Ausgewählte Kapitel der Mathematik

Jason Uhing

WS 2023/2024

Inhaltsverzeichnis

Kapitel 1

Lineare Algebra

1.1 Lineare Gleichungssysteme

1.1.1 Einführung

Ein lineares Gleichungssystem ist eine Sammlung endlich vieler Gleichungen mit Unbekannten x_i, zum Beispiel

$$3x_1 = 7, \quad x_1 + x_2 = -1, \quad \left| \begin{array}{rcr} x_1 + x_2 & = & -1 \\ 2x_2 - x_1 & = & 0 \end{array} \right| \tag{1.1}$$

Ein nicht-lineares Gleichungssysteme ist zum Beispiel

$$\left| \begin{array}{rcr} x_1^2 + x_2 & = & -1 \\ x_2 + x_1 & = & 4 \end{array} \right|$$

'2-dimensionale' Geometrie: GEometrisch lassen sich Gleichungen mit zwei Variablen als Geraden in $\mathbb{R}^2$ darstellen.

Lösungsmethode Einsetzungsverfahren

$$\left| \begin{array}{rcr} x_2 + x_1 & = & -1 \\ 2x_2 - x_1 & = & 0 \end{array} \right| \mapsto \left| \begin{array}{rcrcr} x_2 + x_1 & = & -1 & & \\ x_1 & = & 2x_2 & = & 0 \end{array} \right| \tag{1.2}$$

$$\Rightarrow 3x_2 = -1 \Rightarrow x_2 = -\frac{1}{3} \Rightarrow x_1 = 2x_2 = -\frac{2}{3}$$

Lösungsmethode Additionsverfahren

$$\left| \begin{array}{rcr} x_2 + x_1 & = & -1 \\ 2x_2 - x_1 & = & 0 \end{array} \right| \mapsto \left| \begin{array}{rcr} 3x_2 & = & -1 \\ 2x_2 - x_1 & = & 0 \end{array} \right| \tag{1.3}$$

$$\Rightarrow x_2 = -\frac{1}{3}, x_1 = -\frac{2}{3}$$

Es sei $n \in \mathbb{N}$, $n \geq 2$. Ein n-Tupel ist eine geordnete Aufzählung von n reellen Zahlen x_i und wir

notieren dieses so

$$(x_1, x_2, \ldots, x_n), \quad x_i \in \mathbb{R}, \quad 1 \leq i \leq n.$$

Die Menge solcher Tupel notieren wir als

$$\mathbb{R}^n := \{(x_1, x_2, \ldots, x_n) \mid x_i \in \mathbb{R}, \quad 1 \leq i \leq n\}.$$

Auf $\mathbb{R}^n$ können wir komponentenweise eine Addition und eine Multiplikation definieren:

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) := (x_1 + y_1, \ldots, x_n + y_n)$$

und für $\lambda \in \mathbb{R}$

$$\lambda(x_1, \ldots, x_n) := (\lambda x_1, \ldots, \lambda x_n).$$

Da wir komponentenweise die Addition und Multiplikation aus $\mathbb{R}$ verwenden, sind diese Verknüpfungen auch assoziativ, kommutativ. Es gelten die Distributivgesetze.

Liegt ein LGS in den Unbekannten (oder Variablen) $x_1, \ldots, x_n$ vor, so gibt man die Lösungsmenge $\mathbb{L}$ des LGS als Teilmenge von $\mathbb{R}^n$ an:

$$\mathbb{L} \subset \mathbb{R}^n.$$

Im obigen Beispiel also

$$\mathbb{L} = \{(-\frac{2}{3}, -\frac{1}{3})\} \subset \mathbb{R}^2.$$

'3-dimensionale' Geometrie: Eine Gleichung $ax_1 + bx_2 + cx_3 = b$ beschreibt eine Ebene in $\mathbb{R}^3$. Die Lösungsmenge eines LGS mit dreiVariablen entspricht dem Schnitt von Ebenen und idt daher leer oder eine Gerade oder eine Ebene. Beweise kommen später.

'n-dimensionale' Geometrie: das wird später in der Theorie der Vektorräume behandelt.

Beispiel 1. Zur Auflistung von Internetseiten nach einer Google-Suche wird der Pagerank-Algorithmus verwendet. Dabei muss ein LGS mit n Gleichungen und n Unbekannten gelöst werden. Dabei ist n die Anzahl der gefundenen Internetseiten.

LGS

Definition 2. Ein lineares Gleichungssystem (LGS) mit m Gleicungen und n Variablen ist eine Menge von Gleichungen der Form

$$\sum_{j=1}^{n} a_{ij} x_j = b_i, \quad a_{ij}, b_i \in \mathbb{R}, \ 1 \leq i \leq m, \ 1 \leq j \leq n.$$

Falls alle $b_i = 0$ sind, dann nennt man das LGS homogen.

1.1.2 Elementare Zeilenumformungen

Die Gleichungen eines LGS schreibt man untereinander. So ergibt sich eine Liste von Gleichungen. Steht eine Gleichung auf Listenplatz i, so spricht man von der $i-$ten Gleichung oder Gleichung i.

Definition 3. Als elementare Zeilenumformungen (eZU) bezeichnet man folgende Modifikationen eines LGS:

$$\begin{aligned} V_{ij} &= \text{vertauschen der Gleichungen } i \text{ und } j \\ M_i(\lambda) &= \text{multiplizieren der Gleichung } i \text{ mit } \lambda \neq 0 \\ E_{ij} &= \text{multiplizieren der Gleichung } j \text{ mit } \lambda \neq 0 \text{ und addieren zur Gleichung } i \end{aligned}$$

Beispiel 4.

$$\left|\begin{array}{rcl} x_2 + 2x_3 & = & 10 \\ 5x_1 - 3x_2 + x_3 & = & 5 \\ -2x_2 + 2x_3 & = & -4 \end{array}\right| \overset{V_{12}}{\mapsto} \left|\begin{array}{rcl} 5x_1 - 3x_2 + x_3 & = & 5 \\ x_2 + 2x_3 & = & 10 \\ -2x_2 + 2x_3 & = & -4 \end{array}\right|$$

$$\overset{M_2(2)}{\mapsto} \left|\begin{array}{rcl} 5x_1 - 3x_2 + x_3 & = & 5 \\ 2x_2 + 4x_3 & = & 20 \\ -2x_2 + 2x_3 & = & -4 \end{array}\right| \overset{E_{32}(1)}{\mapsto} \left|\begin{array}{rcl} 5x_1 - 3x_2 + x_3 & = & 5 \\ 2x_2 + 4x_3 & = & 20 \\ 8x_3 & = & 16 \end{array}\right|$$

Aus dem letzten System errechnen wir $x_3 = 2$. Einsetzen in die zweite Gleichung ergibt $x_2 = 4$ und schliesslich $x_1 = 3$. Wir schreiben die Lösungsmenge als

$$\mathbb{L} = \{(3, 4, 2)\} \subset \mathbb{R}^2.$$

thm:ezu

Satz 5. *Die Lösungsmenge eines LGS bleibt unter eZU unverändert.*

Zum Beweis dieses Satzes brauchen wir noch einige Vorbereitungen.

1.1.3 Matrizen

Definition 6. Eine $m \times n$-Matrix über $\mathbb{R}$ ist ein Zahlenschema

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

mit m Zeilen und n Spalten und $a_{ij} \in \mathbb{R}$ für $1 \leq i \leq m, 1 \leq j \leq n$. Bezeichnet man die obige Matrix mit A so schreibt man $A_{ij} := a_{ij}$. Die Menge aller $m \times n$ - Matrizen mit Einträgen in $\mathbb{R}$ bezeichnen wir mit

$$\mathrm{Mat}_{m,n} := \{A \mid A \text{ ist } m \times n \text{ Matrix}\}.$$

Definition 7. Operationen mit Matrizen

1. Für $A, B \in \mathrm{Mat}_{m,n}$ definiert man $A + B \in \mathrm{Mat}_{m,n}$ durch $(A + B)_{ij} := A_{ij} + B_{ij}$
2. Für $\lambda \in \mathbb{R}, A \in \mathrm{Mat}_{m,n}$ definiert man $\lambda A \in \mathrm{Mat}_{m,n}$ durch $(\lambda A)_{ij} := \lambda A_{ij}$
3. Für $A \in \mathrm{Mat}_{m,n}$ und $B \in \mathrm{Mat}_{n,l}$ definiert man $AB \in \mathrm{Mat}_{m,l}$ durch

$$(AB)_{ij} := \sum_{k=1}^{n} A_{ik} B_{kj}.$$

4. Für $A \in \mathrm{Mat}_{m,n}$ definiert man $A^T \in \mathrm{Mat}_{n,m}$ durch $A^T_{ij} := A_{ji}$.

Satz 8. *Sofern die folgenden Matrizenoperationen definiert sind, gelten die folgeden Rechenregeln:*

1. $A + B = B + A$
2. $A(B + C) = AB + AC, \quad (A + B)C = AC + BC$
3. $(\lambda + \mu)A = \lambda A + \mu A, \quad \lambda(A + B) = \lambda A + \lambda B.$
4. $A(BC) = (AB)C$
5. $(AB)^T = B^T A^T$

Definition 9. Vorgelegt sei ein LGS wie in Definition 2. Die Matrix

$$A := \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \in \mathrm{Mat}_{m,n}$$

nennt man Koeffizientenmatrix zum LGS. Die Matrix

$$b := \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix} \in \mathrm{Mat}_{m,1}$$

nennt man rechte Seite. Die Matrix

$$(A \mid b) := \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} & b_1 \\ a_{21} & a_{22} & \dots & a_{2n} & b_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} & b_m \end{pmatrix} \in \mathrm{Mat}_{m,n+1}$$

nennt man erweiterte Koeffizientenmatrix. Die Lösungsmenge eines LGS mit erweiterter Koeffizientenmatrix $(A \mid b)$ bezeichnen wir mit $\mathbb{L}_{A,b} \subset \mathbb{R}^n$

Bemerkung 10. 1. Da Addition und Multiplikation in $\mathbb{R}^n$ und $\mathrm{Mat}_{n,1}$ jeweils komponentenweise definiert sind, können wir diese beiden Mengen identifizieren. Damit kann man

$$\mathbb{L}_{A,b} = \{x \in \mathrm{Mat}_{n,1} \mid Ax = b\}$$

schreiben.

2. Matrizenmultiplikation ist nicht kommutativ und nicht nullteilerfrei:

$$\begin{pmatrix} 2 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 5 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

1.1.4 Elementarmatrizen

Definition 11. Es sei $n \in \mathbb{N}$, $1 \leq i < j \leq n$ und $\lambda \in \mathbb{R}, \lambda \neq 0$. Die folgenden Matrizen nennt man Elementarmatrizen. Außerhalb der MArkierten Einträge stehen Nullen. Auf der Diagonale stehen die PPukte für Einsen, sonst für Nullen.

1.

$$V_{ij} := \begin{pmatrix} 1 & & & & & & & & \\ & \ddots & & & & & & & \\ & & 1 & & & & & & \\ & & & 0 & \cdots & 1 & & & \\ & & & & 1 & & & & \\ & & & \vdots & & \vdots & & \vdots & \\ & & & & & & 1 & & \\ & & & 1 & \cdots & 0 & & & \\ & & & & & & & 1 & \\ & & & & & & & & \ddots \\ & & & & & & & & & 1 \end{pmatrix}$$

Dabei steht die erste Null auf der Diagonalen in der i-ten Zeile, die zweite Null in der j-ten Spalte.

2.

$$M_i(\lambda) := \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & \lambda & & \\ & & & & 1 & \\ & & & & & \ddots \\ & & & & & & 1 \end{pmatrix}$$

Dabei steht λ auf der Diagonalen in der i-ten Zeile.

3.
$$E_{ij}(\lambda) := \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & 1 & \cdots & \lambda & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix}$$

Dabei steht λ auf der Diagonalen in der i-ten Zeile und die Eins in der j-ten Spalte.

Satz 12. *Es sei $E \in \mathrm{Mat}_{n,n}$ eine Elementarmatrix und $A \in \mathrm{Mat}_{n,m}$. Dann geht $E \cdot A$ aus A durch eine elementare Zeilenumformung gemäß E aus Definition* **??** *hervor.*

Proof. Durch Nachrechnen. □

1.1.5 Inverse Matrizen

Eine $n \times n$- Matrix, die deren Diagonalelemente Eins und deren restliche Einträge Null sind, nennt man Einheitsmatrix und bezeichnet sie mit E_n.

Definition 13. Es sei $A \in \mathrm{Mat}_{n,n}$. Eine Matrix B heißt invers zu A falls $AB = BA = E_n$ gilt. In diesem Fall schreibt man $A^{-1} := B$.

Beispiel 14. 1. Zur Nullmatrix ist keine Matrix invers.

2. Die Matrix
$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$
ist nicht die Nullmatrix, besitzt aber auch keine Inverse, denn für jedes $B \in \mathrm{Mat}_{2,2}$ gilt $(AB)_{2,2} = 0$.

3. Es seien
$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad B = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}, \quad ad - bc \neq 0.$$
Dann gilt $A^{-1} = B$.

Satz 15. *Elementarmatrizen sind invertierbar und es gelten:*

1. $M_i(\lambda)^{-1} = M_i(\frac{1}{\lambda})$,
2. $E_{ij}(\lambda)^{-1} = E_{ij}(-\lambda)$,
3. $V_{ij}^{-1} = V_{ji} = V_{ij}$.

Proof. Durch Nachrechnen. □

Satz 16. *Es seien $A, B \in \mathrm{Mat}_{n,n}$ invertierbar. Dann gilt $(AB)^{-1} = B^{-1}A^{-1}$.*

Proof. Durch Nachrechnen. □

Satz 17. *Es seien $A \in \mathrm{Mat}_{n,n}$ invertierbar. Dann ist A^{-1} eindeutig bestimmt.*

Proof. Durch Nachrechnen. □

Nun können wir beweisen, dass elementare Zeilenumformungen die Lösungsmenge eines LGS nicht verändern.

Proof. von Satz 5 □

1.1.6 Zeilenstufenform

dfn:zstf

Definition 18. Eine $m \times n$-Matrix heißt in Zeilenstufen form (ZSTF), wenn sie folgende Gestalt hat:

$$\begin{pmatrix}
0 & \cdots & 0 & 1 & * & \cdots & * & 0 & * & \cdots & * & 0 & \cdots & 0 & * & \cdots & * \\
0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 1 & * & \cdots & * & 0 & \cdots & 0 & * & \cdots & * \\
0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 1 & \cdots & 0 & * & \cdots & * \\
\vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & \ddots & 0 & \vdots & & \vdots \\
0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\
0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0
\end{pmatrix}$$

Eine $m \times n$-Matrix heißt in spezieller Zeilenstufen form (sZSTF), wenn sie folgende Gestalt hat:

$$\begin{pmatrix}
1 & 0 & \cdots & 0 & 0 & c_{1\,r+1} & c_{1\,r+2} & \cdots & c_{1\,n} \\
0 & 1 & \cdots & 0 & 0 & c_{2\,r+1} & c_{2\,r+2} & \cdots & c_{2\,n} \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & & \vdots \\
0 & 0 & \cdots & 1 & 0 & c_{r-1\,r+1} & c_{r-1\,r+2} & \cdots & c_{r-1\,n} \\
0 & 0 & \cdots & 0 & 1 & c_{r\,r+1} & c_{r\,r+2} & \cdots & c_{r\,n} \\
0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 \\
\vdots & \vdots & & \vdots & \vdots & \vdots & \vdots & & \vdots \\
0 & 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0
\end{pmatrix}$$

Bemerkung 19.

1. Eine sZSTF ergibt sich durch Spaltenvertauschungen aus einer ZSTF und umgekehrt.
2. $A \cdot V_{ij}$ bewirkt Vertauschen der Spalten i und j von A. Das kann man wie folgt für $E = V_{ij}$ sehen: $AE = (E^T A^T)^T = (EA^T)^T =$ Vertauschen der Zeilen i und j an $A^T =$ Vertauschen der Spalten i und j von A.
3. Allgemein: Multiplikation von rechts mit Elementarmatrizen ergibt elementare Spaltenumformungen.

