^{-1}, falls $A \in \mathbb{R}^{n\times n}$ invertierbar

Möglichkeit 1

Der Ansatz $A^{-1}A = I_n$ oder $AA^{-1} = I_n$ führt auf ein LGS mit

- n^2 Gleichungen (vom Vergleich der n^2 Einträge auf der linken mit den n^2 Einträgen auf der rechten Seite) und
- n^2 Unbekannten (den Einträgen von A^{-1}).

Löse das LGS und erhalte so die Einträge von A^{-1}.

Berechnung von A^{-1}, falls $A \in \mathbb{R}^{n \times n}$ invertierbar

Beispiel (mit Möglichkeit 1)

$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$, $A^{-1} = \begin{pmatrix} \widetilde{a}_{11} & \widetilde{a}_{12} \\ \widetilde{a}_{21} & \widetilde{a}_{22} \end{pmatrix}$

Ansatz: $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} \widetilde{a}_{11} & \widetilde{a}_{12} \\ \widetilde{a}_{21} & \widetilde{a}_{22} \end{pmatrix} \overset{!}{=} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Vergleich der Einträge auf linker und rechter Seite liefert das LGS

$$\begin{array}{rcrrcrcl} \widetilde{a}_{11} & + & 2\widetilde{a}_{21} & & & & = & 1 \\ 3\widetilde{a}_{11} & + & 4\widetilde{a}_{21} & & & & = & 0 \\ & & & \widetilde{a}_{12} & + & 2\widetilde{a}_{22} & = & 0 \\ & & & 3\widetilde{a}_{12} & + & 4\widetilde{a}_{22} & = & 1 \end{array}$$

Löse das LGS und erhalte $\widetilde{a}_{11} = -2$, $\widetilde{a}_{21} = \frac{3}{2}$, $\widetilde{a}_{12} = 1$, $\widetilde{a}_{22} = -\frac{1}{2}$, das heißt,

$$A^{-1} = \begin{pmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{pmatrix}$$

Berechnung von A^{-1}, falls $A \in \mathbb{R}^{n\times n}$ invertierbar

Möglichkeit 2

Löse

$$Ax^{(1)} = e_1, \dots, Ax^{(n)} = e_n$$

simultan, wobei e_k den k-ten kanonischen Basisvektor bezeichnet. Forme dazu A mit Gaußverfahren so lange um, bis A in die Einheitsmatrix umgeformt ist. Führe die gleichen Umformungen an I_n durch. Die daraus resultierende Matrix ist A^{-1}:

$$(A|I_n) \to \dots \text{ Gauß-Verfahren } \dots \to (I_n|A^{-1}).$$

Berechnung von A^{-1}, falls $A \in \mathbb{R}^{n\times n}$ invertierbar

Beispiel (mit Möglichkeit 2)

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$

$$(A|I_2) = \left(\begin{array}{cc|cc} 1 & 2 & 1 & 0 \\ 3 & 4 & 0 & 1 \end{array}\right) \xrightarrow{(ii)-3(i)} \left(\begin{array}{cc|cc} 1 & 2 & 1 & 0 \\ 0 & -2 & -3 & 1 \end{array}\right)$$

$$\xrightarrow{-\frac{1}{2}(ii)} \left(\begin{array}{cc|cc} 1 & 2 & 1 & 0 \\ 0 & 1 & \frac{3}{2} & -\frac{1}{2} \end{array}\right) \xrightarrow{(i)-2(ii)} \left(\begin{array}{cc|cc} 1 & 0 & -2 & 1 \\ 0 & 1 & \frac{3}{2} & -\frac{1}{2} \end{array}\right)$$

Links von dem senkrechten Strich steht nun die Einheitsmatrix und Rechts davon die Inverse von A:

$$A^{-1} = \begin{pmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{pmatrix}.$$

Was passiert mit der Determinante bei den Matrizenoperationen?

Bemerkung (ohne Beweis)

Seien $A, B \in \mathbb{R}^{n \times n}$ und $\lambda \in \mathbb{R}$. Dann gilt Folgendes:

- $\det(A + B) \overset{\text{i. A.}}{\neq} \det(A) + \det(B)$,
- $\det(\lambda A) = \lambda^n \det(A)$,
- Determinantenmultiplikationssatz: $\det(AB) = \det(A)\det(B)$,

  insbesondere: $\det\left(A^{-1}\right) = \dfrac{1}{\det(A)}$.

