Assoziativ	Kommutativ	Distributiv	Neutrales Element (nur 1)	Inverses Element (für jedes Element)
$(x \circ y) \circ z = x \circ (y \circ z).$	$x \circ y = y \circ x.$	$a \circ (b+c) = a \circ b + a \circ c$ $(b+c) \circ a = b \circ a + c \circ a.$	$\varepsilon \circ x = x \circ \varepsilon = x.$	$a \circ b = b \circ a = \varepsilon.$

Abelsche, Kommutatuve => Vorbedingungen + Kummutativ

Name	Assoziativ	Kommutativ	Neutrales Element	Inverses Element
Halbgruppe	X			
Monoid	X		X	
Gruppe	X		X	X
Abelsche Gruppe	X	X	X	X

Satz

Alle Permutationen einer Menge M bilden mit der Hintereinanderausführung $\circ$ eine Gruppe, die die symmetrische Gruppe von M genannt wird, in Zeichen S_M.

Name	+	o	Distributiv
Ring	Abelsche Gruppe	Halbgruppe	X
Ring mit Einselement	Abelsche Gruppe	Monoid	X
Kommutativer Ring	Abelsche Gruppe	Abelsche Halbgruppe	X
Körper	Abelsche Gruppe	Abelsche Gruppe(Menge ohne 0)	X

Restklassenoperationen

$[\mathbb{Z}_n, +, \cdot]$ *ist ein kommutativer Ring mit Einselement.*

$a \in \mathbb{Z}_n$ *ist invertierbar* $\iff \operatorname{ggT}(a, n) = 1 \quad$ *(a und n teilerfremd).*

If n prim => invertierbat

Falls p eine Primzahl ist, dann ist $[\mathbb{Z}_p, +, \cdot]$ ein (endlicher) Körper.

EEA2

r	s	t	q
37	1	0	
27	0	1	1

27 passt 1 mal in 37
Die obere zeile 1 mal von der unteren abziehen

EEA1

1. Bestimme die Kofaktoren s und t so, dass
$$1 = \operatorname{ggT}(a, n) = s \cdot n + t \cdot a$$
2. Also $1 - t \cdot a = s \cdot n$, d.h. $1 \sim_n t \cdot a$ und somit
$$[t]_n \cdot [a]_n = [t \cdot a]_n = [1]_n$$
3. Daher: $[a]_n^{-1} = [t]_n$. Man schreibt auch $a^{-1} = t \pmod n$.

Erweiterter Euklidischer Algorithmus(EEA)

a ist invertierbar in Modulo n(Beispiel a = 27 und n = 37) $[27]_{37}^{-1}$

In unserem Beispiel: aus $1 = -8 \cdot 37 + 11 \cdot 27$ folgt $[27]_{37}^{-1} = [11]_{37}$.
In der Tat gilt: $27 \cdot 11 = 297 = 1 \quad$ (modulo 37).

EEA3

r	s	t	q
37	1	0	
27	0	1	1
10	1	-1	2

10 passt 2 mal in 27
Die obere Zeile 2 mal von der unteren abziehen =>
Wiederholen bis r = 0, die Zeile darüber gibt s und t aus.

Sei $p \in \mathbb{N}$ eine Primzahl. Für jedes $a \in \mathbb{Z}_p \setminus \{0\}$ gilt:
$$a^{p-1} \sim_p 1 \qquad \text{d.h.} \qquad [a]_p^{p-1} = [1]_p.$$

Sei $n = p \cdot q$ für zwei (unterschiedliche) Primzahlen $p, q \in \mathbb{N}$. Falls $a \in \mathbb{Z}_n$ teilerfremd zu n ist, d.h. $\operatorname{ggT}(a, n) = 1$, dann gilt:
$$a^{(p-1)(q-1)} \sim_n 1 \qquad \text{bzw.} \qquad [a]_n^{(p-1)(q-1)} = [1]_n.$$

r	s	t	q
37	1	0	
27	0	1	1
10	1	-1	2
7	-2	3	1
3	3	-4	2
1	-8	11	3
0			

Komplexe Zahlen

$\mathbb{C} := \{x + yi \mid x, y \in \mathbb{R}\}$	Menge der komplexen Zahlen
$\operatorname{Re}(z) := x$	Realteil von z
$\operatorname{Im}(z) := y$	Imaginärteil von z
$\lvert z\rvert := \sqrt{x^2 + y^2}$	Absolutbetrag von z
$\bar{z} := x - yi$	konjugiert komplexe Zahl zu z