Beispiel 20. 1. Folgende Matrix ist in ZSTF

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

2.
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} V_{12} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} b & a \\ d & c \end{pmatrix}$$

thm:vartausch

Satz 21. *Es seien $A', A \in \mathrm{Mat}_{m,n}$, $b' \in \mathrm{Mat}_{n,1}$. Die Matrix A' gehe aus A durch einen Spaltentausch hervor, das heißt es gilt $A' = AV_{ij}$. Dann gilt*

$$x \in \mathbb{L}_{(A'|b')} \Leftrightarrow V_{ij}x \in \mathbb{L}_{(A|b')}.$$

Beweis □

Beispiel 22. Vorgelegt seien Matrizen

$$A = \begin{pmatrix} 0 & 1 & 2 & 0 & 1 \\ 0 & 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad b = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

Wir tauschen die Spalten wie folgt um eine sZSTF zu erhalten:

$$A' := AV_{12}V_{24} = \begin{pmatrix} 1 & 0 & 2 & 0 & 1 \\ 0 & 1 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Das LGS $A'x = b$ stellen wir um und schreiben es als

$$x_1 = -2x_3 - x_5, \quad x_2 = -3x_5.$$

Daher ergibt sich als Lösungsmenge

$$\mathbb{L}_{(A'|b)} = \{(-2x_3 - x_5, -3x_5, x_3, x_4, x_5) \,|\, x_3, x_4, x_5 \in \mathbb{R}\}.$$

Nach Satz 21 erhalten wir

$$\mathbb{L}_{(A|b)} = V_{12}V_{24}\mathbb{L}_{(A'|b)} = \{(x_4, -2x_3 - x_5, x_3, -3x_5, x_5) \,|\, x_3, x_4, x_5 \in \mathbb{R}\}.$$

lgsloeshom

Satz 23. *Es sei A in sZSTF wie in Definition 18. Die Lösung des LGS $Ax = 0$ läßt sich schreiben als*

$$\mathbb{L}_{A,0} = \left\{ \lambda_1 \begin{pmatrix} c_{1\,r+1} \\ c_{2\,r+1} \\ \vdots \\ c_{r-1\,r+1} \\ c_{r\,r+1} \\ -1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \lambda_2 \begin{pmatrix} c_{1\,r+2} \\ c_{2\,r+2} \\ \vdots \\ c_{r-1\,r+2} \\ c_{r\,r+2} \\ 0 \\ -1 \\ \vdots \\ 0 \end{pmatrix} + \cdots + \lambda_{n-r} \begin{pmatrix} c_{1\,n} \\ c_{2\,n} \\ \vdots \\ c_{r-1\,n} \\ c_{r\,n} \\ 0 \\ 0 \\ \vdots \\ -1 \end{pmatrix} , \ \lambda_1, \ldots, \lambda_{n-r} \in \mathbb{R} \right\}$$

Beweis □

Bemerkung 24. Für eine erweiterte Koeffizientenmatrix $(A|b)$ mit ZSTF $(A'|b')$ und sZSTF $(A''|b')$ haben wir nach Satz 21 also

$$\mathbb{L}_{(A|b)} = \mathbb{L}_{(A'|b')} = \mathbb{L}_{(A|b)} = S\mathbb{L}_{(A''|b')},$$

wobei S ein Produkt aus Elementarmatrizen V_{ij} gemäß der Spaltenvertauschungen ist.

Satz 25. *Jede Matrix $A \in \mathrm{Mat}_{m,n}$ läßt sich durch eZU in ZSTF bringen.*

Beweis □

Beispiel 26. Vorgelegt sei eine erweiterte Koeffizientenmatrix $(A|b)$. Wir bringen sie mit eZU auf ZSTF.

$$\left(\begin{array}{ccc|c} 1 & 2 & -3 & 6 \\ 2 & -1 & 4 & 2 \\ 4 & 3 & -2 & 14 \end{array}\right) \xrightarrow{E_{41}(-4)E_{21}(-2)} \left(\begin{array}{ccc|c} 1 & 2 & -3 & 6 \\ 0 & -5 & 10 & -10 \\ 0 & -5 & 10 & -10 \end{array}\right)$$

$$\xrightarrow{E_{32}(-1)} \left(\begin{array}{ccc|c} 1 & 2 & -3 & 6 \\ 0 & -5 & 10 & -10 \\ 0 & 0 & 0 & 0 \end{array}\right) \xrightarrow{M_2(-\frac{1}{5})} \left(\begin{array}{ccc|c} 1 & 2 & -3 & 6 \\ 0 & 1 & -2 & 2 \\ 0 & 0 & 0 & 0 \end{array}\right)$$

$$\xrightarrow{E_{12}(-2)} \left(\begin{array}{ccc|c} 1 & 0 & 1 & 2 \\ 0 & 1 & -2 & 2 \\ 0 & 0 & 0 & 0 \end{array}\right)$$

Die Lösung des homogenen LGS können wir nun mit Hilfe von Satz 23 schreiben als

$$\mathbb{L}_{(A|0)} = \left\{ \lambda \begin{pmatrix} 1 \\ -2 \\ -1 \end{pmatrix} \mid \lambda \in \mathbb{R} \right\}$$

Wenn wir die Lösung des inhomogenen Systems 'zu Fuß' bestimmen wollen , erhalten wir aus der ZSTF die Gleichungen

$$x_1 = 2 - x_3, \quad x_2 = 2 + 2x_3,$$

also können wir die Lösung für $\lambda := -x_3$ schreiben als

$$\left\{ \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 2 \\ 2 \\ 0 \end{pmatrix} + \lambda \begin{pmatrix} 1 \\ -2 \\ -1 \end{pmatrix} \mid \lambda \in \mathbb{R} \right\}$$

Mit

$$b' := \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix}$$

ergibt sich daraus

$$\mathbb{L}_{(A|b)} = b' + \mathbb{L}_{(A|0)}.$$

Die Lösungsmenge des inhomogenen LGS läßt sich in dieser Form also die Summe aus der Lösung des homogenen LGS und einer speziellen Lösung schreiben.

Dies gilt auch im Allgemeinen, das besagt der folgende

Satz 27. *Gegeben sei ein LGS $Ax = b$ sowie $x_0 \in \mathrm{Mat}_{n,1}$ mit $Ax_0 = b$. Dann gilt*

$$\mathbb{L}_{(A|b)} = x_0 + \mathbb{L}_{(A|0)}.$$

Beweis □

thm:28

Satz 28. *Es sei $A \in \mathrm{Mat}_{m,n}$ und $(A|b)$ die erweiterte Koeffizientenmatrix eines LGS. Weiter sei $(A'|b')$ eine ZSTF von $(A|b)$ und $(A''|b')$ eine sZSTF wie in 18. Dann gelten:*

1. *$A''x = b'$ lösbar $\quad\Leftrightarrow\quad b'_{r+1} = \cdots = b'_m = 0$.*
2. *Ist $A''x = b'$ lösbar und*

$$\tilde{b} := \begin{pmatrix} b'_1 \\ \vdots \\ b'_r \\ 0 \\ \vdots \\ 0 \end{pmatrix} \in \mathrm{Mat}_{n,1}$$

   so gilt $A''\tilde{b} = b'$.

3. $\mathbb{L}_{(A''|b')} = \tilde{b} + \mathbb{L}_{(A''|0)}$.
4. *Bezeichnet S die Matrix zu den Spaltenumformungen, also $A'' = A'S$, so gilt*

$$\mathbb{L}_{(A|b)} = \mathbb{L}_{(A'|b')} = S\mathbb{L}_{(A''|b')} = S\tilde{b} + S\mathbb{L}_{(A''|0)}.$$

Beweis Der Beweis ergibt sich sofort aus den vorangegangenen Sätzen. □

Beispiel 29. Vorgelegt sei ein LGS $A'x = b'$ mit

$$A' = \begin{pmatrix} 0 & 1 & 2 & 0 & 1 \\ 0 & 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad b' = \begin{pmatrix} 4 \\ 2 \\ 0 \end{pmatrix}.$$

Mit $S = V_{12}V_{24}$ ergibt sich

$$A'' = A'S = \begin{pmatrix} 1 & 0 & 2 & 0 & 1 \\ 0 & 1 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad \tilde{b} = \begin{pmatrix} 4 \\ 2 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

und

$$\mathbb{L}_{(A'|b')} = S\tilde{b} + S\mathbb{L}_{(A''|0)} = \left\{ \begin{pmatrix} 0 \\ 4 \\ 0 \\ 2 \\ 0 \end{pmatrix} + \lambda_1 \begin{pmatrix} 0 \\ 2 \\ -1 \\ 0 \\ 0 \end{pmatrix} + \lambda_2 \begin{pmatrix} -1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \lambda_3 \begin{pmatrix} 0 \\ 1 \\ 0 \\ 3 \\ -1 \end{pmatrix} \mid \lambda_1, \lambda_2, \lambda_3 \in \mathbb{R} \right\}$$

1.2 Vektoren

1.2.1 Verschiebungen

Aus der Elementaren Geometrie kennen wir das Konzept der Verschiebungen einer Ebene. Dazu sei E eine Ebene und $A, B \in E$ Punkte. Eine Verschiebung $\tau_{\overrightarrow{AB}} : E \to E$ bildet jeden Punkt $P \in E$ auf einen Punkt $Q \in E$ derart ab, dass $\overrightarrow{AB}$ und $\overrightarrow{PQ}$ parallelgleich sind. Dabei heißen $\overrightarrow{AB}$ und $\overrightarrow{PQ}$ parallelgleich, falls $|AB| = |PQ|$ gilt und $\overrightarrow{AB}$, $\overrightarrow{PQ}$ parallel und gleichgerichtet sind. Wenn $\overrightarrow{AB}$ und $\overrightarrow{PQ}$ parallelgleich sind, sind die zugehörigen Verschiebungen gleich, also $\tau_{\overrightarrow{AB}} = \tau_{\overrightarrow{PQ}}$. Wegen $Q = \tau_{\overrightarrow{AB}}(P)$ kann man das auch so schreiben

$$\tau_{\overrightarrow{AB}} = \tau_{\overrightarrow{P\tau_{\overrightarrow{AB}}(P)}}. \tag{1.4}$$ eq:versch

1.2.2 Koordinaten

Wir kennen $\mathbb{R}^2$ als Punktmenge

$$\mathbb{R}^2 := \{(x_1, x_2) \mid x_1, x_2 \in \mathbb{R}\}.$$

Jeden Punkt können wir in einem Kooerdinatensystem darstellen:

Zwei Punkte in $X, Y \in \mathbb{R}^2$ definieren eine Verschiebung $\tau_{\overrightarrow{XY}}$ über eine Abbildung

$$\phi : \mathbb{R}^2 \times \mathbb{R}^2 \to \left\{\tau \mid \tau : \mathbb{R}^2 \to \mathbb{R}^2 \text{ Verschiebung}\right\}, \quad \phi\left((X,Y)\right) := \tau_{\overrightarrow{XY}}.$$

Allerdings ist die Abbildung ϕ nicht injektiv, denn verschiedene Paare von Punkten, können dieselbe Verschiebung definieren. Zum Beispiel sind für

$$A = (0,0),\ B = (1,1),\ P = (1,0),\ Q = (1,2)$$

die Strecken $\overrightarrow{AB}$ und $\overrightarrow{PQ}$ parallelgleich. Daher führen wir eine Relation $\sim$ auf $\mathbb{R}^2 \times \mathbb{R}^2$ ein. Es seien

$$X = (x_1, x_2),\ Y = (y_1, y_2),\ X' = (x_1', x_2'),\ Y' = (y_1', y_2') \quad \in \mathbb{R}^2.$$

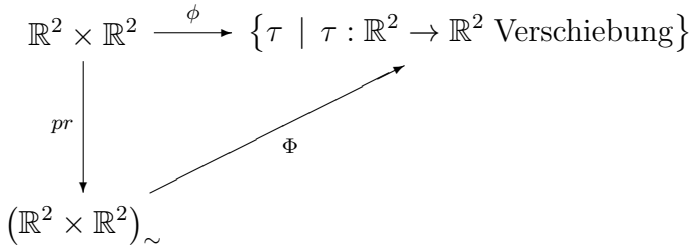
Dann definieren wir für $(X, y), (X', Y') \in \mathbb{R}^2 \times \mathbb{R}^2$:

$$(X,Y) \sim (X',Y') \quad :\Leftrightarrow \quad y_1 - x_1 = y_1' - x_1' \ \text{ und } \ y_2 - x_2 = y_2' - x_2'.$$

Satz 30. *Die Relation $\sim$ ist eine Äquivalenzrelation auf $\mathbb{R}^2 \times \mathbb{R}^2$.*

Beweis □

Aus diesem Satz erhalten wir folgenden kommutatives Diagramm



indem wir

$$pr\left((X,Y)\right) := [(X,Y)] \quad \text{und} \quad \Phi\left([(X,Y)]\right) := \tau_{\overrightarrow{XY}}$$

definieren. Die Abbildung pr bildet jedes Element auf seine Äquivalenzklasse ab und ist daher wohldefiniert.

Satz 31. *Die Abbildung Φ ist wohldefiniert und bijektiv.*

Beweis □

thm:verschformel

Satz 32. *Für $X, Y, A \in \mathbb{R}^2$ gilt $\tau_{\overrightarrow{XY}}(A) = A + Y - X$.*

Wir betrachten nun die Menge

$$\left(\mathbb{R}^2\right)^* := \left\{\overrightarrow{v} := \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} \mid v_1, v_2 \in \mathbb{R}\right\}$$

und die Abbildung

$$\Psi : \left(\mathbb{R}^2 \times \mathbb{R}^2\right)_\sim \longrightarrow \left(\mathbb{R}^2\right)^*,$$

die mit $X = (x_1, x_2)$ und $Y = (y_1, y_2)$ gegeben ist durch

$$\Psi\left([(X,Y)]\right) := \begin{pmatrix} y_1 - x_1 \\ y_2 - x_2 \end{pmatrix}.$$

Satz 33. *Die Abbildung Ψ ist wohldefiniert und bijektiv.*

Die Elemente von $(\mathbb{R}^2)^*$ nennen wir Vektoren. Wir wollen nun auf $(\mathbb{R}^2)^*$, $(\mathbb{R}^2 \times \mathbb{R}^2)_\sim$ und den Verschiebungen jeweils eine Addition definieren, die über Ψ und Φ miteinander verträglich sind. Für Vektoren $\overrightarrow{v}$ und $\overrightarrow{w}$ sei

$$\overrightarrow{v} = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}, \quad \overrightarrow{w} = \begin{pmatrix} w_1 \\ w_2 \end{pmatrix}, \quad \overrightarrow{v} + \overrightarrow{w} := \begin{pmatrix} v_1 + w_1 \\ v_2 + w_2 \end{pmatrix}.$$

Für $X, Y, X', Y' \in \mathbb{R}^2$ sei

$$[(X,Y)] + [(X',Y')] := [(X + X', Y + Y')].$$

Für $A, B, C, D \in \mathbb{R}^2$ sei

$$\tau_{\overrightarrow{AB}} + \tau_{\overrightarrow{CD}} := \tau_{\overrightarrow{CD}} \circ \tau_{\overrightarrow{AB}}.$$

Wir zeigen zunächst, dass die Addition mit Ψ verträglich ist:

$$\begin{aligned} \Psi\left([(X,Y)]\right) + \Psi\left([(X',Y')]\right) &= \begin{pmatrix} y_1 - x_1 \\ y_2 - x_2 \end{pmatrix} + \begin{pmatrix} y_1' - x_1' \\ y_2' - x_2' \end{pmatrix} = \begin{pmatrix} y_1 + y_1' - (x_1 + x_1') \\ y_2 + y_2' - (x_2 + x_2') \end{pmatrix} && (1.5) \\ &= \Psi\left([(X + X', Y + Y')]\right) && (1.6) \end{aligned}$$

Für die Verträglichkeit mit Φ brauchen wir ein

lem:ort

Lemma 34. *Für $X, Y \in \mathbb{R}^2$ gilt $[(X,Y)] = [((0,0), Y - X)]$.*

Nun zur Verträglichkeit von Φ. Nach Lemma 34

$$B' := \tau_{\overrightarrow{CD}}(B) = B + C - D. \tag{1.7}$$

eq:short

Damit rechnen wir

$$\begin{aligned} \Phi\left([(A,B)]\right) + \Phi\left([(C,D)]\right) &= \tau_{\overrightarrow{AB}} + \tau_{\overrightarrow{CD}} = \tau_{\overrightarrow{CD}} \circ \tau_{\overrightarrow{AB}} && (1.8) \\ &= \tau_{\overrightarrow{BB'}} \circ \tau_{\overrightarrow{AB}} && (1.9) \\ &= \tau_{\overrightarrow{AB'}} && (1.10) \\ &= \tau_{\overrightarrow{A\ B+D-C}} && (1.11) \\ &= \tau_{\overrightarrow{0\ \tau_{\overrightarrow{A\ B+D-C}}(0)}} && (1.12) \\ &= \tau_{\overrightarrow{0\ B+D-C-A}} && (1.13) \\ &= \Phi\left([(0, B + D - C - A)]\right) && (1.14) \\ &= \Phi\left([(A + C, B + D)]\right) = \Phi\left([(A,B)]\right) + \Phi\left([(C,D)]\right) && (1.15) \end{aligned}$$

eq:1 eq:2 eq:3 eq:4 eq:5 eq:6 eq:7 eq:8

Dabei gilt (1.8) nach Definition von Φ und der Addition von Verschiebungen. Gleichung (1.9) ergibt sich aus (1.7) und (1.4). Gleichung (1.10) ist die Komposition von Verschiebungen mit den gleichen End- und Anfangspunkt, (1.11) ergibt sich wieder aus (1.7), (1.12) ergibt sich wieder aus (1.4) mit $P = (0, 0)$. Gleichung (1.13) erhält man aus Satz 32, (1.14) ist dann wieder die Definition von Φ, (1.15) ist Lemma 34 und die Definition der Addition.

