

Inhaltsverzeichnis

| | |
|--|----------|
| Komplexe Zahlen | 1 |
| Polarkoordinaten | 2 |
| Lineare Gleichungssysteme | 3 |
| Vereinfachte Schreibweise als Matrix: | 3 |
| Umformen in ZNF: | 3 |
| Rang einer Matrix | 4 |
| Matrix | 4 |
| Besondere Matrizen | 4 |
| Rechenoperationen | 6 |
| Elementarmatrizen | 8 |
| Rechenregeln Matrizen | 8 |
| Gruppen | 10 |
| Untergruppen | 10 |
| Von Elementen erzeugten Untergruppen | 10 |
| Ordnung eines Elements | 11 |
| Sätze von Lagrange und Euler | 11 |
| Die Restklassen modulo n: | 11 |
| Ringe | 12 |
| Einheitengruppe (= Gruppe der invertierbaren Elemente) | 12 |
| Prime Restklassengruppen | 12 |
| Euklidischer Algorithmus | 12 |
| Erweiterte Euklidischer Algorithmus | 13 |
| Berechnung | 13 |
| Eulersche φ -Funktion: | 13 |
| kleiner Satz von Fermat | 13 |
| Das Pohlig Hellman Verfahren | 13 |
| RSA-Verfahren: | 14 |
| Vektorräume | 14 |
| Körper | 14 |
| Sprechweisen und Regeln | 14 |
| Untervektorräume | 15 |
| Linearkombinationen | 15 |
| Das Erzeugnis von X | 15 |
| Lineare Unabhängigkeit: | 15 |
| Basen von Vektorräumen | 16 |
| Merkregeln | 16 |
| Anwendung in Linearen Gleichungssystemen | 16 |
| Spaltenraum | 17 |
| Lineare codes | 17 |
| Wie läuft das Dekodieren ab? | 18 |
| Hamming Gewicht und Abstand | 18 |
| Lineare Codes (Fortsetzung) | 18 |
| Die Kontrollmatrix (Parity Check Matrix) | 18 |
| Vorbereitung auf Determinante | 19 |
| Die Determinante: | 19 |

Komplexe Zahlen

Konstellation von \mathbb{C} :

$$\mathbb{R}^2 = \{(a, b) | a, b \in \mathbb{R}\}$$

$$(0, 1)^2 = -1$$

“imaginäre Einheit:”

$$(0, 1) = i$$

Andere Notation:

$$(a, b) \in \mathbb{R}^2 = (a, 0) + (0, b) = (a, 0) + (0, 1) \cdot (b, 0) = a + i \cdot b$$

$$\mathbb{C} = \{a + ib | a, b \in \mathbb{R}\}$$

Addition:

$$(a + ib) + (c + id) = (a + c) + i(b + d)$$

Multiplikation:

$$(a + ib) \cdot (c + id) = ac + i^2 bd + i(ad + bc) = ac - bd + i(ad + bc)$$

Begriffe:

$$Z = a + ib \in \mathbb{C}, a, b \in \mathbb{R}$$

$$a = \operatorname{Re}(Z)$$

$$b = \operatorname{Im}(Z)$$

wenn $a = 0 \rightarrow Z$ rein imaginär

$$Z = a + ib \rightarrow \overline{Z} = a - ib$$

\overline{Z} ist die zu Z konjugierte komplexe Zahl

Nützliches:

$$Z \cdot \overline{Z} = (a + ib) \cdot (a - ib) = a^2 + b^2$$

$$|Z| = \sqrt{a^2 + b^2}$$

$$\overline{Z + W} = \overline{Z} + \overline{W}$$

$$\overline{Z \cdot W} = \overline{Z} \cdot \overline{W}$$

$$\operatorname{Re}(Z) = \frac{1}{2}(Z + \overline{Z})$$

$$\operatorname{Im}(Z) = \frac{1}{2i}(Z - \overline{Z})$$

Dreiecksungleichung:

$$Z, W \in \mathbb{C} \Rightarrow |Z + W| \leq |Z| + |W|$$

Invertieren: (komplexe Zahl aus Nenner raus bekommen)

$$\frac{a+bi}{c+di} = \frac{a+bi}{c+di} \cdot \frac{c-di}{c-di} = \frac{ac+bd+i(cb-ad)}{c^2+d^2}$$

Polarkoordinaten

Form: $Z = r(\cos \varphi + i \sin \varphi)$

mit Radius $r \in \mathbb{R}$ und Winkel $\varphi \in]-\pi, \pi]$

Umrechnung:

- $Z = a + ib$

1. $r = \sqrt{a^2 + b^2}$

2. $\varphi = \begin{cases} \arccos \frac{a}{r}, b \geq 0 \\ -\arccos \frac{a}{r}, b < 0 \end{cases}$