Darstellende Matrix der Koordinatenabbildung

- Sei $\mathcal{B} = \{b_1, \dots, b_n\}$ eine Basis des $\mathbb{R}^n$. Die Koordinatenabbildung

$$K_{\mathcal{B}} : \mathbb{R}^n \to \mathbb{R}^n, \quad x = \sum_{k=1}^{n} \lambda_k b_k \mapsto \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}$$

ordnet jedem Vektor $x \in \mathbb{R}^n$ seine Koordinaten bezüglich der Basis $\mathcal{B}$ zu und ist bijektiv, siehe Seite 111.

- Außerdem ist $K_{\mathcal{B}}$ linear.

Frage

Was ist die darstellende Matrix von $K_{\mathcal{B}}$?

Darstellende Matrix der Koordinatenabbildung

Überlegung

- Die Koordinaten von $x \in \mathbb{R}^n$ bezüglich $\mathcal{B}$ sind die eindeutig bestimmten Koeffizienten $\lambda_1, \ldots, \lambda_n$, so dass gilt:

$$x = \lambda_1 b_1 + \ldots + \lambda_n b_n.$$

- Ist S die $n \times n$-Matrix, deren k-te Spalte gerade b_k ist, also $S = (b_1 \cdots b_n) \in \mathbb{R}^{n \times n}$, so gilt

$$x = \lambda_1 b_1 + \ldots + \lambda_n b_n = S \underbrace{\begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}}_{=K_{\mathcal{B}}(x)}.$$

- Da S invertierbar ist, folgt

$$\boxed{S^{-1} x = K_{\mathcal{B}}(x).}$$

Fazit

S^{-1} ist die darstellende Matrix der Koordinatenabbildung.

Zusammenfassung der Umrechnung

Sei $\mathcal{B} = \{b_1, \dots, b_n\}$ eine Basis des $\mathbb{R}^n$ und sei S die $n \times n$-Matrix, deren k-te Spalte gerade b_k ist, also $S = (b_1 \cdots b_n) \in \mathbb{R}^{n \times n}$.
Sei $x \in \mathbb{R}^n$ und seien in $x_{\mathcal{B}}$ die Koordinaten von x bezüglich $\mathcal{B}$, also $x_{\mathcal{B}} = K_{\mathcal{B}}(x)$.

Die Darstellungen können wie folgt ineinander umgerechnet werden.

- Umrechnung von $x \in \mathbb{R}^n$ in die Darstellung bezüglich $\mathcal{B}$:

$$\boxed{x_{\mathcal{B}} = S^{-1}x}.$$

- Umrechnung der Darstellung bezüglich $\mathcal{B}$ in die Standarddarstellung:

$$\boxed{x = S x_{\mathcal{B}}}.$$

Abbildungsmatrix bezüglich beliebiger Basis

- Sei $f : \mathbb{R}^n \to \mathbb{R}^n$ linear mit darstellender Matrix $A_f \in \mathbb{R}^{n \times n}$.
- Sei $\mathcal{B} = \{b_1, \ldots, b_n\}$ eine Basis von $\mathbb{R}^n$.
- Sei S die $n \times n$-Matrix, deren k-te Spalte gerade b_k ist, also $S = (b_1 \cdots b_n) \in \mathbb{R}^{n \times n}$.

Frage:

Wie sieht die darstellende Matrix $A_{\mathcal{B},f}$ von f bezüglich $\mathcal{B}$ aus?

Darstellende Matrix bezüglich beliebiger Basis

Besitzt x die Koordinaten $\lambda_1, \ldots, \lambda_n$ bezüglich $\mathcal{B}$, also $K_{\mathcal{B}}(x) = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}$, so soll $A_{\mathcal{B},f} \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}$ die Koordinaten von $f(x)$ bezüglich $\mathcal{B}$ liefern.

Überlegung:

$$\begin{tikzcd} \mathbb{R}^n \arrow[r, "A_f"] & \mathbb{R}^n \arrow[d, "S^{-1}"] \\ \mathbb{R}^n \arrow[u, "S"] \arrow[r, "A_{\mathcal{B},f}"'] & \mathbb{R}^n \end{tikzcd}$$

Antwort: $\boxed{A_{\mathcal{B},f} = S^{-1} A_f S}$

Algebraische Grundlagen der Informatik

SoSe 2024

KAPITEL V: Eigenwerte und Eigenvektoren

1. Grundlagen

Dozentin: Prof. Dr. Agnes Radl

Email: agnes.radl@informatik.hs-fulda.de

Darstellende Matrix bezüglich beliebiger Basis

Sei im Folgenden immer $\mathbb{K} = \mathbb{R}$ oder $\mathbb{K} = \mathbb{C}$.