Gegeben: $a, b, c \in \mathbb{C}$, $a \neq 0$
Gesucht: $x \in \mathbb{C}$, so dass $ax^2 + bx + c = 0$

Lösungsformel für quadratische Gleichungen funktioniert auch in $\mathbb{C}$:
$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

- $p = (a, b) = a + bi = [r; \varphi] = r \cdot (\cos(\varphi) + i \sin(\varphi))$
- Spiegelung an der x-Achse: $p \mapsto a - bi = \bar{p}$
- Spiegelung am Nullpunkt: $p \mapsto -a - bi = -p$
- Verschiebung um $t = (c, d)$: $p \mapsto (a + c) + (b + d)i = p + t = p'$
- Drehung um ω um den Nullpunkt: $p \mapsto [r; \varphi + \omega] = p \cdot [1; \omega] = p''$

$$i^2 = -1,\ i^3 = -i,\ i^4 = 1,\ i^5 = i,\ i^{-1} = \frac{1}{i} = -i$$

$$x = r\cos(\varphi), \quad y = r\sin(\varphi)$$

$$z_1 = [r_1; \varphi_1]$$
$$z_2 = [r_2; \varphi_2]$$

Multiplikation
$$z_1 z_2 = [r_1 r_2; \varphi_1 + \varphi_2]$$

Division
$$\frac{z_1}{z_2} = \left[\frac{r_1}{r_2}; \varphi_1 - \varphi_2\right]$$

$$z^n = [r^n; n\varphi] = r^n \cdot (\cos(n\varphi) + i \sin(n\varphi)).$$

$$r = \sqrt{x^2 + y^2} = |z|, \quad \varphi = \arctan\left(\frac{y}{x}\right) \quad (\text{ggf. } +\pi \text{ oder } +2\pi)$$

Matrix

Hoch t => transponiert => gespiegelt um die Diagonale

Für die Multiplikation Tabelle verwenden

Wurzelziehen in $\mathbb{C}$

Algorithmus

Eingabe: $z \in \mathbb{C}$, $n \in \mathbb{N}$
Ausgabe: $L = \{ u \in \mathbb{C} \mid u^n = z \}$

1. Bestimme r und φ, so dass $z = r \cdot (\cos(\varphi) + i \sin(\varphi)) = [r; \varphi]$.
2. $L := \left\{ \sqrt[n]{r} \left(\cos\left(\frac{\varphi + 2k\pi}{n}\right) + i \sin\left(\frac{\varphi + 2k\pi}{n}\right) \right) \;\middle|\; k = 0, \ldots, n-1 \right\}$

Beispiel

Wir berechnen die dritten Wurzeln ($n = 3$) von $z = -2 + 2i$. Dazu wandeln wir z in die Polarkoordinatendarstellung um: $z = [\sqrt{8}; \frac{3\pi}{4}]$.
$$L = \left\{ \sqrt[3]{\sqrt{8}} \cdot \left(\cos\left(\tfrac{\pi}{4} + \tfrac{2k\pi}{3}\right) + i \sin\left(\tfrac{\pi}{4} + \tfrac{2k\pi}{3}\right) \right) \;\middle|\; k = 0, 1, 2 \right\}$$
$$= \left\{ [\sqrt{2}; \tfrac{\pi}{4}],\ [\sqrt{2}; \tfrac{11\pi}{12}],\ [\sqrt{2}; \tfrac{19\pi}{12}] \right\}$$
$$= \left\{ 1 + i,\ \tfrac{\sqrt{3}-1}{2} - i\tfrac{\sqrt{3}+1}{2},\ -\tfrac{\sqrt{3}+1}{2} + i\tfrac{\sqrt{3}-1}{2} \right\}.$$

Quadratische Wurzel in $\mathbb{C}$

- Wurzelziehen allgemein: verwende Polarkoordinaten!
- Spezialfall $n = 2$: auch in kartesischen Koordinaten möglich.
- Der folgende Algorithmus verwendet nur die Grundoperationen $+, -, \cdot, :, \sqrt{\ }$ in $\mathbb{R}$.

Algorithmus

Eingabe: $x, y \in \mathbb{R} \quad (z = x + yi \in \mathbb{C})$
Ausgabe: $w \in \mathbb{C}$, so dass $w^2 = x + yi = z$

1. $u := \sqrt{\frac{1}{2}(x + \sqrt{x^2 + y^2})}$
2. $v := \sqrt{\frac{1}{2}(-x + \sqrt{x^2 + y^2})}$
3. if $y \geq 0$ then $w := u + vi$ else $w := u - vi$
4. Zweite Lösung für $z \neq 0$: $w' := -w$.