3. $Z = r \cdot (\cos \varphi + i \sin \varphi)$

- $\cos\varphi = \frac{a}{r}$
- $\sin\varphi = \frac{b}{r}$

Multiplikation:

$$Z_1 = r_1(\cos(\varphi_1) + i \sin(\varphi_1))$$

$$Z_2 = r_2(\cos(\varphi_2) + i \sin(\varphi_2))$$

$$Z_1 \cdot Z_2 = r_1 \cdot r_2 \cdot (\cos(\varphi_1 + \varphi_2) + i \sin(\varphi_1 + \varphi_2))$$

Potenzen:

$$Z = r \cdot (\cos(\varphi) + i \sin(\varphi))$$

$$Z^n = r^n \cdot (\cos(n \cdot \varphi) + i \sin(n \cdot \varphi))$$

Wurzeln:

$\sqrt[n]{Z}$ hat genau n Lösungen

$$Z_k = \sqrt[n]{r} \cdot (\cos \frac{\varphi + 2\pi \cdot k}{n} + i \sin \frac{\varphi + 2\pi \cdot k}{n})$$

mit n = "Wurzelexponent",

r = "Radius",

k = "k-te Lösung der Wurzel von 0 bis $n - 1$ "

Lineare Gleichungssysteme

Vereinfachte Schreibweise als Matrix:

$$\begin{array}{c} \text{lineares Gleichungssystem LGS} \\ \begin{array}{ccccccc} a_{11}x_1 & + & \cdots & + & a_{1n}x_1 & = & b_1 \\ \vdots & + & \ddots & + & \vdots & = & \vdots \\ a_{m1}x_n & + & \cdots & + & a_{mn}x_n & = & b_m \end{array} \end{array} \Rightarrow \underbrace{\left(\begin{array}{ccc|c} a_{11} & \cdots & a_{1n} & b_1 \\ \vdots & \ddots & \vdots & \vdots \\ a_{m1} & \cdots & a_{mn} & b_m \end{array} \right)}_{(A|b)} \Rightarrow \cdots$$

$$\cdots \Rightarrow \left(\begin{array}{cccc|c} * & \cdots & \cdots & * & * \\ 0 & * & \cdots & * & \vdots \\ \vdots & 0 & * & * & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & \star \end{array} \right) \Rightarrow \cdots \Rightarrow \underbrace{\left(\begin{array}{cccc|c} 1 & * & \cdots & * & * \\ 0 & 1 & * & * & * \\ 0 & 0 & 1 & * & * \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 \end{array} \right)}_{\text{reduzierte Zeilenstufenform}}$$

*: unbekannter Wert

*: 0

*: wenn $\neq 0$ gibt es keine Lösung

Umformen in ZNF:

Elementare Zeilenumformungen $\left\{ \begin{array}{l} \text{Vertauschen zweier Zeilen} \\ \text{Multiplikation einer Zeile mit } \lambda \neq 0 \\ \text{Addition des } \lambda\text{-fachen einer Zeile zu einer anderen} \end{array} \right.$

Rang einer Matrix

Matrix M auf ZSF bringen

\Rightarrow Anzahl an nicht null Zeilen = Rang von $M = rg(M)$

Das Kriterium für Lösbarkeit:

- Das System ist genau dann lösbar, wenn: $rg(A) = rg(A|b)$
- ist das LGS lösbar, so gilt: Anzahl frei wählbaren Variablen = $n - r$

n = Anzahl der variablen und $r = rg(A)$

- ist das System $(A|b)$ lösbar, so gilt: $\exists_1 \text{ lsg} \Leftrightarrow n = r$

Matrix

$$A = \underbrace{\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}}_{n \text{ Spalten}} \left. \vphantom{\begin{pmatrix} a_{11} \\ \vdots \\ a_{m1} \end{pmatrix}} \right\} m \text{ Zeilen}$$

Stelle (i, j) : i -te Zeile | j -te Spalte

$$\begin{array}{lcl} \mathbb{R}^{m \times n} & = \{(a_{ij})_{m,n} | a_{ij} \in \mathbb{R}\} & \Rightarrow \text{"reelle Matrix"} \\ \mathbb{C}^{m \times n} & = \{(a_{ij})_{m,n} | a_{ij} \in \mathbb{C}\} & \Rightarrow \text{"komplexe Matrix"} \end{array} \underbrace{\hspace{10em}}_{\Rightarrow K(\text{körper})^{m \times n} = \{(a_{ij})_{m,n} | a_{ij} \in K\}}$$

$A = B \Leftrightarrow$ gleich viele Spalten UND gleich viele Zeilen UND gleiche Einträge an den gleichen Stellen

Besondere Matrizen

- $m \times 1$: $S = \begin{pmatrix} S_1 \\ \vdots \\ S_m \end{pmatrix}$ Spaltenvektor
- $1 \times n$: $Z = (Z_1 \ \cdots \ Z_n)$ Zeilenvektor
- $m \times n$: $0 = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix}$ Nullmatrix
- $m = n$: quadratische Matrix

$$\text{Diagonalmatrix: } \text{diag}(\lambda_1 \dots \lambda_n) = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda_n \end{pmatrix}$$

$$\text{Einheitsmatrix: } E_n = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

$$\text{Obere } \Delta\text{-Matrix: } O = \begin{pmatrix} * & * & \dots & * \\ 0 & * & \dots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & * \end{pmatrix}$$

$$\text{Untere } \Delta\text{-Matrix: } U = \begin{pmatrix} * & 0 & \dots & 0 \\ * & * & \ddots & 0 \\ \vdots & \vdots & \dots & \vdots \\ * & * & \dots & * \end{pmatrix}$$