Erinnerung

- Sei $f : \mathbb{K}^n \to \mathbb{K}^n$ linear mit darstellender Matrix $A_f \in \mathbb{K}^{n \times n}$.
- Sei $\mathcal{B} = \{b_1, \ldots, b_n\}$ eine Basis des $\mathbb{K}^n$.
- Sei S die Matrix mit Spalten $b_1, \ldots, b_n$.

Dann ist die darstellende Matrix $A_{\mathcal{B},f}$ von f bezüglich $\mathcal{B}$ gegeben durch

$$\boxed{A_{\mathcal{B},f} = S^{-1} A_f S}.$$

Ziel

Finde eine Basis $\mathcal{B}$ so, dass $A_{\mathcal{B},f}$ besonders einfach wird, am besten eine Diagonalmatrix D.

Fragen

- Wann gibt es solch eine Basis $\mathcal{B}$?
- Wie findet man sie in diesem Fall?

Bedingung für „Diagonalisierbarkeit“

Beobachtung

Sei S eine invertierbare $n \times n$-Matrix mit Spalten $b_1, \dots, b_n$ und D eine Diagonalmatrix mit Diagonaleinträgen $\lambda_1, \dots, \lambda_n$, so dass

$$S^{-1} A_f S = D$$

gilt. Dann gilt

$$A_f S = SD,$$

woraus wiederum folgt

$$A_f b_1 = \lambda_1 b_1, \quad \dots \quad , A_f b_n = \lambda_n b_n.$$

Fazit

Man benötigt n linear unabhängige Vektoren, die durch A_f nur skaliert werden.

Eigenwerte und Eigenvektoren

Definition

Sei $A \in \mathbb{K}^{n \times n}$.

- Ein $\lambda \in \mathbb{K}$ heißt Eigenwert (EW) von A, falls es ein $x \in \mathbb{K}^n, x \neq 0_{\mathbb{K}^n}$, gibt mit

$$\boxed{Ax = \lambda x.}$$

- x heißt dann Eigenvektor (EV) von A zum Eigenwert λ.
- $\sigma(A)$ bzw. $\sigma_{\mathbb{K}}(A)$ bezeichnet die Menge der Eigenwerte von A.

Bemerkung

- Achtung: $0_{\mathbb{K}^n}$ ist nie ein Eigenvektor!
  Hingegen kann 0 als Eigenwert vorkommen.
- Ist x ein Eigenvektor von A zum Eigenwert λ, dann auch cx für alle $c \in \mathbb{K} \setminus \{0\}$.

Auffinden von Eigenwerten

Beobachtung

$$Ax = \lambda x \quad \Leftrightarrow \quad Ax - \lambda x = 0_{\mathbb{K}^n} \quad \Leftrightarrow \quad (A - \lambda I)x = 0_{\mathbb{K}^n}$$

Also:

$$\begin{aligned} \lambda \text{ EW von } A \quad &\Leftrightarrow \quad \text{Es gibt ein } x \neq 0_{\mathbb{K}^n} \text{ so, dass } (A - \lambda I)x = 0_{\mathbb{K}^n}. \\ &\Leftrightarrow \quad \operatorname{Rang}(A - \lambda I) < n \\ &\Leftrightarrow \quad \det(A - \lambda I) = 0 \end{aligned}$$

$$\boxed{\text{Die EW von } A \text{ sind also gerade die Nullstellen von } \det(A - \lambda I).}$$

Charakteristisches Polynom

Definition

Sei $A \in \mathbb{K}^{n \times n}$. Dann ist

$$\boxed{p_A(\lambda) := \det(A - \lambda I)}$$

das charakteristische Polynom von A.

Bemerkung

- p_A ist ein Polynom (in λ) vom Grad n.
- Die Nullstellen von p_A sind gerade die Eigenwerte von A.