Wir wollen nun auf $(\mathbb{R}^2)^*$, $(\mathbb{R}^2 \times \mathbb{R}^2)_\sim$ und den Verschiebungen jeweils eine Multiplikation mit einer Zahl $\lambda \in \mathbb{R}$ definieren definieren, die über Ψ und Φ miteinander verträglich sind. Für Vektoren $\overrightarrow{v}$, $X, Y, A, B \in \mathbb{R}^2$ seien

$$\lambda\overrightarrow{v} := \begin{pmatrix}\lambda v_1\\ \lambda v_2\end{pmatrix}, \quad \lambda[(X, Y)] := [(\lambda X, \lambda Y)], \quad \lambda\tau_{\overrightarrow{AB}} := \tau_{\lambda\overrightarrow{AB}}.$$

Den Beweis zur Verträglichkeit verläuft analog, daher wollen wir hier darauf verzichten.

Offenbar sind Addition und Multiplikation auf $(\mathbb{R}^2)^*$ und $\mathrm{Mat}_{2,1}$ identisch definiert. Auch werden die Elemente jeweils gleich notiert, daher wollen wir diese beiden Mengen identifizieren und in Zukunft nicht mehr unterscheiden:

$$\left(\mathbb{R}^2\right)^* = \mathrm{Mat}_{2,1}\,.$$

Völlig analog gehen wir für $n \in \mathbb{N}$ vor, das bedeutet wir betrachten

$$\mathrm{Mat}_{n,1} = (\mathbb{R}^n)^*$$

als Vektoren mit n Einträgen. Allerdings wollen wir weiterhin zwischen $n-$Tupeln als Elemente von $\mathbb{R}^n$ und Vektoren als Elemente von $\mathrm{Mat}_{n,1}$ unterscheiden.

1.2.3 Anwendungen in der elementaren Geometrie

Wir betrachten Punkte $V := (v_1, v_2)$ und $W := (w_1, w_2)$ in $\mathbb{R}^2$ und Vektoren

$$\overrightarrow{v} := \begin{pmatrix}v_1\\ v_2\end{pmatrix}, \quad \overrightarrow{w} := \begin{pmatrix}w_1\\ w_2\end{pmatrix}.$$

Damit gelten

$$\Psi\left([(V, W)]\right) = \overrightarrow{v} - \overrightarrow{w} \quad \text{und} \quad \Psi\left([((0, 0), V + W)]\right) = \overrightarrow{v} + \overrightarrow{w}.$$

Wir rechnen

$$\overrightarrow{w} + \tfrac{1}{2}(\overrightarrow{v} - \overrightarrow{w}) = \tfrac{1}{2}(\overrightarrow{v} + \overrightarrow{w}).$$

Das bedeutet, dass die Diagonalen in einem Parallelogramm sich jeweils in der Mitte schneiden.

1.3 Vektorräume

1.3.1 Einführung

Wir betrachten Vektoren $\overrightarrow{x}, \overrightarrow{y}, \overrightarrow{z} \in \mathrm{Mat}_{2,1}$. Wir beobachten nach Definition der Verküpfungen aus dem vorigen Abschnitt folgende Rechenregeln:

(GA) $(\overrightarrow{x} + \overrightarrow{y}) + \overrightarrow{z} = \overrightarrow{x} + (\overrightarrow{y} + \overrightarrow{z})$.

(GK) $\overrightarrow{x} + \overrightarrow{y} = \overrightarrow{y} + \overrightarrow{x}$.

(GN) Es gibt ein Element $\overrightarrow{0} \in \mathrm{Mat}_{2,1}$, so dass für jedes $\overrightarrow{x} \in \mathrm{Mat}_{2,1}$ gilt: $\overrightarrow{x} + \overrightarrow{0} = \overrightarrow{x}$. Wir können nämlich

$$\overrightarrow{0} := \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

wählen.

(GI) Zu jedem $\overrightarrow{x} \in \mathrm{Mat}_{2,1}$ gibt es ein $\overrightarrow{y} \in \mathrm{Mat}_{2,1}$, so dass $\overrightarrow{x} + \overrightarrow{y} = \overrightarrow{0}$ gilt. Wir können nämlich

$$\overrightarrow{y} := \overrightarrow{-}x := \begin{pmatrix} -x_1 \\ -x_2 \end{pmatrix}$$

wählen.

dfn:abgr

Definition 35. Eine Menge G heißt [abelsche] Gruppe, falls es eine Abbildung

$$+ : G \times G \to G$$

gibt, so dass mit der Abkürzung $g_1 + g_2 := +(g_1, g_2)$ die Gesetze (GA), [(GK)], (GN), und (GI) gelten. Wir schreiben dann auch $(G, +)$.

Beispiel 36. Beispiele für abelsche Gruppen sind:

1. $(\mathrm{Mat}_{n,1}, +)$
2. $(\mathbb{R}^n, +)$ mit der Addition aus Abschnitt 1.1.1.
3. $(\mathrm{Mat}_{m,n}, +)$ mit der Matrizenaddition
4. Übung: $\mathbb{P}_n := \{a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \,|\, a_i \in \mathbb{R}, 0 \leq i \leq n\}$ = die Menge der Polynome vom Grad $\leq n$.

Wir betrachten wieder $\overrightarrow{x} \in \mathrm{Mat}_{2,1}$ und $\lambda, \mu \in \mathbb{R}$. Wir beobachten nach Definition der Verküpfungen aus dem vorigen Abschnitt folgende Rechenregeln:

(D) $(\lambda + \mu)\overrightarrow{x} = \lambda \overrightarrow{x} + \mu \overrightarrow{x}$.

(A) $\lambda(\mu \overrightarrow{x}) = (\lambda\mu)\overrightarrow{x}$.

(N) Für $1 \in \mathbb{R}$ gilt: $1 \cdot \overrightarrow{x} = \overrightarrow{x}$.

Definition 37. Eine abelsche Gruppe G heißt Vektorraum, falls es eine Abbildung

$$\cdot : \mathbb{R} \times G \to G$$

gibt, für die mit der Abkürzung $\cdot(\lambda, g) := \lambda \cdot g := \lambda g$ die Gesetze (A), (D) und (N) gelten. Wir schreiben dann auch $(G, +, \cdot)$. Die Abbildung $\cdot$ nennt man Skalarmultiplikation.

Beispiel 38. Beispiele für Vektorräume sind

1. $(\mathrm{Mat}_{n,1}, +, \cdot)$ und $(\mathbb{R}^n, +, \cdot)$ mit den bereits behandelten Multiplikationen.
2. Übung: die Menge $\mathbb{P}_n$ mit welcher Multiplikation?

Beispiel 39.
1. Die Pauli-Matrizen bilden keine Gruppe.
2. $(\mathrm{Mat}_{2,2}, \cdot)$ mit der Multiplikation von Matrizen erfüllt (GA), (GN) mit $\overrightarrow{0} := E_2$, aber nicht (GK) und (GI).
3. $GL_{2,2} := \{A \in \mathrm{Mat}_{2,2} \mid A \text{ invertierbar}\}$ ist mit der Matrizenmultiplikation eine Gruppe.

Korollar 40. *In einem Vektorraum V gelten folgende Rechenregeln. Seien $\lambda \in \mathbb{R}$ und $\overrightarrow{x} \in V$.*

1. $0 \cdot \overrightarrow{x} = \overrightarrow{0}$

2. $\lambda \cdot \overrightarrow{x} = \overrightarrow{0} \quad \Rightarrow \quad \lambda = 0$ *oder* $\overrightarrow{x} = \overrightarrow{0}$.

3. $(-1) \cdot \vec{x} = -\vec{x}$.

Beweis □

1.3.2 Untervektorräume

Definition 41. Es sei V ein Vektorraum. Eine Teilmenge $U \subset V$ heißt Untervektorraum von V, falls U selbst ein Vektorraum ist.

Satz 42. *Es sei V ein Vektorraum. Eine Teilmenge $U \subset V$ ist genau dann ein Untervektorraum von V, falls $U = \emptyset$ oder*

1. $\forall\, \overrightarrow{v}, \overrightarrow{w} \in U \;:\; \overrightarrow{v} + \overrightarrow{w} \in U$ *und*

2. $\forall\, \overrightarrow{v} \in U \;\; \forall\, \lambda \in \mathbb{R} \;:\; \lambda \cdot \overrightarrow{v} \in U$

gelten.

Beweis □

Beispiel 43.

1. Für $\overrightarrow{v} \in \mathbb{R}^n$ ist $\{\lambda\overrightarrow{v} \mid \lambda \in \mathbb{R}\}$ ein Untervektorraum von $\mathbb{R}^n$.

2. $\mathbb{L}_{(A|0)}$ ist ein Untervektorraum von $\mathrm{Mat}_{n,1}$, denn entweder ist die Lösungsmenge leer oder für $\overrightarrow{x}, \overrightarrow{y} \in \mathrm{Mat}_{n,1}$ und $\lambda \in \mathbb{R}$ gelten:

$$A(\overrightarrow{x} + \overrightarrow{y}) = A\overrightarrow{x} + A\overrightarrow{y} = \overrightarrow{0} + \overrightarrow{0} = \overrightarrow{0} \text{ und } A(\lambda\overrightarrow{x}) = \lambda A\overrightarrow{x} = \lambda \cdot \overrightarrow{0} = \overrightarrow{0}.$$

1.3.3 Linerkombination und Erzeugnis

Definition 44. Es sei V ein Vektorraum und $M \subset V$ eine nicht-leere Teilmenge.

1. Für $n \in \mathbb{N}$, $\lambda_i \in \mathbb{R}$ und $\overrightarrow{v}_i \in V$, $1 \leq i \leq n$, heißt das Element

$$\sum_{i=1}^{n} \lambda_i \overrightarrow{v}_i \ \in V$$

eine Linearkombination aus Elementen von V.

2. Die Menge aller Linearkombiationen

$$< M >:= \left\{ \sum_{i=1}^{n} \lambda_i \overrightarrow{v}_i \mid \lambda_i \in \mathbb{R}, \overrightarrow{v}_i \in V, 1 \leq i \leq n, n \in \mathbb{N} \right\}$$

heißt Erzeugnis von M.

3. Für ein Erzeugnis $< M >$ nennt man M das Erzeugendensystem. Falls M endlich ist, heißt $< M >$ endlich erzeugt.

Beispiel 45.

$$\left\langle \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\rangle = \left\{ \lambda_1 \begin{pmatrix} 0 \\ 1 \end{pmatrix} + \lambda_2 \begin{pmatrix} 1 \\ 1 \end{pmatrix} \mid \lambda_1, \lambda_2 \in \mathbb{R} \right\} = \mathbb{R}^2$$

Satz 46. *Es sei V ein Vektorraum und $M \subset V$ eine Teilmenge von V. Dann ist $< M > \subset V$ ein Untervektorraum von V.*

Beweis □

Beispiel 47. Die Lösungen eines homogenen LGS lassen sich nach Satz 23 als Erzeugnis von Vektoren schreiben, die man aus einer sZSTF der Koeffizientenmatrix gewinnt.

Zur Motivation der nächsten Definition betrachten wir folgendes

ex:lu

Beispiel 48. 1. Vorgelegt seien die beiden Vektoren

$$\overrightarrow{x} := \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad \overrightarrow{y} := \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Aus diesen kann man den Nullvektor nur trivial kombinieren, denn aus $\lambda\overrightarrow{x} + \mu\overrightarrow{y} = \overrightarrow{0}$ folgt nach kurzer Rechnung $\lambda = \mu = 0$.

2. Betrachten wir zusätzlich
$$\overrightarrow{z} := \begin{pmatrix}1\\0\end{pmatrix},$$
gilt $\overrightarrow{0} = \overrightarrow{x} - \overrightarrow{z} - \overrightarrow{y}$. Hier läßt sich der Nullvektor also nicht-trivial als Linearkombination von $\overrightarrow{x}, \overrightarrow{y}$ und $\overrightarrow{z}$ schreiben.

dfn:lu

Definition 49. Es sei V ein Vektorraum und $M \subset V$.

1. M heißt linear unabhängig, falls gilt:
$$\forall k \in \mathbb{N}\ \forall \overrightarrow{v}_1, \ldots, \overrightarrow{v}_k \in M\ \forall \lambda_1, \ldots, \lambda_k \in \mathbb{R}\ :\ \sum_{i=1}^{k} \lambda_i \overrightarrow{v}_i = \overrightarrow{0} \Rightarrow \lambda_1 = \cdots = \lambda_k = 0.$$

2. M heißt linear abhängig, falls M nicht linear unabhängig ist.

Bemerkung 50. Die formale Negation von 49.1 ergibt das Kriterium zur linearen Abhängigkeit einer Menge $M \subset V$.
$$\exists k \in \mathbb{N}\ \exists \overrightarrow{v}_1, \ldots, \overrightarrow{v}_k \in M\ \exists \lambda_1, \ldots, \lambda_k \in \mathbb{R}\ :\ \sum_{i=1}^{k} \lambda_i \overrightarrow{v}_i = \overrightarrow{0} \text{ und } (\exists i \in \{1, \ldots, k\} : \lambda_i \neq 0)\,.$$
Eine M ist also linear abhängig, falls es in M eine nicht-triviale Linearkombination des Nullvektors gibt.

ex:lula

Beispiel 51.

1. Die Vektoren in 48.1 sind linear unabhängig. Die Vekroen in 48.2 sind linear abhängig.

2. Die leere Menge ist linear unabhängig.

3. Ist $\overrightarrow{0} \in M$, so ist M linear abhängig, denn $1 \cdot \overrightarrow{0} = \overrightarrow{0}$ ist eine nicht-triviale Linearkombination der Null.

4. Es seien $\overrightarrow{v}_1, \ldots, \overrightarrow{v}_n \in \mathbb{R}^m$ und $A \in \mathrm{Mat}_{m,n}$. Die i-te Spalte von A bestehe aus $\overrightarrow{v}_i$. Dann gilt
$$\overrightarrow{v}_1, \ldots, \overrightarrow{v}_n \text{ linear unabhängig } \Leftrightarrow\ \mathbb{L}_{(A|0)} = \{\overrightarrow{0}\}.$$

5. Gilt $n > m$ in Teil 4. dieses Beispiels, dann sind die Vektoren linear abhängig. Daraus folgt zum Beispiel, dass 4 Vektoren in $\mathbb{R}^3$ immel linear abhängig sind.

6. $\{1, x, x^1, \ldots, x^n\} \subset \mathbb{P}_n$ ist linear unabhängig, denn aus $\sum_{i=1}^{n} \lambda_i x^i = 0$ folgt, dass alle Koeffizienten Null sein müssen.

Definition 52. Sei V ein Vektorraum. Eine Menge $M \subset V$ heißt Basis von V, falls $< M >= V$ gilt und M linear unabhängig ist.

Beispiel 53.

1. Es sei $e_i \in \mathbb{R}^n$ derjenige Vektor, der an der i-ten Stelle eine 1 und sonst nur Nullen hat. Damit ist $\{e_1, \ldots, e_n\}$ eine Basis von $\mathbb{R}^n$.