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \in K^{m \times n} = \left(\vec{S}_1, \quad \dots \quad \vec{S}_n \right) = \begin{pmatrix} Z_1 \\ \vdots \\ Z_m \end{pmatrix}$$

Rechenoperationen

Transponieren:

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

Symmetrische Matrix: $A^T = A$

Addieren:

$$A = (a_{ij})_{m,n}, B = (b_{ij})_{m,n}$$

$$A + B = (a_{ij} + b_{ij})_{m,n}$$

$$A = (a_{ij}) = -(-a_{ij}) = -(-A)$$

Skalare Multiplikation (Vervielfachen:)

$$A = (a_{ij})_{m,n} \in \mathbb{K}^{m \times n}$$

$$\lambda \in \mathbb{K}$$

$$\Rightarrow \lambda A = (\lambda a_{ij})$$

Multiplikation:

$$Z = (Z_1, \dots, Z_n) \quad , \quad S = \begin{pmatrix} S_1 \\ \vdots \\ S_n \end{pmatrix}$$

$$Z \cdot S = \sum_{i=1}^n Z_i S_i$$

\Downarrow

$$A = \begin{pmatrix} Z_1 \\ \vdots \\ Z_m \end{pmatrix} \in \mathbb{K}^{m \times n} \quad , \quad B = (S_1 \quad \cdots \quad S_p) \in \mathbb{K}^{n \times p}$$

$$A \cdot B := \begin{pmatrix} Z_1 \cdot S_1 & Z_1 \cdot S_2 & \cdots & Z_1 S_p \\ Z_2 \cdot S_1 & Z_2 \cdot S_2 & \cdots & Z_2 S_p \\ \vdots & \vdots & \ddots & \vdots \\ Z_m \cdot S_1 & Z_m \cdot S_2 & \cdots & Z_m \cdot S_p \end{pmatrix} \in K^{m \times p}$$

$A \cdot B \neq B \cdot A \leftarrow$ keine Kommutativität

$$A^k = \underbrace{A \cdot A \cdots A}_k$$

$$A^0 := E_n$$

Invertieren:

$$A \in K^{n \times n} \quad , \quad B = A^{-1}$$

$$A \cdot B = E_n = B \cdot A$$

Nicht jede Matrix invertierbar!

$$B = \begin{pmatrix} \vec{S}_1 & \dots & \vec{S}_n \end{pmatrix} \quad , \quad e_i = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}$$

$$A \cdot B = A \cdot \begin{pmatrix} \vec{S}_1 & \dots & \vec{S}_n \end{pmatrix} = \begin{pmatrix} A\vec{S}_1 & \dots & A\vec{S}_n \end{pmatrix} = (e_1 \quad \dots \quad e_n) = E_n$$

löse so:

$$(A|E_n) \Rightarrow \dots \text{el. ZUF} \dots \Rightarrow (E_n|A^{-1})$$

Elementarmartizen

Permutationsmatrizen (Vertauschen von Zeilen):

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

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

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

Multiplikation einer Zeile mit $\lambda \neq 0$:

$$D_k(\lambda) = \begin{pmatrix} 1 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ddots & 1 & 0 & 0 & \ddots & 0 \\ 0 & \ddots & 0 & \lambda & 0 & \ddots & 0 \\ 0 & \ddots & 0 & 0 & 1 & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 1 \end{pmatrix} \leftarrow k$$

Addition des λ -fachen der l -ten Zeile zur k -ten Zeile:

$$N_{kl}(\lambda) = \begin{pmatrix} 1 & \cdots & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \lambda & \vdots \\ 0 & \ddots & 1 & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & \cdots & 0 \end{pmatrix} \leftarrow \lambda \text{ an der } k\text{-ten Zeile und } l\text{-ten Spalte}$$

Rechenregeln Matrizen

Addition:

$$\begin{array}{l|l} A + B = B + A & \text{Kommutativitat} \\ (A + B) + C = (A + B) + C & \text{Assoziativitat} \\ (\mu \cdot \lambda)A = \mu(\lambda \cdot A) & \\ 0 + A = A = A + 0 & \text{Neutrales Element} \\ E_n A = A & \\ \forall A \exists B : A + B = 0 & \text{Inverses Element} \\ B = -A & \\ \lambda(A + B) = \lambda A + \lambda B & \text{Distributivitat} \end{array}$$

Transposition:

$$\begin{array}{l|l} (A + B)^T = A^T + B^T & \text{Summe} \\ (\lambda A)^T = \lambda A^T & \text{Skalarmultiplikation} \\ (A^T)^T = A & \text{Zweifache Transposition} \\ (AB)^T = B^T A^T & \text{Produkt} \\ (A^{-1})^T = (A^T)^{-1} & \text{Inverses} \end{array}$$