Eigenräume

Definition

- Ist λ ein Eigenwert von $A \in \mathbb{K}^{n \times n}$, so ist

$$\mathrm{Eig}(A, \lambda) := \{x \in \mathbb{K}^n : (A - \lambda I)x = 0_{\mathbb{K}^n}\}$$

  der Eigenraum von A zum Eigenwert λ.
- Die geometrische Vielfachheit von λ ist

$$V_g(A, \lambda) := \dim \mathrm{Eig}(A, \lambda).$$

Bemerkung

Der Menge der Eigenvektoren von A zum Eigenwert λ ist

$$\mathrm{Eig}(A, \lambda) \setminus \{0_{\mathbb{K}^n}\}.$$

Vorgehen zur Bestimmung der EW und EV von $A \in \mathbb{K}^{n \times n}$

1. Charakteristisches Polynom $p_A(\lambda) = \det(A - \lambda I)$ aufstellen.
2. Bestimmung der Nullstellen von p_A.
   (Dies sind genau die Eigenwerte von A.)
3. Bestimmung der Eigenräume $\mathrm{Eig}(A, \lambda)$ für jeden Eigenwert λ von A durch Lösen des LGS

   $$(A - \lambda I)x = 0_{\mathbb{K}^n}.$$

   (Jedes $x \in \mathrm{Eig}(A, \lambda) \setminus \{0_{\mathbb{K}^n}\}$ ist Eigenvektor von A zum Eigenwert λ.)

Algebraische Grundlagen der Informatik

SoSe 2024

KAPITEL V: Eigenwerte und Eigenvektoren

2. Polynome

Dozentin: Prof. Dr. Agnes Radl

Email: `agnes.radl@informatik.hs-fulda.de`

Fundamentalsatz der Algebra

Satz (ohne Beweis)

Jedes Polynom p mit komplexen Koeffizienten und $\mathrm{grad}(p) \geq 1$ besitzt mindestens eine Nullstelle in $\mathbb{C}$.

Polynomdivision

Bemerkung

- Ist λ_0 eine Nullstelle des Polynoms p, so gilt

$$p(\lambda) = (\lambda - \lambda_0) q(\lambda),$$

  wobei q ebenfalls ein Polynom ist mit $\mathrm{grad}(q) = \mathrm{grad}(p) - 1$.
- Die Nullstellen von p sind λ_0 und die Nullstellen von q.
- Das Polynom q erhält man durch „Polynomdivision“.

Polynome

Satz und Definition

- Jedes Polynom

$$p(\lambda) = a_n\lambda^n + \ldots + a_1\lambda + a_0$$

  mit $n \in \mathbb{N}^*$, $a_0, \ldots, a_n \in \mathbb{C}, a_n \neq 0$, zerfällt in Linearfaktoren, das heißt, sind $\lambda_1, \ldots, \lambda_r \in \mathbb{C}$ die paarweise verschiedenen Nullstellen von p, so gilt

$$p(\lambda) = a_n \prod_{k=1}^{r} (\lambda - \lambda_k)^{m_k},$$

  wobei $m_k \in \mathbb{N}^*$ eindeutig bestimmt ist.
- m_k wird als die algebraische Vielfachheit der Nullstelle λ_k bezeichnet.
- Es gilt: $\sum\limits_{k=1}^{r} m_k = n$.

Bemerkung

$A \in \mathbb{C}^{n\times n}$ besitzt also mindestens einen und höchstens n verschiedene Eigenwerte in $\mathbb{C}$.

Beispiele

- $p(\lambda) = \lambda^2 + 1 = (\lambda - \mathrm{i})(\lambda + \mathrm{i})$

  Die Nullstellen i und $-\mathrm{i}$ haben jeweils die algebraische Vielfachheit 1.

- $p(\lambda) = -\lambda^3 + 3\lambda^2 - 4 = -(\lambda - 2)^2(\lambda + 1)$

  Die Nullstelle 2 hat algebraische Vielfachheit 2.
  Die Nullstelle -1 hat algebraische Vielfachheit 1.

Algebraische Vielfachheit von Eigenwerten

Definition

Ist $\lambda_0 \in \mathbb{C}$ ein Eigenwert einer Matrix $A \in \mathbb{C}^{n \times n}$, so ist die algebriasche Vielfachheit $V_a(A, \lambda_0)$ des Eigenwerts λ_0 gerade die algebraische Vielfachheit der Nullstelle λ_0 im charakteristischen Polynom.