$(A + B) + C = A + (B + C)$	$(A \cdot B) \cdot C = A \cdot (B \cdot C)$
$A + 0 = 0 + A = A$	$A \cdot E = E \cdot A = A$
$A \cdot (B + C) = A \cdot B + A \cdot C$	$(B + C) \cdot A = B \cdot A + C \cdot A$
$A + (-A) = (-A) + A = 0$	$A + B = B + A$
$(\lambda \cdot A) \cdot B = \lambda \cdot (A \cdot B)$	$(A \cdot B)^t = B^t \cdot A^t$

Der (i, j)-Eintrag von $A \cdot B$ ist das Produkt der i-ten Zeile von A mit der j-ten Spalte von B. Merkregel: „Zeile mal Spalte".

Schematisch: $\begin{pmatrix} \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ * & * & * & * \\ \cdot & \cdot & \cdot & \cdot \end{pmatrix} \cdot \begin{pmatrix} \cdot & * & \cdot & \cdot \\ \cdot & * & \cdot & \cdot \\ \cdot & * & \cdot & \cdot \\ \cdot & * & \cdot & \cdot \end{pmatrix} = \begin{pmatrix} \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & * & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{pmatrix}$

Invertierbare Matrizen

Definition (Invertierbarkeit)

Sei A eine $(n \times n)$-Matrix. A heißt invertierbar (regulär) :⇔ $\underset{B \in \mathbb{R}^{n \times n}}{\exists} \quad A \cdot B = B \cdot A = E_n.$

Falls A invertierbar:

$$A^{-1} := \text{ diejenige Matrix } B \text{ mit } A \cdot B = B \cdot A = E.$$

A^{-1} heißt „die Inverse (Matrix) von A".

Invertieren => Gaus auf Matrix und Einheitsmatrix

Seien A und B zwei reguläre Matrizen. Dann gilt:

1. $(A^{-1})^{-1} = A$
2. $(A^t)^{-1} = (A^{-1})^t$
3. $(A \cdot B)^{-1} = B^{-1} \cdot A^{-1}$

Entwicklung nach zweiter Zeile:

$$\begin{vmatrix} 1 & -3 & 4 \\ 0 & 2 & 0 \\ 5 & 0 & -1 \end{vmatrix} = -0 \cdot \begin{vmatrix} -3 & 4 \\ 0 & -1 \end{vmatrix} + 2 \cdot \begin{vmatrix} 1 & 4 \\ 5 & -1 \end{vmatrix} - 0 \cdot \begin{vmatrix} 1 & -3 \\ 5 & 0 \end{vmatrix}$$
$$= 2 \cdot \left(1 \cdot \left|-1\right| + (-1) \cdot 4 \cdot \left|5\right|\right)$$
$$= 2 \cdot (1 \cdot (-1) + (-1) \cdot 4 \cdot 5)$$
$$= -42$$

← Mit TR prüfen

Sei A eine $(n \times n)$-Matrix. Dann gilt:

$$A \text{ ist regulär} \iff |A| \neq 0.$$

Determinante => Volumensänderung

Seien A und B zwei quadratische Matrizen. Dann gilt:

1. $|A^t| = |A|$
2. $|A^{-1}| = |A|^{-1}$ (falls A regulär ist)
3. $|A \cdot B| = |A| \cdot |B|$

Beachte dabei das Vorzeichenmuster:
$$\begin{vmatrix} + & - & + & - & \cdots \\ - & + & - & + & \cdots \\ + & - & + & - & \cdots \\ - & + & - & + & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{vmatrix}$$

Falls $n = 2$: „Hauptdiagonale minus Nebendiagonale":

$$|A| = A_{1,1}A_{2,2} - A_{1,2}A_{2,1}$$

Falls $n = 3$: Regel von Sarrus:

$$|A| = A_{1,1}A_{2,2}A_{3,3} + A_{1,2}A_{2,3}A_{3,1} + A_{1,3}A_{2,1}A_{3,2} - A_{1,3}A_{2,2}A_{3,1} - A_{1,1}A_{2,3}A_{3,2} - A_{1,2}A_{2,1}A_{3,3}$$

Schematisch:

$$\searrow + \searrow + \searrow - \swarrow - \swarrow - \swarrow$$
$$\begin{vmatrix} A_{1,1} & A_{1,2} & A_{1,3} \\ A_{2,1} & A_{2,2} & A_{2,3} \\ A_{3,1} & A_{3,2} & A_{3,3} \end{vmatrix} \begin{matrix} A_{1,1} & A_{1,2} \\ A_{2,1} & A_{2,2} \\ A_{3,1} & A_{3,2} \end{matrix}$$