Multiplikation:

| | |
|--|-------------------|
| $\exists A, B : AB \neq BA$ | nicht kommutativ! |
| $(AB)C = A(BC)$ | Assoziativität |
| $\exists E \in E_n : EA = A$ | Neutrales Element |
| $A(B + C) = AB + AC$ | Distributivität |
| $(B + C)A = BA + CA$ | |
| $(A \cdot B)^{-1} = B^{-1} \cdot A^{-1}$ | Inverses |

Gruppen

G nichtleere Menge mit innerer Verknüpfung \cdot

$$\cdot : G \times G \rightarrow G$$

(G, \cdot) heißt Gruppe, wenn:

$$\left. \begin{array}{l} \forall a, b, c \in G : (a \cdot b) \cdot c = a \cdot (b \cdot c) \\ \exists e \in G : e \cdot a = a = a \cdot e \quad \forall a \in G \\ \forall a \in G \exists b \in G : a \cdot b = e = b \cdot a \end{array} \right\} \begin{array}{l} \text{Assoziativgesetz} \\ \text{neutrales Element} \\ \text{inverses Element} \end{array}$$

G nennt man abelsch (=kommutativ) falls:

$$\bullet \quad ab = ba \quad \forall a, b \in G$$

Untergruppen

(G, \cdot) sei eine Gruppe mit neutralem Element e

$U \subseteq G$ mit:

$$\left. \begin{array}{l} e \in U \\ u, v \in U \Rightarrow u \cdot v \in U \\ u \in U \Rightarrow u^{-1} \in U \end{array} \right\} \begin{array}{l} \text{neutrales Element} \\ \text{abgeschlossen} \\ \text{inverses Element} \end{array} \Rightarrow \left\{ \begin{array}{l} U \text{ ist Untergruppe} \\ U \leq G \end{array} \right.$$

Von Elementen erzeugten Untergruppen

$$\langle a \rangle = \{a^k \mid a \in G, k \in \mathbb{Z}\}$$

- $e \in \langle a \rangle$
- $a^k, a^l \in \langle a \rangle \Rightarrow a^k \cdot a^l = a^{k+l} \in \langle a \rangle$
- $a^k a^{-k} = a^0 = e$

Ordnung eines Elements

(G, \cdot) Gruppe $\rightarrow a \in G$

$$\rightarrow O(a) = |\langle a \rangle| = \begin{cases} n \in \mathbb{N}, & \# \{a^k \mid k \in \mathbb{Z}\} \\ \infty, & \text{sonst.} \end{cases}$$

$O(a)$ = kleinste Zahl n mit $a^n = e$

$$\langle a \rangle = \{e, a, \dots, a^{n-1}\}$$

$$O(a) = n$$

Satz über die Ordnung von Gruppenelementen:

Es sei G eine Gruppe mit neutralem Element e , und es sei $a \in G$:

(a) Falls $O(a) = \infty$, dann: $a^i \neq a^j$, $i \neq j$.

(b) Falls $O(a) \in \mathbb{N}$, so gilt: $O(a) = u$ = kleinste natürliche Zahl, für die $a^u = e$ gilt.

$$a^s = e \Leftrightarrow O(a) \mid s$$

Sätze von Lagrange und Euler

Satz von Lagrange:

G sei eine endliche Gruppe, $U \leq G$

Dann:

$$|U| \mid |G|$$

Satz von Euler:

$$a^{|G|} = e \quad \forall a \in G$$

Die Restklassen modulo n:

Gegeben: $n \in \mathbb{N}$

Betrachte: wähle $a \in \mathbb{Z}$

$$\bar{a} = \{a + nz \mid z \in \mathbb{Z}\}$$

Wir schließen $a, b \in \mathbb{Z}$:

$a \equiv b \pmod{n}$, falls a, b den gleichen Rest bei Div durch n haben:

Es gilt:

$$\left. \begin{array}{l} a = qn + r \\ b = \tilde{q}n + r \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{l} a - b = (q - \tilde{q})n \\ \Leftrightarrow n \mid (a - b) \\ \Leftrightarrow a + n\mathbb{Z} = b + n\mathbb{Z} \\ \Leftrightarrow \bar{a} = \bar{b} \end{array} \right.$$

Menge der Restklassen $\rightarrow \mathbb{Z} \mid n\mathbb{Z} = \mathbb{Z} \mid n = \mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$

$$|\mathbb{Z}_n| = n$$

Addition:

$$\bar{k}, \bar{l} \in \mathbb{Z}$$

$$\rightarrow \overline{\bar{k}} = \bar{l} = \overline{\bar{k} + \bar{l}}$$

Ringe

Eine Menge R mit zwei Verknüpfungen $+$ und \cdot heißt ein Ring falls gilt:

- $(R, +)$ ist abelsche Gruppe
- \cdot ist assoziativ
- Distributivgesetze $a(b + c) = ab + ac$ und $(a + b)c = ac + bc \forall a, b, c \in R$
- \exists Einselement: $1 \in R: 1 \cdot a = a = a \cdot 1 \quad \forall a \in R$