Nullstellen von Polynomen vom Grad 2

Satz

Sei $p(\lambda) = a\lambda^2 + b\lambda + c$ mit $a, b, c \in \mathbb{R}$, $a \neq 0$. Die Nullstellen von p sind

$$\begin{cases} \dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}, & \text{falls } b^2 - 4ac > 0, \\ -\dfrac{b}{2a}, & \text{falls } b^2 - 4ac = 0, \\ -\dfrac{b}{2a} \pm \mathrm{i}\,\dfrac{\sqrt{4ac - b^2}}{2a}, & \text{falls } b^2 - 4ac < 0. \end{cases}$$

Beweis.

Mit „quadratischer Ergänzung“, siehe Literatur. □

Beispiel

- Die Nullstellen von

$$p(\lambda) = -\lambda^2 + \lambda + 2$$

sind

$$\lambda_1 = \frac{-1 + \sqrt{1+8}}{-2} = -1 \quad \text{und} \quad \lambda_2 = \frac{-1 - \sqrt{1+8}}{-2} = 2.$$

- Die Nullstellen von

$$p(\lambda) = \lambda^2 + 2\lambda + 2$$

sind

$$\lambda_1 = \frac{-2 + \mathrm{i}\sqrt{8-4}}{2} = -1+\mathrm{i} \text{ und } \lambda_2 = \frac{-2 - \mathrm{i}\sqrt{8-4}}{2} = -1-\mathrm{i}\,.$$

Algebraische Grundlagen der Informatik

SoSe 2024

KAPITEL V: Eigenwerte und Eigenvektoren

3. Diagonalisierbarkeit

Dozentin: Prof. Dr. Agnes Radl

Email: agnes.radl@informatik.hs-fulda.de

Diagonalisierbarkeit

Definition

Eine Matrix $A \in \mathbb{K}^{n \times n}$ heißt diagonalisierbar, wenn es eine invertierbare Matrix $S \in \mathbb{K}^{n \times n}$ gibt, so dass

$$S^{-1}AS$$

eine Diagonalmatrix ist.

Charakterisierung von Diagonalisierbarkeit

Satz (ohne Beweis)

Eine Matrix $A \in \mathbb{C}^{n \times n}$ ist genau dann diagonalisierbar, wenn für jedes $\lambda \in \sigma_{\mathbb{C}}(A)$ gilt: $V_g(A, \lambda) = V_a(A, \lambda)$

In diesem Fall gibt es eine Basis von $\mathbb{C}^n$ aus Eigenvektoren von A.

Ist $\mathcal{B} = \{b_1, \ldots, b_n\}$ eine Basis von $\mathbb{C}^n$ aus Eigenvektoren von A und ist $S := (b_1 \cdots b_n) \in \mathbb{C}^{n \times n}$, so ist

$$S^{-1}AS = \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \lambda_n \end{pmatrix},$$

wobei λ_k der zu b_k gehörende Eigenwert ist.

Klassen diagonalisierbarer Matrizen

Man kann zeigen, dass folgende Matrizen immer diagonalisierbar sind:

- Diagonalmatrizen
- Matrizen in $\mathbb{C}^{n \times n}$ mit n verschiedenen Eigenwerten.
- symmetrische Matrizen in $\mathbb{R}^{n \times n}$
  (Eine Matrix $A = (a_{ij}) \in \mathbb{R}^{n \times n}$ ist symmetrisch, falls $a_{ij} = a_{ji}$ für alle $i, j \in \{1, \ldots, n\}$ gilt.)
- hermitesche Matrizen in $\mathbb{C}^{n \times n}$
  (Eine Matrix $A = (a_{ij}) \in \mathbb{C}^{n \times n}$ ist hermitesch, falls $a_{ij} = \overline{a_{ji}}$ für alle $i, j \in \{1, \ldots, n\}$ gilt.)
- normale Matrizen in $\mathbb{C}^{n \times n}$
  (Eine Matrix $A = (a_{ij}) \in \mathbb{C}^{n \times n}$ ist normal, falls $AA^* = A^*A$ gilt, wobei $A^* = (\overline{a_{ji}})$.)
- orthogonale Matrizen in $\mathbb{C}^{n \times n}$
  (Eine Matrix $A = (a_{ij}) \in \mathbb{C}^{n \times n}$ ist orthogonal, falls A invertierbar und $A^{-1} = A^T$, wobei $A^T = (a_{ji})$ die Transponierte bezeichnet.)