2. Es sei $E_{i,j} \in \mathrm{Mat}_{m,n}$ diejenige Matrix, die im (i,j)-ten Eintrag eine 1 und sonst nur Nullen hat. Damit ist $\{E_{i,j} \mid 1 \leq i \leq m, 1 \leq j \leq n\}$ eine Basis von $\mathrm{Mat}_{m,n}$.

3. $\{1, x, x^1, \ldots, x^n\} \subset \mathbb{P}_n$ ist eine Basis von $\mathbb{P}_n$.

4. Wir betrachhten die Menge aller Polynome

$$\mathcal{P} := \bigcup_{n \in \mathbb{N}} \mathbb{P}_n$$

zusammen mit der Addition und Skalarmultiplikation, die wie in $\mathbb{P}_n$ definiert sind. Damit ist $\mathcal{P}$ ein Vektorraum mit nicht endlicher Basis $\{1, x, x^1, \ldots, x^n, \ldots\} \subset \mathcal{P}$

5. Die Vektoren in der Darstellung von $\mathbb{L}_{(A|0)}$ in Satz 23 bilden eine Basis für den Vektorraum $\mathbb{L}_{(A|0)}$.

1.3.4 Basisauswahlsatz

Im vorigen Kapitel haben wir für spezielle Vektorräume Basen angeben können. Wir wenden uns nun der Frage zu, ob jeder Vektorraum eine Basis hat.

lem:charla

Lemma 54. *Eine nicht-leere Teilmenge M eines Vektorraumes V ist genau dann linear abhängig, wenn:*

$$\exists\, \overrightarrow{v} \in M \;:\; \overrightarrow{v} \in < M \backslash \{\overrightarrow{v}\} > .$$

.

Beweis □

thm:charbasis

Satz 55. *Es sei $M := \{\overrightarrow{v}_1, \ldots, \overrightarrow{v}_n\} \subset V$ eine endliche Teilmenge eines Vektorraumes V. Es sind äquivalent:*

1. *M ist eine Basis von V.*
2. *$< M >= V$ und für jedes $\overrightarrow{v}_i \in M$ gilt: $< M \backslash \{\overrightarrow{v}_i\} > \neq V$. Nenne M dann unverkürzbares Erzeugendensystem von V.*
3. *M ist linear unabhängig und für jedes $\overrightarrow{v} \in V$ gilt: $M \cup \{\overrightarrow{v}\}$ ist linear abhängig. Nenne M dann unverlängerbar linear unabhängig.*
4. *Jedes $\overrightarrow{v} \in V$ ist eindeutig als Linearkombination mit Elementen aus M darstellbar.*

Beweis □

thm:basisauswahl

Satz 56 (Basisauswahlsatz)**.** *Es sei $M \subset V$ eine endliche Teilmenge eines Vektorraumes V mit $< M >= V$. Dann gibt es eine Teilmenge von M, die eine Basis von V ist.*

Beweis Man nimmt so lange Elemente aus M heraus, bis ein unverkürzbares Erzeugendensystem vorliegt. Satz 56 liefert dann die Behauptung. □

1.3.5 Basisaustauschsatz

Das folgende Lemma ist der Schlüssel zum Beweis des Basisaustauschsatzes. Es besteht aus zwei ähnlichen Aussagen. Aus einem Erzeugendensystem (bzw. linear unabhängigen Menge) kann man einen Vektor durch einen anderen ersetzen, sofern in seiner Dartstellung als Linearkombination der auszutauschende Vektor vorkommt.

lem:austausch

Lemma 57 (Austauschlemma)**.** *Es seien V ein Vektorraum, $M := \{\overrightarrow{v}_1, \ldots, \overrightarrow{v}_n\} \subset V$ sowie $\overrightarrow{w} := \sum_{i=1}^{n} \lambda_i \overrightarrow{v}_i \in V$ mit $\lambda_k \neq 0$ für ein $k \in \{1, \ldots, n\}$. Es gelten:*

1. $< M >= V \Rightarrow < (M \backslash \{\overrightarrow{v}_k\}) \cup \{\overrightarrow{w}\} >= V$
2. *M linear unabhängig* $\Rightarrow < (M \backslash \{\overrightarrow{v}_k\}) \cup \{\overrightarrow{w}\} >$ *linear unabhängig*

Beweis □

Beispiel 58. Bevor wir den Austauschsatz formulieren, diskutieren wir praktische Anwendungen des austauschlemmas in $\mathbb{R}^n$.

1. Vektoren auf lineare Unabhängigkeit prüfen. Gegeben seien drei Vektoren

$$\begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix}, \quad \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \quad \begin{pmatrix} 4 \\ 2 \\ 1 \end{pmatrix} \in \mathbb{R}^3.$$

   Schreiben wir die Vektoren in die Zeilen einer Matrix und bringen diese auf Zeilenstufenform, so erhalten wir zum Beispiel:

$$\begin{pmatrix} 3 & 2 & 1 \\ 1 & 0 & 1 \\ 4 & 2 & 1 \end{pmatrix} \quad \mapsto \cdots \mapsto \quad \begin{pmatrix} 1 & 0 & 1 \\ 0 & 2 & -2 \\ 0 & 0 & -1 \end{pmatrix}$$

   Die Zeilenumformungen (in beide Richtungen) sind Austauschschritte gemäß Lemma 57. Daher kann man and der ZSTF ablesen, ob die Vekoren linear unabhängig sind. In diesem Beispiel sind sie es.

2. Basis eines Erzeugnisses berechnen. Gegeben seien drei Vektoren

$$\begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix}, \quad \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \quad \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \in \mathbb{R}^3.$$

   Schreiben wir die Vektoren in die Zeilen einer Matrix und bringen diese auf Zeilenstufenform, so erhalten wir zum Beispiel:

$$\begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 2 & 1 & 1 \end{pmatrix} \quad \mapsto \quad \begin{pmatrix} 1 & 1 & 0 \\ 0 & -1 & 1 \\ 0 & -1 & 1 \end{pmatrix} \quad \mapsto \quad \begin{pmatrix} 1 & 1 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

Die Zeilenumformungen (in beide Richtungen) sind Austauschschritte gemäß Lemma 57. Daher kann man and der ZSTF ablesen, welche Vekoren erzeugen. In diesem Beispiel ergibt sich

$$M = \left\langle \left\{ \begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \right\} \right\rangle = \left\langle \left\{ \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ -1 \\ 1 \end{pmatrix} \right\} \right\rangle.$$

Daher ist insbesondere

$$\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ -1 \\ 1 \end{pmatrix}$$

eine Basis von M.

thm:bauss

Satz 59 (Basisaustauschsatz)**.** *Es sei $\mathcal{B}$ eine endliche Basis eines Vektorraums V und $L \subset V$ eine linear unabhängige Teilmenge. Dann gibt es $K \subset \mathcal{B}$, so dass $|K| = |L|$ gilt und $(\mathcal{B} \backslash K) \cup L$ eine Basis von V ist.*

Beweis Ausgelassen. □

Bemerkung 60. Satz 59 besagt, dass im Falle einer endlichen Basis $\mathcal{B}$ jede linear unabhängige Teilmenge weniger oder genauso viele Elemente hat wie $\mathcal{B}$ und dass diese in die Basis eingewechselt werden kann.

1.3.6 Basisergänzungssatz

thm:berg

Satz 61. *Es sei V ein endlich erzeugter Vektorraum und $L =: \{\overrightarrow{v}_1, \ldots, \overrightarrow{v}_m\} \subset V$ eine linear unabhängige Teilmenge. Dann gibt es Vektoren $\{\overrightarrow{v}_{m+1}, \ldots, \overrightarrow{v}_n\}$, so dass $\{\overrightarrow{v}_1, \ldots, \overrightarrow{v}_n\}$ eine Basis von V ist.*

Beweis □

1.3.7 Dimension

cor:dim1

Korollar 62. *Hat ein Vektorraum eine Basis mit endlich vielen Elementen, dann hat jede Basis endlich viele Elemente.*

Beweis Ausgelassen. □

cor:dim2

Korollar 63. *Je zwei endliche Basen eines Vektorraumes haben gleich viele Elemente.*

Beweis □

thm:haupt1

Theorem 64. *Jeder Vektorraum hat eine Basis.*

Beweis Ausgelassen. □

dfn:dim

Definition 65. Die Dimension eines Vektorraumes ist definiert durch

$$\dim V := \begin{cases} r & : \text{ Es gibt eine Basis der Länge } r \in \mathbb{N}. \\ \infty & : \text{ Es gibt keine endliche Basis.} \end{cases}$$

Bemerkung 66. rem:dim

1. Der Beweis zu 64 verwendet Hilfsmittel aus der Mengenlehre, sofern der Vektorraum nicht endlich erzeugt ist.
2. Wegen der Korollare 62 und 63 ist der Begriff der Dimension wohldefiniert.
3. $\dim \mathbb{R}^n = n, \quad \dim \mathrm{Mat}_{m,n} = mn, \quad \dim \mathbb{P}_n = n$
4. Aus Satz 23 ergibt sich $\dim \mathbb{L}_{(A|0)} = n - r$.

cor:uvrdim

Korollar 67. *Es seien $W \subset V$ endlich erzeugte Vektorräume. Dann gelten:*

1. $\dim W \leq \dim V$,

2. $\dim W = \dim V \Rightarrow V = W$.

Beweis (2. ausgelassen) □

1.4 Situation in $\mathbb{R}^3$

1.4.1 Untervektorräume von $\mathbb{R}^3$

Es sei $U \subset \mathbb{R}^3$ ein Untervektorraum. Nach Korollar 67 gilt $0 \leq \dim U \leq 3$. Für $\dim U = 0$ ergibt sich $U = \{\overrightarrow{0}\}$. Für $\dim U = 1$ gibt es also eine Basis der Länge 1, daher gibt es einen Vektor $\overrightarrow{v} \neq 0$, so dass $U =< \overrightarrow{v} >$ gilt. In diesem Fall nennt man U eine Gerade. Für $\dim U = 2$ gibt es also eine Basis der Länge 2, daher gibt es linear unabhängige Vektoren $\overrightarrow{w}, \overrightarrow{v}$, so dass $U =< \overrightarrow{v}, \overrightarrow{w} >$ gilt. In diesem Fall nennt man U eine Ebene. Im Falle $\dim U = 3$ folgt $U = \mathbb{R}^3$ aus Korollar 67.

1.4.2 Ebenen in $\mathbb{R}^3$

Es sei $A \in \mathrm{Mat}_{m,3}$ und $(A|0)$ eine erweiterte Koeffizientenmatrix eines LGS. Aus einer ZSTF A' von A lesen wir wie in Satz 23 die Zahl $r \in \{0, 1, 2, 3\}$ ab. Es gilt dann $\dim \mathbb{L}_{(A|0)} = 3 - r$ gemäß Bemerkung 66, daher liefert jedes r einen der obigen Fälle, denn die Lösungsmenge eines LGS ist ein Untervektorraum. Für $r = 1$ ist eine sZSTF von der Gestalt $A' = (1 \quad b \quad c) \in \mathrm{Mat}_{1,3}$. Insbesondere liefert also ein LGS $ax_1 + bx_2 + cx_3 = 0$ einen Untervektorraum der Dimension 2, also eine Ebene in $\mathbb{R}^3$.

Es sei umgekehrt zu linear unabhängigen Vektoren $\overrightarrow{v}, \overrightarrow{w} \in \mathbb{R}^3$ eine Ebene

$$E_{\overrightarrow{v},\overrightarrow{w}} := \{\lambda_1 \overrightarrow{v} + \lambda_2 \overrightarrow{w} \mid \lambda_1, \lambda_2 \in \mathbb{R}\} =< \overrightarrow{v}, \overrightarrow{w} >$$

vorgelegt. Wir definieren das Kreuzprodukt von $\overrightarrow{v}$ mit $\overrightarrow{w}$ durch

$$\overrightarrow{n} := \begin{pmatrix} v_2w_3 - w_2v_3 \\ -(v_1w_3 - w_1v_3) \\ v_1w_2 - w_1v_2 \end{pmatrix} \in \mathbb{R}^3.$$

Wir definieren $A := (n_1 \quad n_2 \quad n_3)$ und rechnen nach, dass $A\overrightarrow{v} = A\overrightarrow{w} = \overrightarrow{0}$ gilt. Damit gilt $\overrightarrow{v}, \overrightarrow{w} \in \mathbb{L}_{(A|0)}$, also $< \overrightarrow{v}, \overrightarrow{w} > \subset \mathbb{L}_{(A|0)}$. Aus Korollar 67 folgt daher $< \overrightarrow{v}, \overrightarrow{w} > = \mathbb{L}_{(A|0)}$.

1.4.3 Skalarprodukt

Für

$$\overrightarrow{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}, \quad \overrightarrow{y} = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} \in \mathbb{R}^3$$

heißt

$$\overrightarrow{x} \cdot \overrightarrow{y} := x_1y_1 + x_2y_2 + x_3y_3 \in \mathbb{R}$$

das Skalarprodukt von $\overrightarrow{x}$ und $\overrightarrow{y}$. Zwei Vektoren $\overrightarrow{x}, \overrightarrow{y} \in \mathbb{R}^3$ heißen senkrecht zueinander, falls $\overrightarrow{x} \cdot \overrightarrow{y} = 0$ gilt. In $\mathbb{R}^3$ bedeutet dies, dass die Vektoren einen Winkel von 90 Grad einschließen. Ein Winkel soll hier (aus Zeitgründen) nicht näher definiert werden, sondern aus der Anschauung plausibel sein. Die Standardvektoren stehen zum Beispiel paarweise aufeinander senkrecht.

Für zwei linear unabhängige Vektoren $\overrightarrow{v}$, $\overrightarrow{w}$ und deren Kreuzprodukt $\overrightarrow{n}$ mit $A := (n_1 \quad n_2 \quad n_3)$ kann man also schreiben:

$$E_{\overrightarrow{v},\overrightarrow{w}} = \mathbb{L}_{(A|0)} = \{\overrightarrow{x} \in \mathbb{R}^3 \mid \overrightarrow{n} \cdot \overrightarrow{x} = 0\}.$$

Man nennt $\overrightarrow{n}$ den Normalenvektor zu $E_{\overrightarrow{v},\overrightarrow{w}}$. Er steht auf jedem Vektor der Ebene senkrecht. Andersherum läßt sich jede Ebene durch einen Normalenvektor ausdrücken.

1.5 Lineare Abbildungen

1.5.1 Einführung

Bekannt sind Funktionen vom Typ $f : \mathbb{R}^1 \to \mathbb{R}^1$. Diese sind im allgemeinen „nicht linear“, beispielsweise $f(x) := x^3 + 4$ oder $f(x) := \sin x$. Wir wollen uns nun auf lineare Abbildungen beschränken, aber dafür die Dimensionen von Definitions- und Wertebereich erhöhen.

Definition 68. Eine Abbildung $f : V \to W$ zwischen Vektorräumen V und W heißt linear falls

1. $\forall\ \overrightarrow{v}_1, \overrightarrow{v}_2 \in V\ :\ f(\overrightarrow{v}_1 + \overrightarrow{v}_2) = f(\overrightarrow{v}_1) + f(\overrightarrow{v}_2)$ und
2. $\forall\ \overrightarrow{v} \in V\ \forall\lambda \in \mathbb{R}\ :\ f(\lambda\overrightarrow{v}) = \lambda f(\overrightarrow{v})$

gelten.

ex:linear

Beispiel 69. 1. $f : \mathbb{R} \to \mathbb{R}, \quad f(x) := ax, \quad a \in \mathbb{R}$

2. $f : \mathbb{R}^2 \to \mathbb{R}^3, \quad f(x_1, x_2) := (x_1 - x_2, 2x_2 + x_1, x_2)$. Manchmal ist es praktischer, die Abbildung vektoriell aufzuschreiben:
$$f\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}\right) := \begin{pmatrix} x_1 - x_2 \\ 2x_2 + x_1 \\ x_2 \end{pmatrix}.$$
Beise Schreibweisen sind geläufig.