Einheitengruppe (= Gruppe der invertierbaren Elemente)

Gegeben: Ring $(R, +, \cdot)$

$$R^\times = \{a \in R \mid a \text{ ist invertierbar}\} = \{a \in R \mid \exists b \in R : ab = 1 = ba\}$$

R^\times ist die Einheitengruppe von R

Prime Restklassengruppen

$$\begin{aligned} n \in \mathbb{N} \rightarrow \mathbb{Z}_n^\times &= \{\bar{a} \text{ ist invertierbar}\} \\ &= \{\bar{a} \in \mathbb{Z}_n \mid \exists j \in \mathbb{Z}_n : \bar{a}j = 1\} \\ &= \{\bar{a} \in \mathbb{Z}_n \mid \text{ggT}(a, n) = 1\} \end{aligned}$$

$$a, b \text{ sind relativ prim/teilerfremd} \Leftrightarrow \text{ggT}(a, b) = 1$$

$(\mathbb{Z}_n, +, \cdot)$ ist Körper $\Leftrightarrow n \in (\mathbb{P})$

$$\begin{aligned} \bar{a} \text{ invertierbar} &\Leftrightarrow \exists \bar{b} \in \mathbb{Z}_n && : \bar{a}\bar{b} = \bar{1} \\ &\Leftrightarrow \exists b \in \mathbb{Z} && : (a + n\mathbb{Z})(b + n\mathbb{Z}) = 1 + n\mathbb{Z} \\ &\Leftrightarrow \exists b \in \mathbb{Z} && : n \mid ab - 1 \\ &\Leftrightarrow \exists b \in \mathbb{Z} \exists x \in \mathbb{Z} && : ab - 1 = nx \\ &\Leftrightarrow \exists b \in \mathbb{Z} \exists x \in \mathbb{Z} && : ab - nx = 1 \\ &\Rightarrow && \text{ggT}(a, n) = 1 \end{aligned}$$

Euklidischer Algorithmus

$$a_1 = a, a_2 = b \mid b > 0$$

Sukzessive Division mit Rest:

$$\begin{array}{rclcl} a_1 & = & q_1 a_2 & + & a_3, \quad 0 < a_3 < a_2 \\ a_2 & = & q_2 a_3 & + & a_4, \quad 0 < a_4 < a_3 \\ \vdots & = & \vdots & + & \vdots \\ a_{n-2} & = & q_{n-2} a_{n-1} & + & a_n, \quad 0 < a_n < a_{n-1} \\ a_{n-1} & = & q_{n-1} a_n & + & 0 \quad \nwarrow \underline{a_n = \text{ggT}(a_1, a_2)} \end{array}$$

$$\exists r, s \in \mathbb{Z} : ra + sb = a_n \quad \Leftarrow \text{erweiterter euklidischer Algorithmus}$$

Erweiterter Euklidischer Algorithmus

Der Erweiterter Euklidischer Algorithmus findet zwei weitere Zahlen $s, t \in \mathbb{Z}$ die eine Linearkombination bilden, die folgende Gleichung erfüllt:

$$s \cdot a + t \cdot b = \text{ggT}(a, b)$$

Berechnung

Bei dem Erweiterten Euklidischen Algorithmus wird die bisherige Folge r_x um drei weitere (q_x, s_x, t_x) erweitert, welche mit der folgenden Formeln bestimmt werden

$$\begin{aligned} q_{x+1} &:= \left\lfloor \frac{r_{x-1}}{r_x} \right\rfloor \\ r_{x+1} &:= \begin{cases} a & \text{wenn } x = 0, \\ b & \text{wenn } x = 1 \\ r_{x-1} - q_x \cdot r_x & \end{cases} \\ s_{x+1} &:= \begin{cases} 1 & \text{wenn } x = 0, \\ 0 & \text{wenn } x = 1 \\ s_{x-1} - q_x \cdot s_x & \end{cases} \\ t_{x+1} &:= \begin{cases} 0 & \text{wenn } x = 0, \\ 1 & \text{wenn } x = 1 \\ t_{x-1} - q_x \cdot t_x & \end{cases} \end{aligned} \quad \longrightarrow \quad \begin{aligned} \text{ggT}(a, b) &= r_n \\ &= s_n \cdot a + t_n \cdot b \quad \text{mit } r_{n+1} = 0 \end{aligned}$$

Eulersche φ -Funktion:

Man nennt $\varphi(n) = \#\{a \in \{1, \dots, n\} \mid \text{ggT}(a, n) = 1\}$

$$\varphi(n) = |\mathbb{Z}_n^\times|$$

$$\varphi(p) = p - 1 \quad \forall p \in \mathbb{P}$$

kleiner Satz von Fermat

Es sei $p \in \mathbb{P}$ dann gilt: $\forall a \in \mathbb{Z} : a^p \equiv a \pmod{p}$