Algebraische Grundlagen der Informatik

SoSe 2024

KAPITEL VI: Abstände und Winkel in $\mathbb{R}^n$

1. Norm und Skalarprodukt

Dozentin: Prof. Dr. Agnes Radl

Email: agnes.radl@informatik.hs-fulda.de

Die Norm eines Vektors im $\mathbb{R}^n$

Definition

Ist $x = (x_1, \ldots, x_n)^T \in \mathbb{R}^n$, so ist

$$\|x\| := \sqrt{x_1^2 + \cdots + x_n^2} \in [0, \infty)$$

die (euklidische) Norm von x.

Bemerkung

Die Norm eines Vektors interpretiert man oft als den „Abstand von x zu $0_{\mathbb{R}^n}$“ bzw. als „Länge von x“.

Beispiel

- $\|\left(\begin{smallmatrix} 1 \\ 2 \end{smallmatrix}\right)\| = \sqrt{1^2 + 2^2} = \sqrt{5}$
- $\left\|\begin{pmatrix} -1 \\ 2 \\ -3 \end{pmatrix}\right\| = \sqrt{(-1)^2 + 2^2 + (-3)^2} = \sqrt{14}$

Eigenschaften der Norm

Seien $x, y \in \mathbb{R}^n$. Dann gelten:

- $\|x\| = 0 \Leftrightarrow x = 0_{\mathbb{R}^n}$,
- $\|\lambda x\| = |\lambda| \, \|x\|$ für alle $\lambda \in \mathbb{R}$,
- $\|x + y\| \leq \|x\| + \|y\|$. („Dreiecksungleichung“)

Ziel

Was ist der Winkel zwischen zwei Vektoren?

Skalarprodukt im $\mathbb{R}^n$

Definition

Für $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \in \mathbb{R}^n$ definieren wir das (Standard-)Skalarprodukt von x und y durch

$$\langle x, y \rangle := \sum_{k=1}^{n} x_k y_k.$$

Beispiel

$$\left\langle \begin{pmatrix} -1 \\ 2 \\ -3 \end{pmatrix}, \begin{pmatrix} 4 \\ 5 \\ -6 \end{pmatrix} \right\rangle = (-1) \cdot 4 + 2 \cdot 5 + (-3) \cdot (-6) = 24$$

Beobachtung

Für $x \in \mathbb{R}^n$ ist $\|x\| = \sqrt{\langle x, x \rangle}$.

Eigenschaften des Skalarprodukts

- Für alle $x \in \mathbb{R}^n$ gilt $\langle x, x \rangle \geq 0$;
  außerdem $\langle x, x \rangle = 0 \Leftrightarrow x = 0_{\mathbb{R}^n}$. („positiv definit“)
- Für alle $x, y \in \mathbb{R}^n$ gilt $\langle x, y \rangle = \langle y, x \rangle$. („symmetrisch“)
- Für alle $x, y, z \in \mathbb{R}^n$ und alle $\alpha, \beta \in \mathbb{R}$ gelten
  - $\langle \alpha x + \beta y, z \rangle = \alpha \langle x, z \rangle + \beta \langle y, z \rangle$
  - $\langle x, \alpha y + \beta z \rangle = \alpha \langle x, y \rangle + \beta \langle x, z \rangle$

  („bilinear“)

Cauchy-Schwarz-Ungleichung

Satz (Cauchy-Schwarz-Ungleichung)

Für $x, y \in \mathbb{R}^n$ gilt:

$$|\langle x, y \rangle| \leq \|x\| \, \|y\| \, .$$

Es gilt $|\langle x, y \rangle| = \|x\| \, \|y\|$ genau dann, wenn x und y linear abhängig sind.

Beweis.
siehe Literatur. □

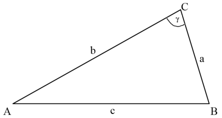
Folgerung

Für alle $x, y \in \mathbb{R}^n \setminus \{0_{\mathbb{R}^n}\}$ ist

$$\frac{\langle x, y \rangle}{\|x\| \, \|y\|} \in [-1, 1].$$

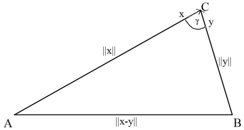
Erinnerung (Kosinussatz aus der Schule)

$$c^2 = a^2 + b^2 - 2ab\cos(\gamma)$$



bzw.

$$\begin{aligned} &\|x-y\|^2 \\ &= \|x\|^2 + \|y\|^2 - 2\,\|x\|\,\|y\|\cos(\gamma) \end{aligned}$$



Umformen ergibt $\cos(\gamma) = \frac{\langle x,y\rangle}{\|x\|\|y\|}$.