Dreieicksmatrix => Deteminante ist Produkt von Diagonale
Gaus => ändert determinate nicht, vertauschen => mal -1

Eine algebraische Struktur $[(V,K),+,\oplus,\otimes,\cdot]$ ist ein Vektorraum :⟺

1. $[V,+]$ *ist eine abelsche Gruppe,*
2. $[K,\oplus,\otimes]$ *ist ein Körper,*
3. $\cdot : K \times V \to V$,

   für alle $\lambda, \lambda_1, \lambda_2 \in K$ *und* $v, v_1, v_2 \in V$:
4. $\lambda \cdot (v_1 + v_2) = \lambda \cdot v_1 + \lambda \cdot v_2$,
5. $(\lambda_1 \oplus \lambda_2) \cdot v = \lambda_1 \cdot v + \lambda_2 \cdot v$,
6. $(\lambda_1 \otimes \lambda_2) \cdot v = \lambda_1 \cdot (\lambda_2 \cdot v)$,
7. $1 \cdot v = v$.

2. *A heißt linear unabhängig (l.u.) :⟺*
$$\underset{\lambda_1,\ldots,\lambda_k \in K}{\forall} \left(\sum_{i=1}^{k} \lambda_i a_i = 0 \implies \underset{1 \leq i \leq k}{\forall} \lambda_i = 0\right).$$
3. *A heißt linear abhängig (l.a.) :⟺ A ist nicht l.u.* ⟺
$$\underset{\lambda_1,\ldots,\lambda_k \in K}{\exists} \left(\sum_{i=1}^{k} \lambda_i a_i = 0 \wedge \underset{1 \leq i \leq k}{\exists} \lambda_i \neq 0\right).$$

1. $U \neq \emptyset$

   und für alle $v_1, v_2 \in U$ *und* $\lambda \in K$:
2. $v_1 + v_2 \in U$ *(Abgeschlossenheit bzgl. +)*
3. $\lambda v_1 \in U$ *(Abgeschlossenheit bzgl. ·)*

Manigfaltigkeit => Unterraum um Vektor verschoben

$$v \cdot w := \sum_{i=1}^{n} v_i w_i. \qquad \|v\| := \sqrt{v \cdot v}. \qquad d(v,w) := \|v - w\| \quad \left(= \sqrt{(v_1 - w_1)^2 + \cdots + (v_n - w_n)^2}\right)$$

$$\cos(\alpha) = \frac{v \cdot w}{\|v\| \cdot \|w\|}. \qquad v_i' := \frac{1}{\|v_i\|} v_i. \qquad v_i := b_i - \sum_{j=1}^{i-1} \mathrm{proj}_{v_j}(b_i)$$

Orthogonal => rechte winkel
normal => Länge = 1

$$v \perp w :\iff v \cdot w = 0.$$

$$\mathrm{proj}_w(v) := \frac{v \cdot w}{\|w\|^2} w$$

Sei $\{b_1, \ldots, b_r\}$ eine ONB von U (zumindest orthogonal!)

$$p := \sum_{j=1}^{r} \mathrm{proj}_{b_j}(v)$$

Matrixrang => Zeilen/Spalten ohne 0 Vektor

$$\underset{\substack{\uparrow \\ \text{partikuläre Lösung} \\ \text{des inhomogenen} \\ \text{Systems}}}{LM(A,b) = p} + \underset{\substack{\uparrow \\ \text{alle Lösungen} \\ \text{des homogenen} \\ \text{Systems}}}{LM(A,0)}$$

$LM(A,b)$ ist also eine lineare Mannigfaltigkeit im $\mathbb{R}^n$.

Allgemeine Lösung des homogenen Systems $(A,0)$:

$$LM(A,0) = \{x \in \mathbb{R}^n \mid A \cdot x = 0\}$$

ist ein Untervektorraum des $\mathbb{R}^n$ mit Dimension $n - r$.
Jede Linearkombination von Lösungen des homogenen Systems ist wieder eine Lösung des homogenen Systems.

n => Variablen
r => Rang
n – r => Variablen in der Lösungsmenge
=> Dimension der Lösungsmenge

Linare Optimierung

Standartform(alles auf kleiner gleich und dann auf = mit + y => Simplex(größte Endspalte, kleinster quotient => 0, einheitsvektor => Tausch => Repeat
Unteres spallte überall - => perfekt, 0 kreislauf => unendlich, geht nix mehr => keine