3. $f : \mathbb{R}^n \to \mathbb{R}^m, \quad f(\overrightarrow{x}) := \overrightarrow{a}$ ist genau für $\overrightarrow{a} = \overrightarrow{0}$ linear, denn:
$$\overrightarrow{a} = f(\overrightarrow{x} + \overrightarrow{x}) = f(\overrightarrow{x}) + f(\overrightarrow{x}) = 2\overrightarrow{a} \Leftrightarrow \overrightarrow{a} = \overrightarrow{0}.$$

4. $f : \mathbb{R}^2 \to \mathbb{R}, \quad f(x_1, x_2) := x_1 \cdot x_2$ ist nicht linear, denn:
$$f(1,0) + f(0,1) = 0 \neq 1 = f(1,1) = f((1,0) + (0,1)).$$

5. Es sei $f : \mathbb{R}^n \to \mathbb{R}^m$ und $A \in \mathrm{Mat}_{n,m}$. Wir definieren f durch $f(\overrightarrow{x}) := A\overrightarrow{x}$. Damit ist f linear, denn für $\overrightarrow{x}, \overrightarrow{y} \in \mathbb{R}^n$ gilt
$$f(\overrightarrow{x} + \overrightarrow{y}) = A(\overrightarrow{x} + \overrightarrow{y}) = A\overrightarrow{x} + A\overrightarrow{y} = f(\overrightarrow{x}) + f(\overrightarrow{y})$$
$$\text{und für } \lambda \in \mathbb{R} : f(\lambda\overrightarrow{x}) = A(\lambda\overrightarrow{x}) = \lambda(A\overrightarrow{x}) = \lambda f(\overrightarrow{x}).$$
Dieses Beispiel zeigt, dass man eine linerae Abbildung durch eine Matrix erhalten kann. Später sehen wir, dass umgekehrt jede lineare Abbildung durch eine Matrix gegeben ist.

Lineare Abbildungen sind in der Geometrie wichtig, dnn sie beschreiben Spiegelungen und Drehungen des Raumes.

ex:dreh

Beispiel 70 (Drehungen)**.** Für $\alpha \in \mathbb{R}$ betarchten wir $f : \mathbb{R}^2 \to \mathbb{R}^2$ gegeben durch die Matrix
$$D_\alpha := \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}.$$
Es sei $\overrightarrow{v} = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} \in \mathbb{R}^2$, so dass der Punkt (v_1, v_2) auf dem Einheitskreis in $\mathbb{R}^2$ liegt. Wir wollen zeigen, dass der Vektor $f(v_1, v_2)$ aus $\overrightarrow{v}$ durch Drehung um den Winkel α hervorgeht. Da $\overrightarrow{v}$ auf dem Einheitskreis liegt, gilt
$$\overrightarrow{v} = \begin{pmatrix} \cos\beta \\ \sin\beta \end{pmatrix}.$$

Es sei $\overrightarrow{w} = \begin{pmatrix} w_1 \\ w_2 \end{pmatrix}$ der Vektor, der durch Drehung aus $\overrightarrow{v}$ um den Winkel α hervorgeht. Dann gilt

$$\overrightarrow{w} = \begin{pmatrix} \cos(\alpha+\beta) \\ \sin(\alpha+\beta) \end{pmatrix}$$

Dazu rechnen wir

$$\begin{aligned} f(v_1, v_2) &= \begin{pmatrix} v_1\cos\alpha - v_2\sin\alpha \\ v_1\sin\alpha + v_2\cos\alpha \end{pmatrix} = \begin{pmatrix} \cos\alpha\cos\alpha - \sin\alpha\sin\alpha \\ \cos\alpha\sin\alpha + \sin\alpha\cos\alpha \end{pmatrix} && (1.16) \\ &= \begin{pmatrix} \cos(\alpha+\beta) \\ \sin(\alpha+\beta) \end{pmatrix} := \begin{pmatrix} w_1 \\ w_2 \end{pmatrix} =: \overrightarrow{w} && (1.17) \end{aligned}$$

Also entsteht $\overrightarrow{w}$ aus $\overrightarrow{v}$ durch Drehung um den Winkel α.

1.5.2 Lineare Abbildungen mit Basen

Bemerkung 71. Es sei $\mathcal{B} := \{\overrightarrow{v}_1, \ldots, \overrightarrow{v}_n\}$ Basis eines Vektorraumes V und $f : V \to W$ eine linerae Abbildung. Es sei $\overrightarrow{v} \in V$ ein Vektor. Diesen kann man nach Satz 55 eindeutig durch die Basis $\mathcal{B}$ ausdrücken, also $\overrightarrow{v} = \sum_{i=1}^{n} \lambda_i \overrightarrow{v}_i$. Dann gilt

$$f(\overrightarrow{v}) = f\left(\sum_{i=1}^{n} \lambda_i \overrightarrow{v}_i\right) = \sum_{i=1}^{n} \lambda_i f(\overrightarrow{v}_i).$$

Das bedeutet, die Abbildung f ist durch die Bilder auf den Basisvektoren eindeutig festgeleg.

Nach Beispiel 69.5 liefern Matrizen lineare Abbildungen. Umgekehrt gilt: jede lineare Abbildung $f : \mathbb{R}^n \to \mathbb{R}^m$ läßt sich durch eine Matrix ausdrücken. Das ist die Aussage des folgenden

thm:fdurchmatrix

Satz 72. *Es sei $f : \mathbb{R}^n \to \mathbb{R}^m$ eine lineare Abbildung. Es seien $\mathcal{B} := \{\overrightarrow{e}_1, \ldots, \overrightarrow{e}_n\}$ bzw. $\mathcal{B}' := \{\overrightarrow{e}'_1, \ldots, \overrightarrow{e}'_m\}$ die Standardbasen von $\mathbb{R}^n$ bzw. $\mathbb{R}^m$. Für $j \in \{1, \ldots, n\}$ sei*

$$f(\overrightarrow{e}_j) = \sum_{i=1}^{m} a_{i,j} \overrightarrow{e}'_i = \begin{pmatrix} a_{1,j} \\ a_{2,j} \\ \vdots \\ a_{m,j} \end{pmatrix}.$$

Definiere $A \in \mathrm{Mat}_{m,n}$ durch $A_{i,j} := a_{i,j}$ für $1 \le i \le m, 1 \le j \le n$. Dann ist f eindeutig durch $f(\overrightarrow{x}) := A\overrightarrow{x}$ festgelegt.

Beweis □

ex:fmatrix

Beispiel 73. Wir betrachten $f : \mathbb{R}^2 \to \mathbb{R}^3$ gegeben durch $f(x_1, x_2) := (x_1 + x_2, x_1, 2x_2 - x_1)$. Dann gelten:

$$f(1,0) = (1,1,-1) = 1 \cdot \overrightarrow{e}'_1 + 1 \cdot \overrightarrow{e}'_2 - \overrightarrow{e}'_3$$

$$f(0,1) = (1,0,2) = 1 \cdot \overrightarrow{e}'_1 + 0 \cdot \overrightarrow{e}'_2 + 2 \cdot \overrightarrow{e}'_3.$$

Definiert man nun

$$A := \begin{pmatrix} 1 & 1 \\ 1 & 0 \\ -1 & 2 \end{pmatrix}$$

so gilt $f(\overrightarrow{x}) = A\overrightarrow{x}$ nach Satz 72.

Bemerkung 74. In Satz 72 gilt also kurz gesagt: in der j-ten Spalte steht das Bild des j-ten Basisvektors.

1.5.3 Kern, Bild und Rang

Es sei $f : V \to W$ eine lineare Abbildung zwischen endlich erzeugten Vektorräumen.

dfn:kernbild

Definition 75. Das Urbild des Nullvektors $\overrightarrow{0} \in W$ heißt Kern von f und man schreibt $\operatorname{Kern} f := f^{-1}(\overrightarrow{0}) = \{\overrightarrow{v} \in V \mid f(\overrightarrow{v}) = \overrightarrow{0}\}$. Das Bild von f ist definiert duch $\operatorname{Bild} f := \{f(\overrightarrow{v}) \mid \overrightarrow{v} \in V\}$.

cor:kernbild

Korollar 76. *Kern und Bild einer linearen Abbildung sind Untervektorräume.*

Beweis Übung □

dfn:rang

Definition 77. Der Rang von f ist die Dimension des Bildes von f und man schreibt $\operatorname{Rang} f := \dim \operatorname{Bild} f$. Der Rang einer Matrix ist der Rang der zugehörigen linearen Abbildung und man schreibt $\operatorname{Rang} A$.

rem:erzbild

Bemerkung 78. Es sei $f : \mathbb{R}^n \to \mathbb{R}^m$ linear und gegeben durch die Matrix A. Die Spalten der Matrix seien $a^1, \ldots, a^n \in \mathrm{Mat}_{m,1}$. Dann gilt

$$\operatorname{Bild} f =< A\overrightarrow{x} \mid \overrightarrow{x} \in \mathbb{R}^n >=< \{a^1, \ldots, a^n\} > .$$

Das Bild wird also von den Spalten der Matrix erzeugt.

cor:erzbild

Korollar 79. *In Bemerkung 78 ist der Rang von f bzw. der Rang von A gleich der maximalen Anzahl unabhängiger Spalten von A.*

Beweis □

Beispiel 80.

1. Die Spalten a^1, a^2 der Drehmatrix aus Beispiel 70 stehen wegen $a^1 \cdot a^2 = 0$ senkrecht aufeinander. Daher sind sie linear unabhängig (Übung), also ist der Rang der Drehmatrix gleich zwei.

2. Wir betrachten die Matrix

$$A := \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix}.$$

Man rechnet

$$f(x_1, x_2) = A \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = x_1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + x_2 \begin{pmatrix} 2 \\ 0 \end{pmatrix}.$$

Daher ist

$$\text{Bild } f = \left\langle \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \end{pmatrix} \right\rangle = \left\langle \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\rangle$$

Also $\text{Rang } f = 1$. Geometrisch ist das Bild daher die x_1-Achse von $\mathbb{R}^2$. Der Kern von f berechnet sich so:

$$\text{Kern } f = \{(x_1, x_2) \,|\, (0,0) = f(x_1, x_2)\} = \{(x_1, x_2) \,|\, x_2 = -\tfrac{1}{2}x_1\}.$$

Geometrisch ist der Kern also eine Gerade in $\mathbb{R}^2$ mit Steigung $-\frac{1}{2}$.

Satz 81 (Dimensionsformel)**.** *Es sei $f : V \to W$ eine lineare Abbildung zwischen endlich erzeugten Vektorräumen V und W. Dann gilt*

$$\dim V \;=\; \dim \text{Bild } f \;+\; \text{Rang } f.$$

Beweis □

Lemma 82. *Es sei $A \in \text{Mat}_{m,m}$ invertierbar und f die zugehörige linerae Abbildung. Dann gelten*

1. *$\overrightarrow{v}_1, \ldots, \overrightarrow{v}_m \in \mathbb{R}^m$ linear unabhängig $\Rightarrow$ $A\overrightarrow{v}_1, \ldots, A\overrightarrow{v}_m \in \mathbb{R}^m$ linear unabhängig*
2. *$\text{Rang } f = m$, $\text{Kern } f = \{\overrightarrow{0}\}$*

Die zweite Aussage bedeutet, dass lineare Abbildungen, die durch invertierbare Matrizen gegeben sind, sowohl surjektiv als auch injektiv (Übung) sind.

1.5.4 Anwendung auf LGS

Es sei $A \in \text{Mat}_{m,n}$ Koeffizientenmatrix eines LGS mit rechter Seite $\overrightarrow{b} \in \mathbb{R}^m$. Sei $f : \mathbb{R}^n \to \mathbb{R}^m$, $f(\overrightarrow{x}) = A\overrightarrow{x}$ die zugehörige lineare Abbildung. Dann gelten $\mathbb{L}_{(A|0)} = \text{Kern } f$ und $\mathbb{L}_{(A|\overrightarrow{b})} = f^{-1}(\overrightarrow{b})$. Nach Bemerkung 66 gilt also $n - r = \dim \text{Kern } f$ wobei r aus einer sZSTF von A kommt.

thm:ranZSTF

Satz 83. *Sei $A \in \text{Mat}_{m,n}$ und $r \in \mathbb{N}$ aus der sZSTF von A wie in Definiton 18. Dann gilt $r = \text{Rang } A$.*

Mit dem Rangbegriff können wir nun Lösungsmengen von LGS charakterisieren.

Satz 84. *Es sei $A \in \text{Mat}_{m,n}$, $\overrightarrow{b} \in \mathbb{R}^m$ und $(A|\overrightarrow{b})$ erweiterte Koeffizintenmatrix eines LGS. Dann gelten:*

1. *$\text{Rang}(A|\overrightarrow{b}) = \text{Rang } A \;\Leftrightarrow$ LGS ist lösbar mit $\dim \mathbb{L}_{(A|0)} = n - \text{Rang } A$*
2. *$\text{Rang}(A|\overrightarrow{b}) > \text{Rang } A \;\Leftrightarrow$ LGS ist nicht lösbar*

Beweis Ergibt sich direkt aus Satz 28 und Satz 83. □

Beispiel 85. Wir betrachten eine erweiterte Koeffizientenmatrix $A|\overrightarrow{b}$) wie folgt:

$$\left(\begin{array}{cccccc|c} 0 & 1 & 1 & 2 & 0 & 2 & b_1 \\ 0 & -1 & -1 & 2 & 0 & 0 & b_2 \\ 0 & 0 & 0 & 2 & 0 & 1 & b_3 \end{array}\right) \quad \left(\begin{array}{cccccc|c} 0 & 1 & 1 & 2 & 0 & 1 & b_1 \\ 0 & 0 & 0 & 4 & 0 & 2 & b_1 + b_2 \\ 0 & 0 & 0 & 2 & 0 & 1 & b_3 \end{array}\right)$$

$$\mapsto \left(\begin{array}{cccccc|c} 0 & 1 & 1 & 2 & 0 & 1 & b_1 \\ 0 & 0 & 0 & 2 & 0 & 1 & b_3 \\ 0 & 0 & 0 & 0 & 0 & 0 & b_1 + b_2 - 2b_3 \end{array}\right)$$

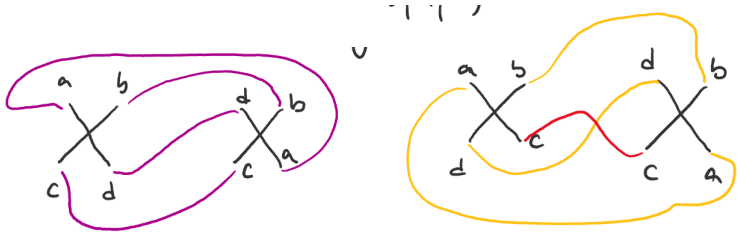
Durch weitere Umformungen kann man eine sZSTF herstellen, aber man sieht so bereits, dass der Rang der erweiterten Koeffizientenmatrix genau dann 2 ist wenn $b_1+b_2-2b_3 = 0$ gilt. Die homogene Lösungsmenge hat daher die Dimension $6 - 2 = 4$. Andernfalls ist $\text{Rang}(A|\overrightarrow{b}) = 3 > 2 = \text{Rang}\, A$ und es gibt keine Lösungen.

Kapitel 2

Virtuelle Verkettungen

2.1 Kurven und Schatten

Wir betrachten „Kreuzungen “, „Stränge“und Anleitungen wie diese in der Ebene verbunden werden sollen. Etikettierungen der Enden der Kreuzungen geben an, welche Enden miteinander durch eine Kurve verbunden werden sollen.



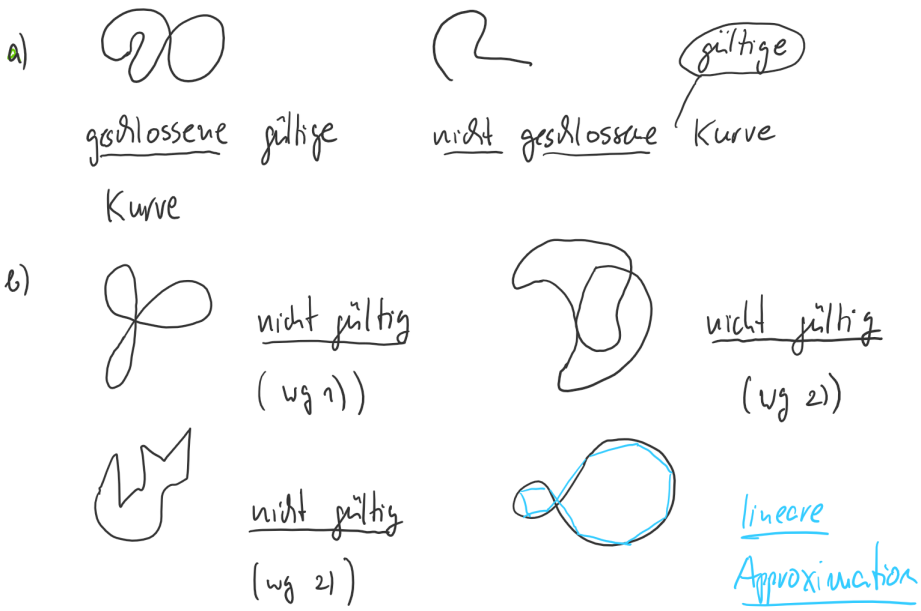
Im rechten Beispiel scheint es ohne einen weiteren Doppelpunkt nicht zu klappen. So ergeben sich zwei Typen von Doppelpunkten. In beiden Fällen haben wir Kurven in die Ebene gezeichnet. Wir wollen präzisieren, was wir unter einer gültigen Kurve verstehen wollen:

1. Schnittpunkte werden von höchstens zwei Abschnitten der Kurve erzeugt. Soche Schnittpunkte heißen Doppelpunkte.

2. Die Kurve ist „glatt“, das heißt es gibt keine „Ecken“, so dass es an jedem Punkt eine Tangente an die Kurve gibt. An jedem Doppelpunkt gibt es genau zwei verschiedene Tangenten.