Definition

Für $x, y \in \mathbb{R}^n \setminus \{0_{\mathbb{R}^n}\}$ heißt

$$\varphi(x,y) := \arccos\left(\frac{\langle x,y\rangle}{\|x\|\,\|y\|}\right) \in [0,\pi]$$

der von x und y eingeschlossene Winkel.

Algebraische Grundlagen der Informatik

SoSe 2024

KAPITEL VI: Abstände und Winkel in $\mathbb{R}^n$

2. Orthogonalität

Dozentin: Prof. Dr. Agnes Radl

Email: `agnes.radl@informatik.hs-fulda.de`

Orthogonal und parallel

Definition

- $x, y \in \mathbb{R}^n$ sind orthogonal, falls $\langle x, y \rangle = 0$.
  Notation: $x \perp y$
- $x, y \in \mathbb{R}^n$ sind parallel, falls $x = \lambda y$ für ein $\lambda \in \mathbb{R}$.
  Notation: $x \| y$

Orthogonalprojektion

Satz (und Definition)

Sei $v \in \mathbb{R}^n \setminus \{0_{\mathbb{R}^n}\}$. Jedes $x \in \mathbb{R}^n$ kann bezüglich v eindeutig in zwei zueinander orthogonale Komponenten $x_{p,v}$ und $x_{o,v}$ zerlegt werden, so dass

$$x = x_{p,v} + x_{o,v} \quad \text{und} \quad x_{p,v} \| v, \quad x_{o,v} \perp v.$$

Dabei ist

$$x_{p,v} = \frac{\langle x, v \rangle}{\langle v, v \rangle} v \quad \text{und} \quad x_{o,v} = x - x_{p,v} = x - \frac{\langle x, v \rangle}{\langle v, v \rangle} v.$$

Man bezeichnet $x_{p,v}$ als orthogonale Projektion von x in Richtung v und $x_{o,v}$ als das orthogonale Komplement von x in Richtung v.

Bemerkung

Dieser Satz ist die Grundlage für die Abstandsberechnung zwischen Punkten, Geraden und Ebenen.

Orthogonale Matrizen

Definition

Eine Matrix $A \in \mathbb{R}^{n \times n}$ heißt orthogonal, falls

$$AA^T = A^T A = I$$

gilt, das heißt, A ist invertierbar und $A^{-1} = A^T$.

Bemerkung

Eine orthogonale Matrix A erhält Abstände und Winkel, denn für alle $x, y \in \mathbb{R}^n$ gilt

- $\langle Ax, Ay \rangle = x^T A^T Ay = x^T A^{-1} Ay = x^T y = \langle x, y \rangle$,
- $\|Ax\|^2 = \langle Ax, Ax \rangle = \langle x, x \rangle = \|x\|^2$.

Beispiele für orthogonale Matrizen

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

  (Drehung in $\mathbb{R}^2$ um den Winkel α gegen den Uhrzeigersinn.)

- $S_\alpha = \begin{pmatrix} \cos(2\alpha) & \sin(2\alpha) \\ \sin(2\alpha) & -\cos(2\alpha) \end{pmatrix}$

  (Spiegelung in $\mathbb{R}^2$ an der Ursprungsgeraden, die durch $\begin{pmatrix} \cos(\alpha) \\ \sin(\alpha) \end{pmatrix}$ geht.)

Orthogonale Vektoren in $\mathbb{R}^2$

Bemerkung

Ist $v = \begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{R}^2$, so sind zum Beispiel die Vektoren $\begin{pmatrix} -b \\ a \end{pmatrix}$ und $\begin{pmatrix} b \\ -a \end{pmatrix}$ orthogonal zu v.

Vektorprodukt im $\mathbb{R}^3$

Definition

Sind $v = \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix}, w = \begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix} \in \mathbb{R}^3$, so ist das Vektorprodukt oder Kreuzprodukt von v und w der Vektor

$$v \times w := \begin{pmatrix} v_2 w_3 - v_3 w_2 \\ v_3 w_1 - v_1 w_3 \\ v_1 w_2 - v_2 w_1 \end{pmatrix} \in \mathbb{R}^3.$$

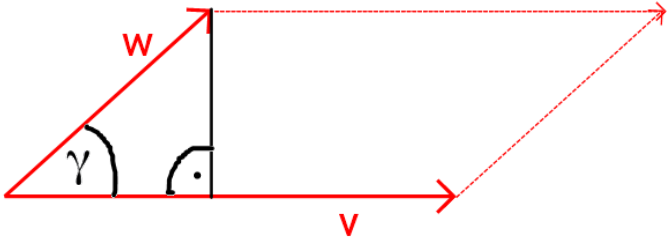
Bemerkung

Sind $v, w \in \mathbb{R}^3$, so prüft man leicht nach, dass gilt:

- $v \times w \perp v$,
- $v \times w \perp w$.