Das Pohlig Hellman Verfahren

$$p = (\text{gro\ss e}) \text{ Primzahl} \parallel \mathcal{N} = \text{Klartext} \mid \mathcal{N} \in \mathbb{Z}_p^\times \parallel e, d = \text{Schl\"ussel}$$

Wähle $e \in \mathbb{N}$ mit $\text{ggT}(e, p-1) = 1$

Bestimme d mit:

$$\begin{aligned} ed &\equiv 1 \pmod{p-1} \\ ed &= 1 + r(p-1) \\ 1 &= ed - r(p-1) \\ &\Rightarrow \text{euklidischer Algorithmus} \end{aligned}$$

Verschl\"usseln:

$$\mathcal{C} = \mathcal{N}^e$$

Entschl\"usseln:

$$\mathcal{C}^d = (\mathcal{N}^e)^d = \mathcal{N}^{ed} = \mathcal{N}^{1+r(p-1)} = \mathcal{N}^1 \cdot (\mathcal{N}^{(p-1)})^r \stackrel{\text{Satz von Euler - Fermat}}{=} \mathcal{N}$$

Wähle p am besten mit $\frac{p-1}{2}$ auch prim \leftarrow sichere Primzahl

RSA-Verfahren:

Vorbereitung des Empfängers (Erzeugers der Schlüssel):

1. wähle große $p, q \in \mathbb{P} : p \neq q$ und $p \pm 1, q \pm 1$ müssen große Primteiler haben
2. setze $n = p \cdot q$
3. $\left| \mathbb{Z}_n^\times \right| = \left| \{a \in \{1, \dots, n\} \mid \text{ggT}(a, n) = 1\} \right| = \varphi(n) = \varphi(p \cdot q) = (p-1)(q-1)$
4. wähle $e \in \{1, \dots, n\} : \text{ggT}(e, \varphi(n)) = 1$
5. berechne $d : e \cdot d \equiv 1 \pmod{\varphi(n)}$
6. veröffentliche Schlüssel (n, e)

Verschlüsselung des Senders:

$$\mathcal{C} \equiv \mathcal{N}^e \pmod{n}$$

Entschlüsselung des Empfängers:

$$\mathcal{N} \equiv \mathcal{C}^d \pmod{n}$$

Vektorräume

Körper

Ein Ring K ($K, +, \cdot$) mit:

1. K ist kommutativ
2. \exists Einselement $1 : 1 \cdot \lambda = \lambda = \lambda \cdot 1 \quad \forall \lambda \in K$
3. Jedes $\lambda \neq 0$ ist invertierbar $\Leftrightarrow K^\times = K \setminus \{0\}$

V heißt ein K -Vektorraum falls $\forall \lambda, \mu \in K, \forall u, v, w \in V :$

$$\left. \begin{array}{l} 1. v + w \in V, \lambda \cdot v \in V \\ 2. u + (v + w) = (u + v) + w \\ 3. \exists 0 \in V : 0 + v = v \\ 4. \exists v' \in V : v + v' = 0 \\ 5. u + v = v + u \end{array} \right\} (V, +) : \text{abelsche Gruppe}$$
$$\left. \begin{array}{l} 6. \lambda(u + v) = \lambda u + \lambda v \\ 7. (\lambda + \mu)v = \lambda v + \mu v \\ 8. (\lambda \mu)v = \lambda(\mu v) \\ 9. 1v = v \end{array} \right\} \text{Verträglichkeitsgesetze}$$

Sprechweisen und Regeln

Vektor: Element eines Vektorraumes

Nullvektor: 0-Element des Vektorraumes

Entgegengesetzte Vektoren (Negative): $-v \rightarrow w + (-v) = w - v$

$K = \mathbb{R}$: reeller Vektorraum

$K = \mathbb{C}$: komplexer Vektorraum

$\lambda \in K$: Skalare

3 Regeln:

$$0 \cdot v = (0 + 0) \cdot v = 0 \cdot v + 0 \cdot v \quad | - (0v)$$

$$0 = 0 \cdot v$$

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

$$0 = \lambda \cdot 0$$

$$\lambda \cdot v = 0 \iff \lambda = 0 \vee v = 0$$

Untervektorräume

V sei ein K -Vektorraum

$U \subseteq V$ heißt Untervektorraum, falls U wieder ein K -Vektorraum ist

d.h.