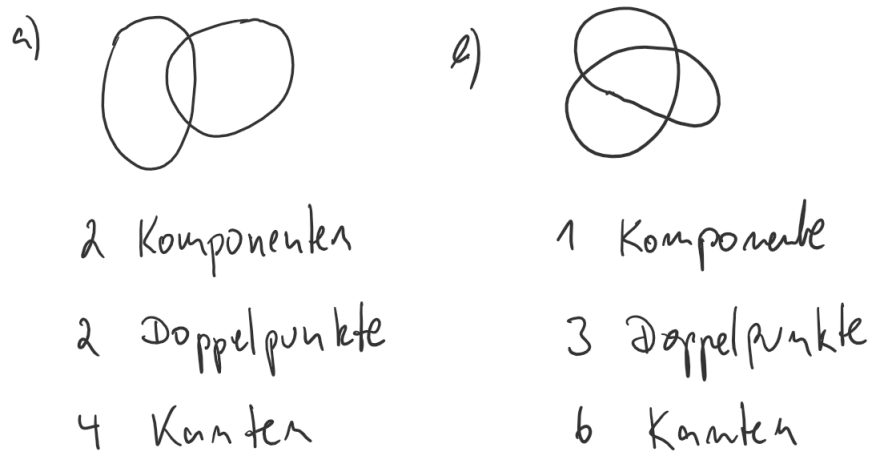
3. Die Kurve kann durch endlich vieleStrecken approximiert werden.

Beispiel 86.



Definition 87. Eine Menge von $n \in \mathbb{N}$ geschlossenen gültigen Kurven nennt man Schatten. Eine einzelne solche Kurve nennt man Komponente. Eine Kante ist ein Segment der Kurve zwischen zwei Doppelpunkten

Beispiel 88.

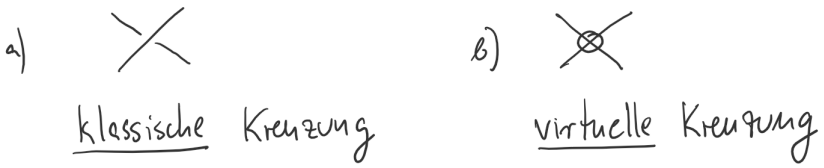


Bemerkung 89. Ein Schatten mit $n \in \mathbb{N}$ Doppelpunkten besitzt $2n$ Kanten.

2.2 Virtuelle Diagramme

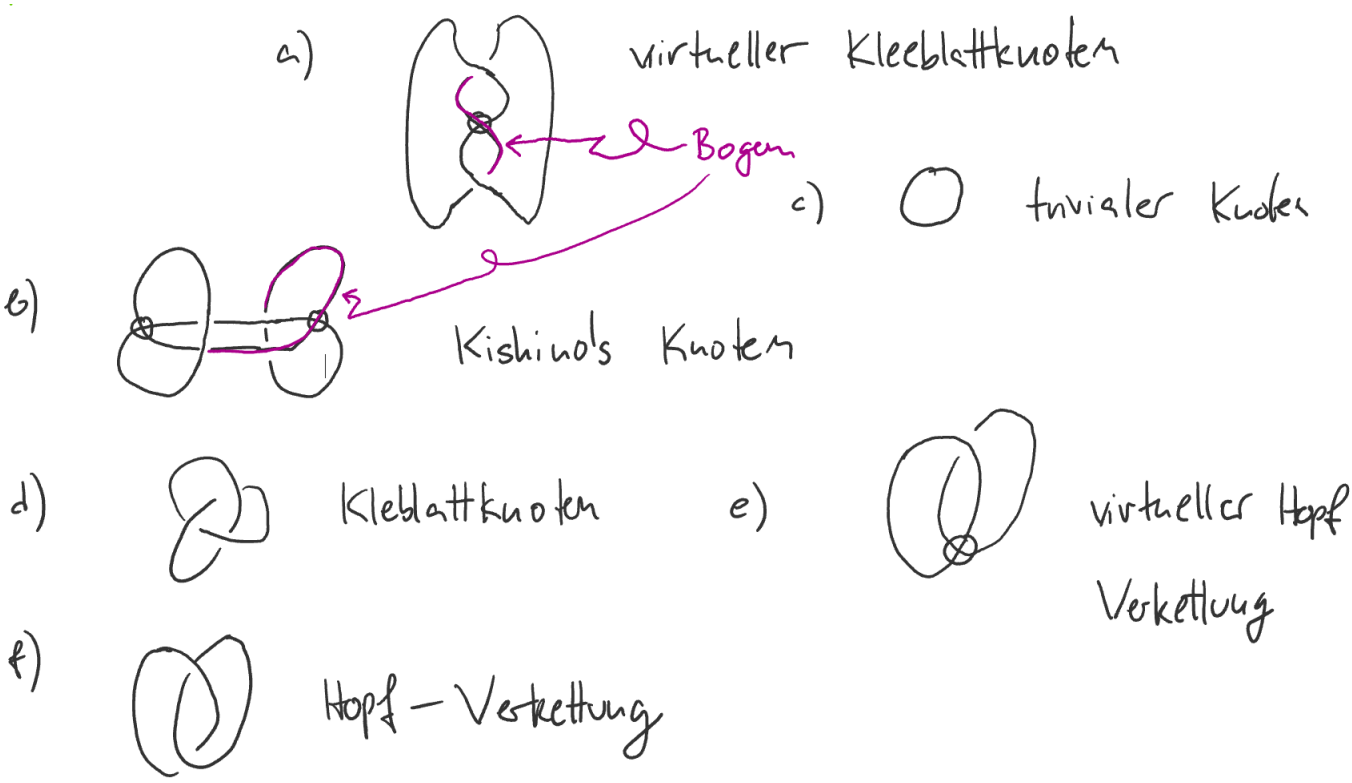
dfn:vD

Definition 90. Ein virtuelles diagramm ist ein Schatten zusammen mit Kreuzungsinformationen der Art



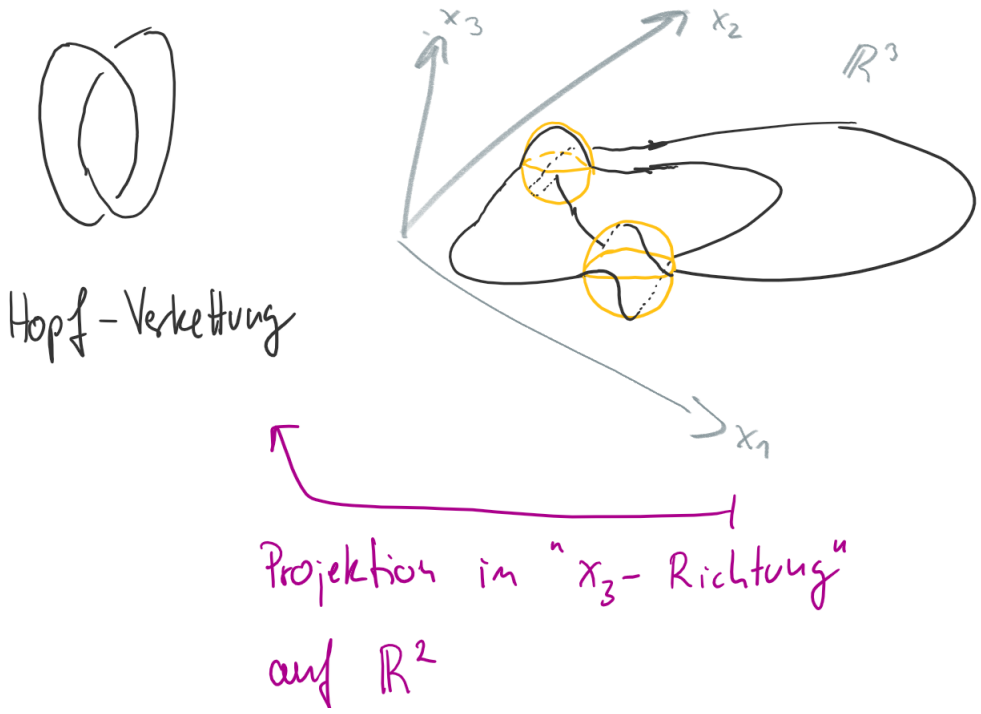
Ein virtuelles Knotendiagramm hat genau eine Komponente. Ein virtuelles Verkettungsdiagramm hat mehr als eine Komponente. Ein Bogen eines virtuellen Diagramms beginnt und endet an einer unterkreuzenden Information einer klassischen Kreuzung.

Beispiel 91.



2.3 Räumliche Verkettungen

Eine virtuelles Diagramm ohne virtuelle Kreuzungen (also nur mit klassischen Kreuzungen) läßt sich in $\mathbb{R}^3$ wie folgt interpretieren: man zeichnet das Diagramm in $\mathbb{R}^2$ und ersetzt die Kreuzungen durch dreidimensionale Kugeln. Außerhalb dieser Bälle verläuft das Diagramm in der Ebene. Man erzeugt Über- und Unterkreuzungen, indem man die Stränge über die jeweiligen Halbkugeln führt.



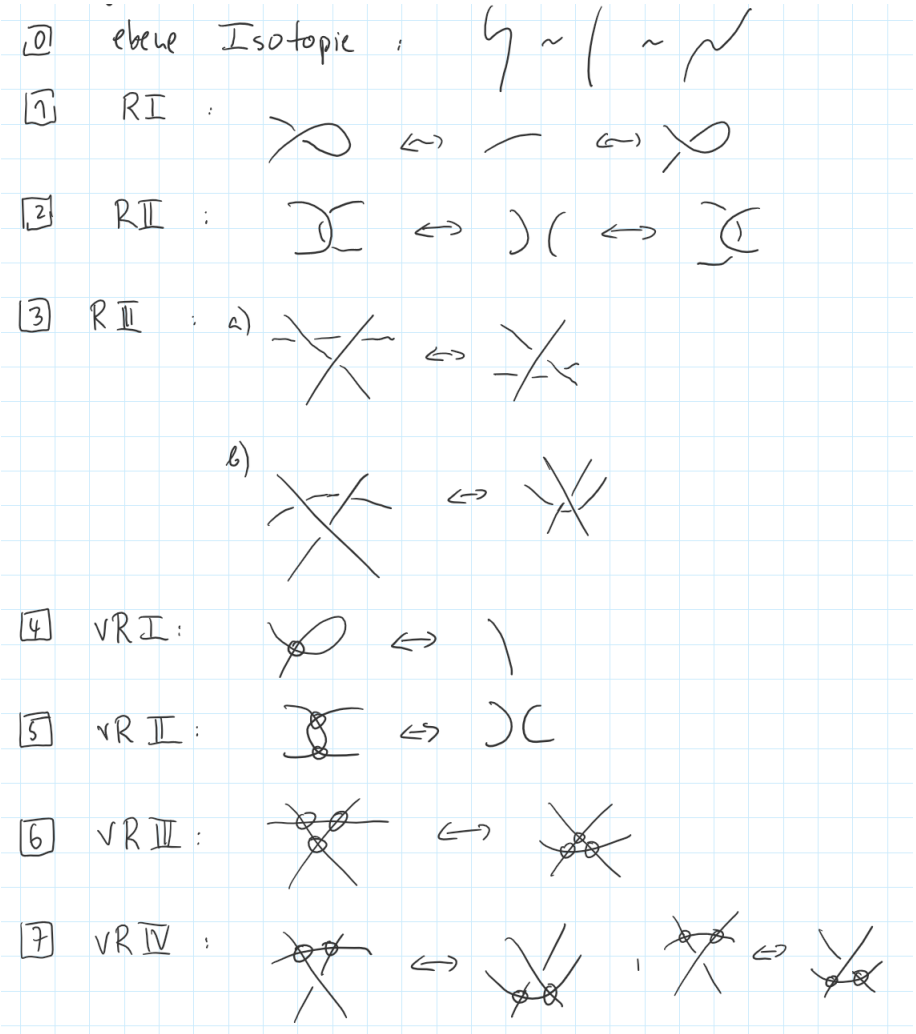
So ergibt sich eine Kurve in $\mathbb{R}^3$, die eine klassische Verkettung repräsentiert. Durch eine orthogonale Projektion in x_3-Richtung auf die Ebene erhält man den Schatten zurück. Dabei verliert man die Kreuzungsinformationen. Orthogonale Projektionen lassen sich mit Hilfe der linearen Algebra formalisieren. In den 20er Jahren des 20ten Jahrhunderts hat Kurt Reidemeister bewiesen, dass die Theorie der klassischen Diagramme (damals gab es noch keine virtuellen) äquivalent zur Theorie der klassischen Verkettungen im Raum ist. In den 90er Jahren erfand Louis Kauffman die virtuellen Diagramme und erst Anfang der 2000er wurde von Greg Kuperberg deren geometrische Bedeutung geklärt. Es handelt sich um Diagramme, die man statt in die Ebene zum Beispiel auf einem Torus zeichnet.

2.4 Reidemeister-Bewegungen

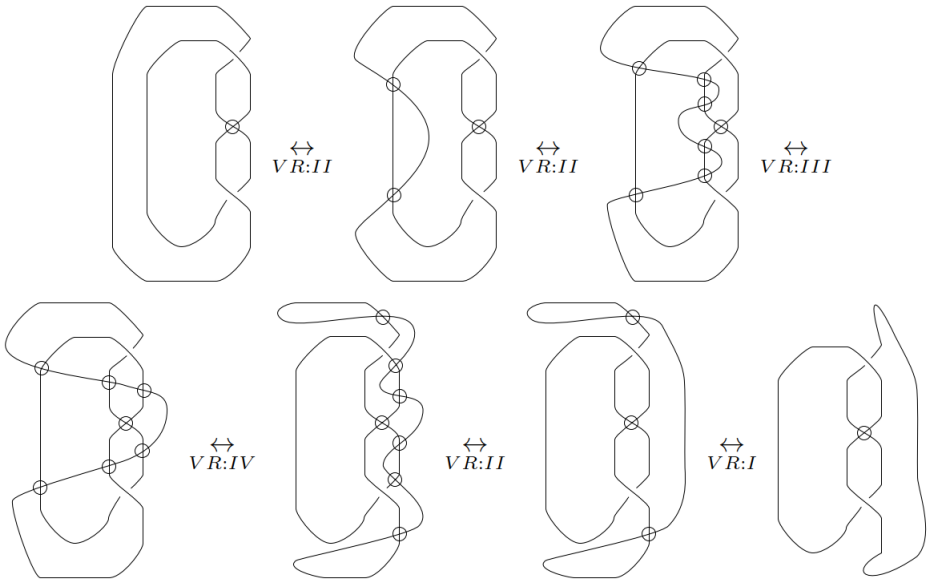
Wann sollen zwei virtuelle diagramme als gleich betrachtet werden? Dazu betrachten wir Diagrammbewegeungen. Bezüglich der Bögen sollen „Dehnungen“und „Verschiebungen“den Typ des Diagramms nicht verändern. Solche Diagramm bewegungen nennen wir ebene Isotopie.

`dfn:vkreide`

Definition 92. Zwei virtuelle Diagramme heißen äquivalent, wenn sie durch eine endlich Folge von ebenen Isotopien, Reidemeister-Bewegungen oder virtuellen Reidemeister-Bewegungen ineinander überführt werden können.