Flächeninhalt eines Parallelogramms in $\mathbb{R}^3$

Seien $v, w \in \mathbb{R}^3 \setminus \{0_{\mathbb{R}^3}\}$.



Der Flächeninhalt des von v und w aufgespannten Parallelogramms ist

$$A_{Parallelogramm} = \|v\| \, \|w\| \, |\sin(\gamma)| \,.$$

Zusammenhang zum Vektorprodukt

Erinnerung: Seien $v, w \in \mathbb{R}^3 \setminus \{0_{\mathbb{R}^3}\}$ und γ der Winkel zwischen v und w. Dann gilt $\cos(\gamma) = \frac{\langle v,w\rangle}{\|v\|\|w\|}$ bzw.

$$\langle v, w\rangle^2 = \|v\|^2 \|w\|^2 \cos^2(\gamma). \quad (*)$$

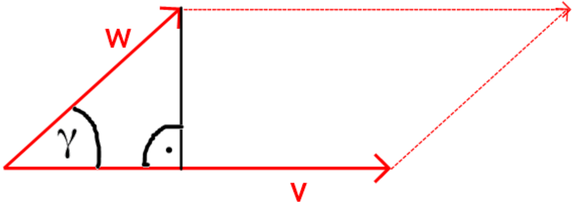
Damit erhält man

$$\begin{aligned}
\|v \times w\|^2 &\overset{\text{nachrechnen}}{=} \|v\|^2 \|w\|^2 - \langle v, w\rangle^2 \\
&\overset{(*)}{=} \|v\|^2 \|w\|^2 - \|v\|^2 \|w\|^2 \cos^2(\gamma) \\
&= \|v\|^2 \|w\|^2 (1 - \cos^2(\gamma)) \\
&\overset{\text{trig. Pyth.}}{=} \|v\|^2 \|w\|^2 \sin^2(\gamma).
\end{aligned}$$

Daraus folgt

$$\|v \times w\| = \|v\| \|w\| |\sin(\gamma)| .$$

Flächeninhalt eines Parallelogramms in $\mathbb{R}^3$



Fazit

Die Norm des Vektorprodukts von v und w gibt den Flächeninhalt des von v und w erzeugten Parallelogramms in $\mathbb{R}^3$ an:

$$A_{\text{Parallelogramm}} = \|v\| \, \|w\| \, |\sin(\gamma)| = \|v \times w\| \, .$$

Flächeninhalt eines Parallelogramms in $\mathbb{R}^2$

Seien $v = \left(\begin{smallmatrix} v_1 \\ v_2 \end{smallmatrix}\right), w = \left(\begin{smallmatrix} w_1 \\ w_2 \end{smallmatrix}\right) \in \mathbb{R}^2$.

Um den Flächeninhalt des von v und w erzeugten Parallelogramms zu bestimmen, „betten wir zunächst v und w in $\mathbb{R}^3$ ein“:

- Statt $v \in \mathbb{R}^2$ betrachte $\tilde{v} := \begin{pmatrix} v_1 \\ v_2 \\ 0 \end{pmatrix} \in \mathbb{R}^3$.
- Statt $w \in \mathbb{R}^2$ betrachte $\tilde{w} := \begin{pmatrix} w_1 \\ w_2 \\ 0 \end{pmatrix} \in \mathbb{R}^3$.

Der Flächeninhalt ergibt sich nun zu

$$A_{\text{Parallelogramm}} = \|\tilde{v} \times \tilde{w}\| = \left\| \begin{pmatrix} 0 \\ 0 \\ v_1 w_2 - v_2 w_1 \end{pmatrix} \right\| = |v_1 w_2 - v_2 w_1| \, .$$

Fazit

Der Flächeninhalt des von v und w aufgespannten Parallelogramms ist

$$A_{\text{Parallelogramm}} = |v_1 w_2 - v_2 w_1| = \left| \det \begin{pmatrix} v_1 & w_1 \\ v_2 & w_2 \end{pmatrix} \right| .$$