- $0 \in U$
- $u, v \in U \Rightarrow u + v \in U$
- $\lambda \in K, u \in U \Rightarrow \lambda u \in U$

Linearkombinationen

$v_1, \dots, v_n \in V, \lambda_1, \dots, \lambda_n \in K$

wenn gilt:

$$v = \lambda_1 v_1 + \dots + \lambda_n v_n = \sum_{i=1}^n \lambda_i v_i \in V$$

ist v eine Linearkombination von v_1, \dots, v_n

Das Erzeugnis von X

Geg.: $V : K$ -Vektorraum $X \subseteq V$

$$\begin{aligned} \text{Setze : } \langle X \rangle &= \text{lin}(X) = \text{span}(X) \\ &= \left\{ \sum_{i=1}^n \lambda_i v_i \mid \lambda_i \in K, v_i \in X, n \in \mathbb{N} \right\} \\ &= Kv_1 + \dots + Kv_n \\ &= \text{Menge aller endlichen Linearkombinationen von Elementen aus } X \\ &= \text{Erzeugnis von } X \\ &= \text{lineare Hülle von } X \end{aligned}$$

- $\langle X \rangle \leq V \iff \langle X \rangle$ ist ein Untervektorraum von V

Definition:

$$X = \emptyset \rightarrow \langle \emptyset \rangle = \{0\}$$

Lineare Unabhängigkeit:

Geg.: K -Vektorraum V

$v_1, \dots, v_n \in V$ heißen linear unabhängig, falls:

$$\forall T \subsetneq \{v_1, \dots, v_n\} \Rightarrow \langle T \rangle \subsetneq \langle v_1, \dots, v_n \rangle \leftarrow \text{"keins unnötig"}$$

Das Kriterium für lineare Unabhängigkeit:

Gegeben: $v_1, \dots, v_n \in V, 0_v \in V$

Ansatz:

$$\lambda_1 v_1 + \dots + \lambda_n v_n = 0_v$$

Falls:

$$\exists_1 \text{Lsg.} \Rightarrow v_1, \dots, v_n \text{ linear unabhängig}$$

Basen von Vektorräumen

Ist V ein K -Vektorraum, so nennt man $B \subseteq V$ eine Basis von V , falls:

- B linear unabhängig
- B erzeugt V

Merkregeln

- Jeder K -Vektorraum hat eine Basis
- $B \subseteq V$ ist eine Basis von $V \iff B$ ist eine maximal-linear-unabhängige Teilmenge von V
 $\iff B$ ist minimales Erzeugendensystem von V
- Jede linear unabhängige Menge von V kann man zu einer Basis ergänzen
- Jedes Erzeugendensystem von V kann zu einer Basis verkürzt werden
- Ist B eine Basis von V , so kann jedes $v \in V$ als genau eine Weise bzgl. B dargestellt werden:

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

- Je zwei Basen von V haben die gleiche Mächtigkeit : B_1, B_2 Basen von $V \Rightarrow |B_1| = |B_2|$
- Die Dimension eines Vektorraumes V :

Wähle Basis B von V

$$\dim(V) = |B| = \begin{cases} n \\ \infty \end{cases}$$

- Ist V ein Vektorraum der Dimension n : $\dim(V) = n$:

Dann:

- Jede linear unabhängige Menge mit n Elementen ist eine Basis
- Jedes Erzeugendensystem mit n Elementen ist eine Basis
- Mehr als n Vektoren sind immer linear abhängig
- $U \subseteq V \Rightarrow \dim(U) \leq \dim(V)$
- $U \subseteq V \wedge \dim(U) = \dim(V) \Rightarrow U = V$
- $\dim(\mathbb{R}[x]_n) = n + 1$

Anwendung in Linearen Gleichungssystemen

$$A \in K^{m \times n} = (a_{ij}) = \begin{pmatrix} s_1 & \dots & s_n \end{pmatrix} = \begin{pmatrix} z_1 \\ \vdots \\ z_m \end{pmatrix}$$

$$S_A = \langle s_1, \dots, s_n \rangle = \text{Spaltenraum von } A \quad \left| \quad Z_A = \langle z_1, \dots, z_m \rangle = \text{Zeilenraum von } A \right.$$
$$\dim(S_A) = \text{Spaltenrang von } A \quad \left| \quad \dim(Z_A) = \text{Zeilenrang von } A \right.$$

$$\text{rg}(A) = \text{Zeilenrang} = \text{Spaltenrang} \quad \forall A \in K^{m \times n}$$

Spaltenraum

$$A = \begin{pmatrix} s_1 & \dots & s_n \end{pmatrix} \in K^{m \times n}$$

$$\begin{aligned} \langle s_1, \dots, s_n \rangle &= \left\{ \sum_{i=1}^n \lambda_i s_i \mid \lambda_i \in K \right\} \\ &= \left\{ \begin{pmatrix} s_1 & \dots & s_n \end{pmatrix} \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} \mid \lambda_1, \dots, \lambda_n \in K \right\} \\ &= \{ A \cdot x \mid x \in K^n \} \end{aligned}$$

$$Ax = 0: (A|0) \rightarrow ZSF$$

$$\left. \begin{array}{l} \text{Lösungsraum von } A \cdot x = 0 \\ \text{Kern}(A) \\ \text{ker}(A) \end{array} \right\} \leq K^n$$

$$\dim(\text{Kern}(A)) = n - \text{rg}(A)$$

Lineare codes

datenübertragung: Bits $\rightarrow x_1, x_2, x_3, \dots$

Strom von Bits über gestörten Kanal

$p \approx 10^{-6}$ falsches Bit wird übertragen

G = Generatormatrix

$$G = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \ddots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \dots & 1 \\ 1 & 0 & \dots & 0 \\ 0 & 1 & \ddots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \dots & 1 \end{pmatrix} \quad \text{Wiederholungsmatrix}$$
$$G = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \ddots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \dots & 1 \\ 1 & 1 & \dots & 1 \end{pmatrix} \quad \text{Parity-Check Matrix}$$

$$\text{Die Menge } C := \left\{ G \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} \mid \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix} \in K^k \right\} \leq K$$

heißt (n, k) -Code:

$$\begin{aligned} n &= \text{Länge} \\ n - k &= \text{Redundanz} \end{aligned}$$

$$\begin{aligned} \dim(C) &= k \\ \frac{k}{n} &= \text{Informationsrate} \\ \text{rg}(G) &= k \end{aligned}$$

Wie läuft das Dekodieren ab?