Beispiel 93. Zwei äquivalente Diagramme des virtuellen Kleeblattknotens.



thm:reideaequ

Satz 94. *Die Reidemeister-Bewegungen definieren eine Äquivalenzrelation auf der Menge $\mathcal{V}_d$ der virtuellen Diagramme.*

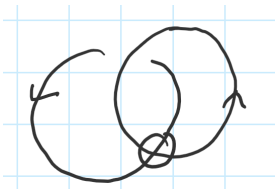
Beweis □

dfn:virtverkett

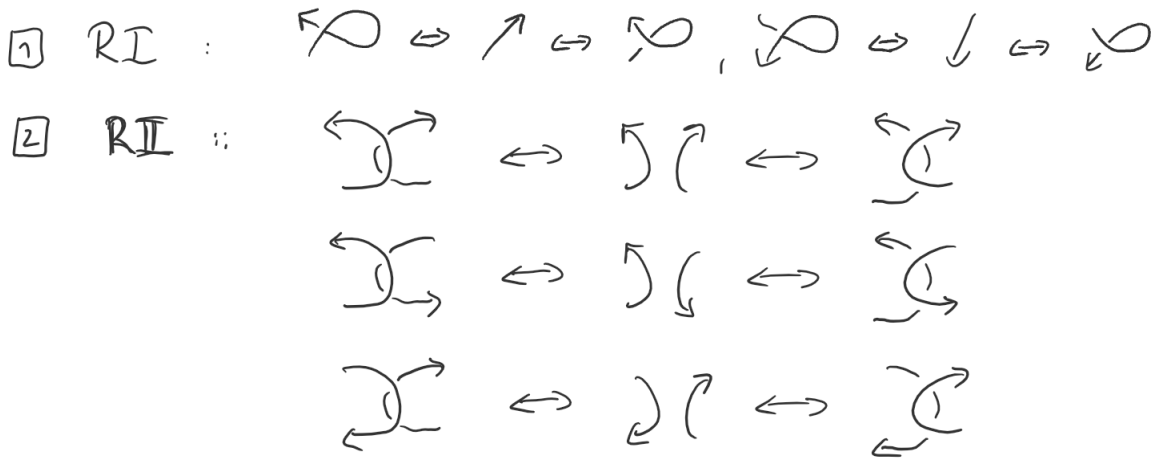
Definition 95. Ein:e virtuelle:r Verkettung bzw. Knoten ist eine Äquivalenzklasse eines virtuellen Diagramms. Die Menge der virtuellen Verkettungen ist $\mathcal{V} := \{[D] \mid D \text{ ist virtuelles Diagramm}\}$. Eine Verkettung $L \in \mathcal{V}$ heißt klassisch, falls es ein zu L äquivalentes Diagramm mit $L = [D]$ gibt.

2.5 Orientierte Diagramme

Ein virtuelles Diagramm heißt orientiert, falls jede Komponente mit einer Durchlaufrichtung versehen ist. Dies geschieht durch Anfügen eines Pfeils an eine Komponente zum Beispiel



Für die Äquivalenz orientierter virtueller Diagramme benötigen wir orientierte Reidemeister-Bewegungen. Diese ergeben sich aus den Diagrammbewegungen der Definition 92, indem man alle Möglichkeiten betrachtet die Stränge mit einem Pfeil zu versehen. Das ergibt zum Beispiel zwei orientierte Reidemeister-Bewegungen vom Typ I und II wie folgt



Die vierte Möglichkeit zu Reidemeister II ergibt sich durch Drehung der ersten um 180 Grad. Da eine RM III Bewegung drei Stränge hat, ergben sich 8 mögliche orientierte Bewegungen. Diese lassen sich mit Hilfe von orientierten RM II auf eine einzige zurückführen, nämlich

2.6 Selbstschnittzahl und Verschlingungszahl

2.6.1 Verkettungsinvarianten

Es sei S eine Menge. Eine Verkettungsinvariante I ist eine Abbildung $I : \mathcal{V} \to S$, die äquivalenten Verkettungen dasselbe Bild zuordnet. Sind $D_1, D_2 \in \mathcal{V}$ äquivalent, so gilt $I(D_1) = I(D_2)$. Man kann dabei die Äquivalenz orientierter oder nicht-orientierter Diagramme betrachten. Damit gilt

$$I(D_1) \neq I(D_2) \;\Rightarrow\; D_1 \neq D_2.$$

Mit Hilfe einer Invariante kann man also zeigen, dass Verkettungen nicht äquivalent sind.

cor:inv

Korollar 96. *Es seien $D, D' \in \mathcal{V}_d$ Diagramme, so dass D' aus D durch eine Diagrammbewegung hervorgeht. Eine Abbildung $I : \mathcal{V} \to S$ ist eine Verkettungsinvariante, falls $I([D]) = I([D'])$ gilt.*

Das Korollar besagt, dass man zum Nachweis einer Invariante die Auswirkungen auf die (virtuellen) Reidemeister-Bewegungen prüfen muss.

2.6.2 Selbstschnittzahl

In einem orientierten Verkettungsdiagramm ergeben sich zwei Typen von klassischen Kreuzungen. Es sei c eine klassische Kreuzung. Das Vorzeichen der Kreuzung definiert man durch $\epsilon(c) = +1$ bzw. $\epsilon(c) = -1$ gemäß der folgenden lokalen Situation an der Kreuzung c:

(a) $+1$ crossing

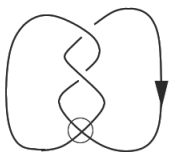
(b) -1 crossing

dfn:writhe

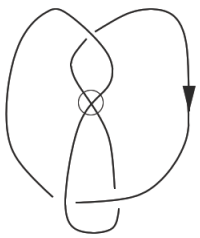
Definition 97. Die Selbstschnittzahl $w(D)$ eines virtuellen Diagramms $D \in \mathcal{V}_d$ ist die Summe über alle Vorzeichen der klassischen Kreuzungen, also

$$w(D) := \sum_{c \text{ klassische Kreuzung}} \epsilon(c).$$

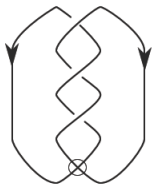
Beispiel 98.



(a) $w(K_1) = -2$



(b) $w(K_2) = -1$



(c) $w(K_3) = 3$

thm:writhe

Satz 99. *Die Selbstschnittzahl ist invariant unter allen Diagrammbewegungen außer der klassischen Reidemeister-Bewegung I.*

Beweis □

2.6.3 Verschlingungszahl

dfn:lk

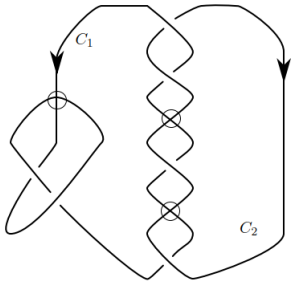
Definition 100. Es sei $D \in \mathcal{V}_d$ ein orientiertes Diagramm mit $n \in \mathbb{N}$ Komponenten $C_1, \ldots, C_n$. Es sei $C_j^i(D)$ die Menge der Kreuzungen, an denen die Komponente C_i die Komponente C_j überkreuzt. Die Verschlingungszahl von C_i über C_j ist definiert durch

$$\mathcal{L}_j^i(D) := \sum_{c \in C_j^i(D)} \epsilon(c).$$

Bemerkung 101.

1. Für $C_j^i(D) = \emptyset$ ergibt sich $\mathcal{L}_j^i(D) = 0$.
2. Die Zahl $\mathcal{L}_j^i(D)$ hängt von der Nummerierung der Komponeneten ab.

Beispiel 102. Für das folgende Diagramm D gilt $\mathcal{L}_1^2(D) = -3$ und $\mathcal{L}_2^1(D) = -1$.



thm:lk

Satz 103. *Die Verschlingungszahl $\mathcal{L}_j^i$ ist invariant unter Diagrammbewegungen nummerierter, orientierter virtueller Diagramme.*

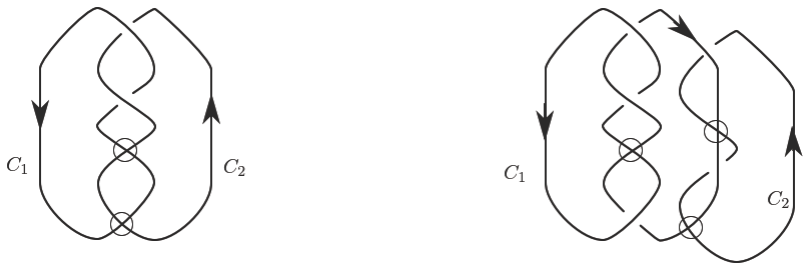
Beweis □

Aus Korollar 96 erhält man sofort folgende die Aussage.

Korollar 104. *Die Verschlingungszahl $\mathcal{L}_j^i$ ist eine Invariante nummerierter, orientierter virtueller Verkettungen.*

ex:vklinking

Beispiel 105. Wir berechnen die Verschlingungszahlen der folgenden Verkettungen. Für das Diagramm D auf der linken Seite ergibt sich $\mathcal{L}_2^1(D) = 1, \mathcal{L}_1^2(D) = -1$. Da sich in diesem Diagramm die virtuellen Kreuzungen mit einer virtuellen Reidemeister-Bewegung II elimineiren lassen, erkennt man, dass die orientierte Hopf-Verkettung nicht äquivalent zur trivialen Verkettung mit zwei Komponenten ist.



Für das Diagramm D' auf der rechten Seite sei C_3 die mittlere Komponente. Dann ergibt sich

$$\mathcal{L}_2^1(D') = 0,\ \mathcal{L}_1^2(D') = 0,\ \mathcal{L}_3^1(D') = 0,\ \mathcal{L}_1^3(D') = -1,\ \mathcal{L}_2^3(D') = -2,\ \mathcal{L}_3^2(D') = 0.$$

thm:vklinkzwei

Satz 106. *Für eine klassische Verkettung L mit zwei Komponenten gilt $\mathcal{L}_1^2(L) = \mathcal{L}_2^1(L)$.*

Beweis □

Korollar 107. *Für eine klassische Verkettung L mit $n \in \mathbb{N}$ Komponenten gilt $\mathcal{L}_i^j(L) = \mathcal{L}_j^i(L)$ für alle $1 \leq i, j \leq n$.*

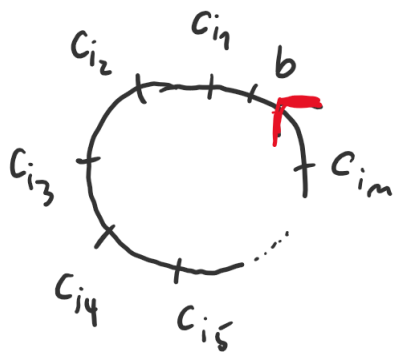
Beweis Folgt sofort aus Satz 106. □

Bemerkung 108. Es sei $L \in \mathcal{V}$ mit $\mathcal{L}_i^j(L) \neq \mathcal{L}_j^i(L)$, dann ist L nicht klassisch. Es gibt also kein Diagramm $D \in \mathcal{V}_d$ ohne virtuelle Kreuzungen mit $L = [D]$. Das trifft auf Beipiel 105 zu.

2.6.4 Die ungerade Selbstschnittzahl

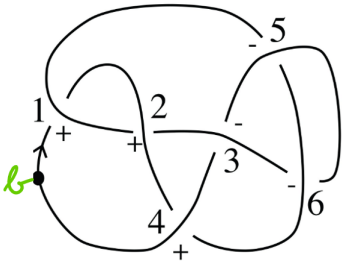
Wir haben gesehen, dass die Selbstschnittzahl eines Diagramms keine Invariante liefert. Indem wir die Menge der Kreuzungen, deren Vorzeichen wir summieren, einschränken, erhalten wir eine Invariante von virtuellen Knoten.

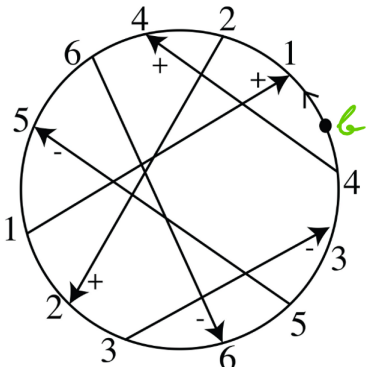
Es sei $D \in \mathcal{V}_d$ ein orientiertes Knotendiagramm. Dabei seien $c_1, \ldots, c_n$ die klassischen Kreuzungen von D. Wir wählen einen Punkte b auf dem Diagramm, der kein Doppelpunkt des Schattens sein darf. Nun durchlaufen wir D gemäß der Orientierung beginnend beim Startpunkt b. Daraus ergibt sich eine geordnete Liste von Kreuzungen, in der jede Kreuzung zweimal auftaucht, sobald wir wieder bei b angelangt sind. Wir tragen b, die Orientierung und die Liste auf einem Kreis ab:



Es sei $c_{i_j} = c_{i_k}$ für $j < k$, also taucht c_{i_j} vor c_{i_k} auf dem Kreis auf. Wir verbinden c_{i_j} mit c_{i_k} durch einen Pfeil, der von c_{i_j} nach c_{i_k} gerichtet ist, genau dann, wenn man bei c_{i_j} den überkreuzenden und bei c_{i_k} den unterkreuzenden Strang durchläuft. Schließlich fügen wir an jeden Pfeil das Vorzeichen der Kreuzung an. Ein solches Diagramm nennt man Gauss-Diagramm zu D.

Ein Beispiel für eine klassische Verkettung:





rem:vkgausseven

Bemerkung 109. Es sei c eine Kreuzung in einem Gauss-Digramm. Diese taucht zweimal auf. Sei A_c und B_c die Anzahl der Markierungen (aus Kreuzungen), auf den beiden Kreissegmenten, die durch c geliefert werden. Dann sind A_c und B_c entweder beide gerade oder beide ungerade, denn: falls nicht, ist die Anzahl $A_c + B_c + 2$ aller Markierungen ungerade. Da aber jede Kreuzung zweimal durchlaufen wird, also zweimal auf dem Kreis auftaucht, muss die Anzahl aller Markierungen gerade sein.

Wegen Bemerkung 109 ist die folgende Definition möglich.

Definition 110. Es sei $D \in \mathcal{V}_d$ ein orientiertes Knotendiagramm. Eine Kreuzung c von D heißt gerade bzw. ungerade, falls A_c (und B_c) aus Bemerkung 109 gerade bzw. ungerade sind. Es sei $odd(D)$ die Menge aller ungeraden Kreuzungen von D. Wir definieren die ungerade Selbstschnittzahl (engl. odd writhe) durch

$$w_{odd}(D) := \sum_{c \in odd_D} \epsilon(c).$$

lem:vkgerade

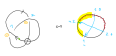
Lemma 111. *Es sei $L \in \mathcal{V}$ ein klassischer orientierter Knoten. Dann ist in einem Diagramm von L jede Kreuzung gerade.*

thm:oddinv

Satz 112. *Die ungerade Selbstschnittzahl ist eine Invariante orientierter virtueller Knoten.*

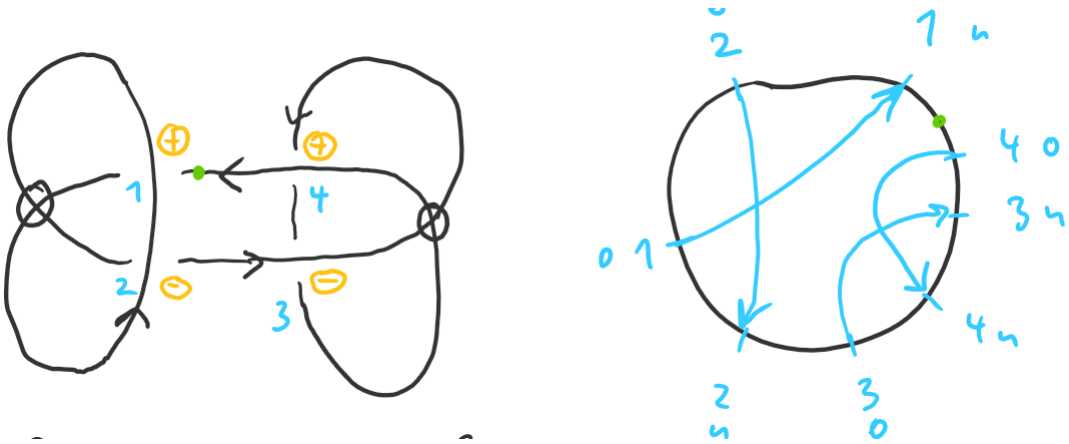
Korollar 113. *Ist $w_{odd}(D) \neq 0$, so folgt aus Lemma 111, dass D kein klassischen Knoten repräsentiert.*

Beispiel 114. 1. Der rechtshändrige virtuelle Kleeblattknoten.