1. Fall $c' \in C$:

$$\text{Dekodiere : } G \cdot x = c' \Rightarrow x \in k^k$$

2. Fall: $c' \notin C$:

Suche c'' , das sich von c' möglichst wenig unterscheidet:

$$\begin{array}{l|l} \exists_1 c'' & \exists c''_1, \dots, c''_n : c''_1, \dots, c''_n \text{ paarweise disjunkt} \\ \text{nächstes } c' \text{ an } c'' \text{ wählen und wie in Fall 1 dekodieren} & \text{Nachricht neu senden lassen} \end{array}$$

Hamming Gewicht und Abstand

Für $c = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} \in K^n$ ist das Hamming-Gewicht:

$$w(c) = \left| \left\{ i \in \{1, \dots, n\} \mid c_i \neq 0 \right\} \right|$$

Für $c, c' \in K^n$ ist der Hamming-Abstand:

$$d(c, c') = w(c - c') = \left| \left\{ i \in \{1, \dots, n\} \mid c_i \neq c'_i \right\} \right|$$

Für $C \subseteq K^n$ gilt:

$$\begin{array}{l|l} d(C) = \min \{ d(c, c') & c, c' \in C, c \neq c' \} \\ d(C) = \min \{ w(c) & c \in C \setminus \{0\} \} \end{array}$$

Lineare Codes (Fortsetzung)

$$d(c, c'') \leq d(c, c') + d(c', c'')$$

Es sei $C \in K^n$ ein Code:

$$\begin{array}{l|l} d(C) = 2e + 1 & d(C) = 2e + 2 \\ C \text{ ist } e\text{-fehlerkorrigierend} & \begin{array}{l} C \text{ ist } e\text{-fehlerkorrigierend} \\ C \text{ ist } (e + 1)\text{-fehlererkennend} \end{array} \end{array}$$

Die Kontrollmatrix (Parity Check Matrix)

$$G = \begin{pmatrix} E_k \\ A \end{pmatrix} \in K^{n \times k}$$

$$P = (-A \quad E_{n-k}) \in K^{(n-1) \times n}$$

Es gilt:

$$P \cdot G = 0$$

Damit:

- $Pc = 0 \forall c \in C$
- $\dim(C) = \dim(\text{Lösungsraum } Px = 0) = n - (n - k) = k$

$C = \text{"Lösungsmenge } Px = 0\text{"}$

Vorbereitung auf Determinante

Die symmetrische Gruppe:

Menge aller Permutationen (=Bijektionen) von $\{1, 2, \dots, n\}$

$$S_n = \left\{ \sigma : I_n \rightarrow I_n \mid \sigma \text{ bijektiv} \right\}$$

$$|S_n| = n!$$

Verknüpfung: Komposition (Hintereinanderausführung):

$$f \circ g = f(g(x))$$

Das Signum (Vorzeichen) einer Permutation:

Wir nennen (j, i) einen Fehlstand der Permutation σ , falls

$$i < j, \text{ aber } \sigma(i) > \sigma(j)$$

Hat σ f Fehlstände, so setze $sgm(\sigma) = (-1)^f$

Es gilt:

$f = \# \text{Fehlstände von } \sigma \leftarrow$ ist ein Homomorphismus:

$$sgm(\sigma \circ \tau) = sgm(\sigma) \cdot sgm(\tau) \quad \forall \sigma, \tau \in S_n$$

$$sgm(\sigma \circ \tau) = \prod_{i < j} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{j - i}$$

$$\begin{aligned} sgm(\sigma \circ \tau) &= \prod_{i < j} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{j - i} \\ &= \underbrace{\prod_{i < j} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)}}_{sgm(\sigma)} \cdot \underbrace{\prod_{i < j} \frac{\tau(j) - \tau(i)}{j - i}}_{sgm(\tau)} \end{aligned}$$

Die Determinante:

Für jede quadratische Matrix $A \in K^{n \times n}$, K Körper, heißt

$$|A| = \det(A) = \sum_{\sigma \in S_n} sgm(\sigma) \prod_{i=1}^n a_i \cdot \sigma(i)$$

die Determinante von A (Leibniz'sche Formel).

Weiter:

$$per(A) = \sum_{\sigma \in S_n} \prod_{i=1}^n a_i \cdot \sigma(i)$$