Es ist $odd(D) = \{1, 2\}$, also gilt $w_{odd}(D) = -2$. Damit ist D nicht-trivial und nicht-klassisch. Außerdem auch verschieden vom linkshändrigen virtuellen Kleeblattknoten (Vertauschen der Vorzeichen der Kreuzungen).

2. Kinoshitos Knoten.



Hier ist $odd(D) = \{1, 2, 3, 4\}$ also $w_{odd}(D) = 0$. Auf diese Art können wir D daher nicht vom trivialen Knoten unterscheiden.

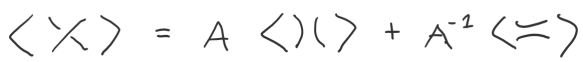
2.7 Das Klammerpolynom

Im Jahr 1984 veröffentlicht V.Jones eine Arbeit über eine polynomielle Invariante klassischer Verkettungen. Dieses Polynom wird später nach ihm bennant und heißt Jones-Polynom. Dafür erhielt er 1985 die Fields-Medaille. Gegen 1987 fand L.Kauffman einen kombinatorischen Weg das Jones-Polynom zu erhalten. Im Gegensatz zu der Arbeit von Jones ist dieser Zugang frappierend elementar. Dieses Polynom heißt Klammerpolynom von Kauffman. Es ist ein Polynom in den Variablen A und A^{-1}, zum Beispiel $2A^{-2} + 3 + A^5$.

dfn:skein

Definition 115. Es sei $D \in \mathcal{V}_d$ ein virtuelles Verkettungsdiagramm. Das Klammerpolynom $< D >$ wird sukzessive mit den folgenden Regeln berechnet.

1. skein relation



2. Vereinigung mit trivialem Knoten

$$< \mathrm{O} \cup L >= -(A^2 + A^{-2}) < L >$$

3. Normierung

$$< \mathrm{O} >= 1$$

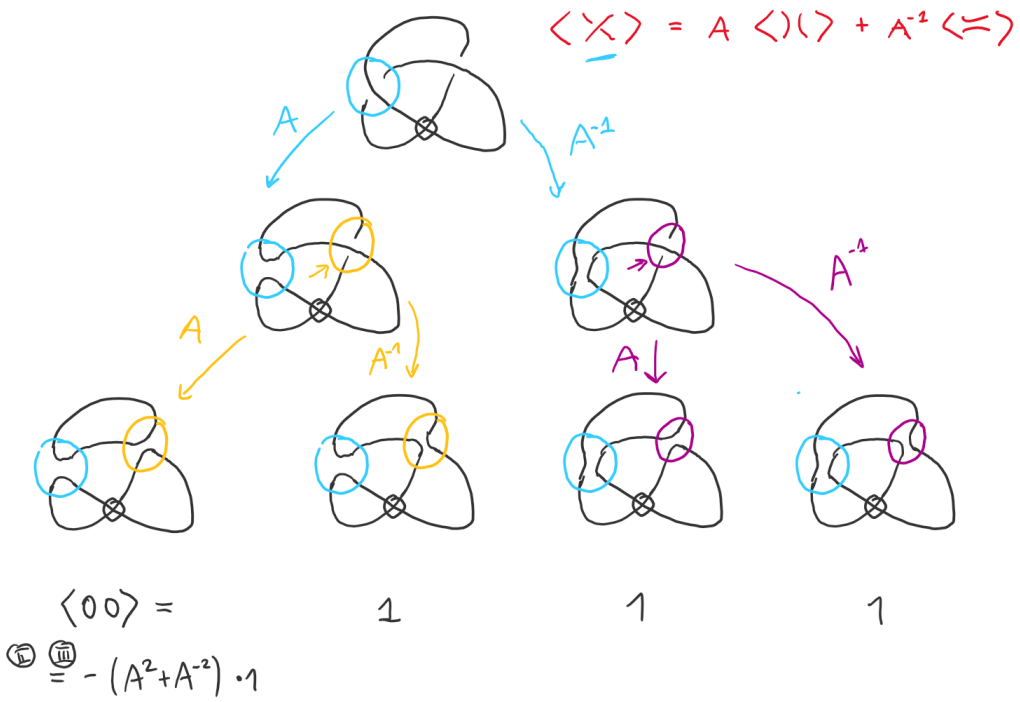
Bemerkung 116. rem:bracket

1. Regel I liefert zwei neue Diagramme mit jeweils einer klassischen Kreuzung weniger. Ist $n \in \mathbb{N}$ die Anzahl der klassischen Kreuzungen, so ergebn sich durch wiederholtes Anwenden der Regel I insgesamt 2^n Diagramme ohne klassische Kreuzungen (virtuelle kann es geben).

2. Die Auswahl der Kreuzungen bei Regel I ist beliebig. Das Klammerpolynom hängt davon nicht ab, allerdings ist das zu diesem Zeitpunkt noch völlig unklar! Wir behandeln das später.

ex:baumtrefoil

Beispiel 117. Der virtuelle rechtshändige Kleeblattknoten

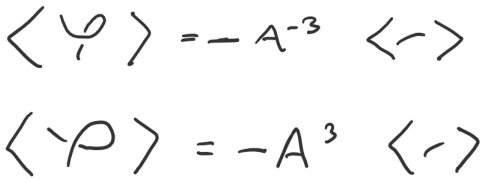


Das Klammerpolynom berechnet sich nun, indem man die Gewichte entlang der Pfade multipliziert und diese aufsummiert:

$$< D > = A \cdot A \cdot (-A^2 - A^{-2}) + A \cdot A^{-1} \cdot 1 + A^{-1} \cdot A \cdot 1 + A^{-1} \cdot A^{-1} \cdot 1 \quad (2.1)$$

$$= -A^{-4} + 1 + A^{-2} \quad (2.2)$$

Satz 118. *Das Klammerpolynom ist invariant unter allen Reidemeister-Bewegungen außer der klassischen Reidemeister-Bewegung I. Hier gelten:*



Beweis □

Wir wollen aus der Klammer eine Invariante machen, dazu müssen wir uns um Reidemeister-Bewegung I kümmern.

Definition 119. Es sei $D \in \mathcal{V}_d$ eine orientierte virtuelle Verkettung. Dann heißt

$$f_D(A) := \left(-A^{-3}\right)^{w(D)} < D >$$

das f-Polynom oder normierte Klammerpolynom von D.

Satz 120. *f_D ist eine Invariante orientierter virtueller Verkettungen.*

Beweis □

Bemerkung 121.

1. Zu einem orientierten Knotendiagramm D sei $-D$ das Diagramm mit entgegengesetzter Orientierung. Dann gilt $f_D(A) = f_{-D}(A)$, denn: für Knoten ändert sich die Selbstschnittzahl nicht, wenn man die Orientierung umkehrt. Daher ist das f-Polynom eine Invariante für *unorientierte* Knoten.

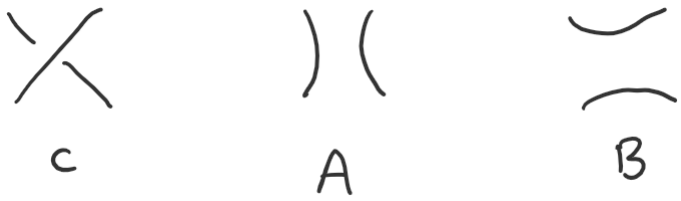
2. Zu einem orientierten Verkettungsdiagramm D, sei $\overline{D}$ das Diagramm, das durch Ändern (plus zu minus, minus zu plus) aller Vorzeichen der Kreuzungen hervorgeht. Dann gilt $f_D(A) = f_{\overline{D}}(A^{-1})$. (Übung)

2.8 Das Zustandsmodell (engl. state sum)

Wir kommen zurück auf Bemerkung 116 und wollen nun die Wohldefiniertheit der Klammer besprechen.

dfn:state

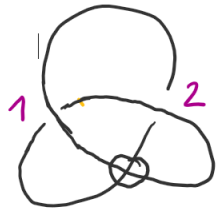
Definition 122. Es sei $D \in \mathcal{V}_d$ ein virtuelles Diagramm und c eine klassische Kreuzung von D. Wir definieren die A-Aufspaltung und die B-Aufspaltung von c wie folgt:

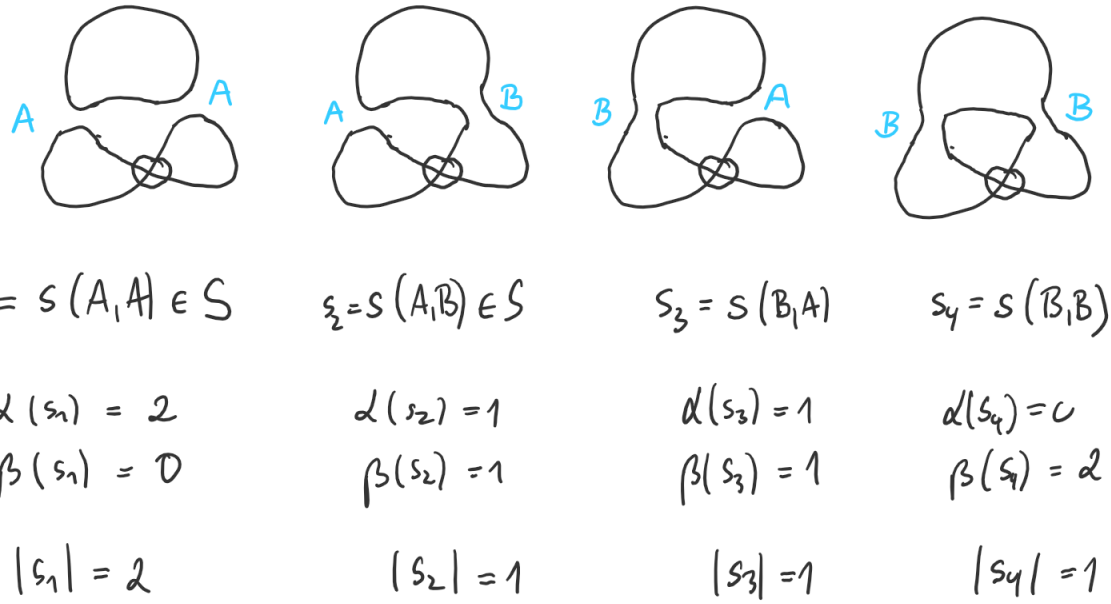


Ein Zustand Von D ist eine Wahl von Aufspaltungen an jeder Kreuzung von D. Sind $c_1, \ldots, c_n$ die klassischen Kreuzungen von D, so bezeichnet $s(x_1, \ldots, x_n)$ mit $x_i \in \{A, B\}$ einen Zustand mit Aufspaltung x_i an Kreuzung c_i. Es sei S die Menge der Zustände von D. Für $s \in S$ sei $\alpha(s)$ die Anzahl derA-Aufspaltungen und $\beta(s)$ die Anzahl der B-Aufspaltungen. Der Zustand s ist ein Diagramm ohne klassische Kreuzungen, die Anzahl der Komponenten von s bezeichnen t man mit $|s|$.

ex:statetref

Beispiel 123. Die Zustände des virtuellen Kleeblattknotens aus Beispiel 117 sehen so aus:





Man erkennt an diesem Beispiel, dass ein Diagramm mit n klassischen Kreuzungen genau 2^n Zustände besitzt.

dfn:statesum

Definition 124. Es sei $D \in \mathcal{V}_d$. Die Zustandssumme (engl. state sum) von D ist definiert als

$$< D > = \sum_{s \in S} A^{\alpha(s)-\beta(s)} d^{|s|-1}$$

mit $d := -A^2 - A^{-2}$.

Die Zustandssumme erhält dasselbe Symbol wie die Kauffmann-Klammer. Das liegt an dem folgenden

thm:stateisbracket

Satz 125. *Die Zustandssumme erfüllt die Bedingungen aus Definition 115.*

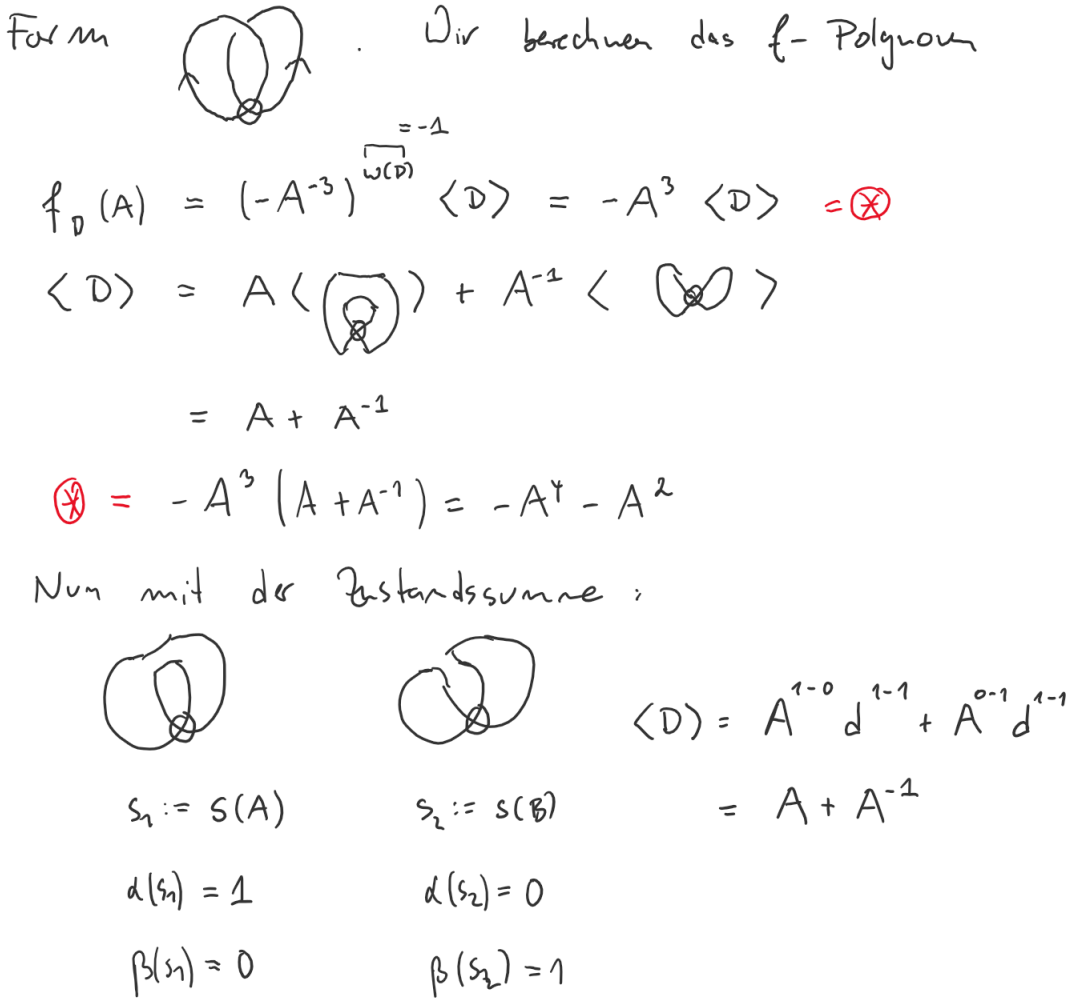
Beweis An einem BEispiel klargemacht. □

Korollar 126. *Nach Satz 125 läßt sich $< D >$ aus Definition 124 mit der Definition 115 berechnen. Dabei ist die Reihenfolge der Auswahl der Kreuzungen in Regel 1 unerheblich, denn sie spielt in Definition 124 keine Rolle (denn egal wie man nummeriert: es wird über alle Zustände summiert).*

Beispiel 127. Die Zustandssumme aus Beispiel 123 sieht so aus:

$$\begin{aligned} < D > &= \sum_{i=1}^{4} A^{\alpha(s_i)-\beta(s_i)} d^{|s_i|-1} \\ &= A^2 d + 1 + 1 + A^{-2} = -A^4 + 1 + A^{-2} \end{aligned}$$

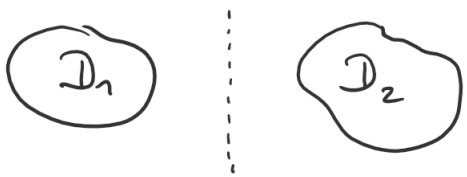
Als weiteres Beispiel berechnen wir das f-Polynom einer orientierten virtuellen Hopf-Verkettung auf zwei Arten.



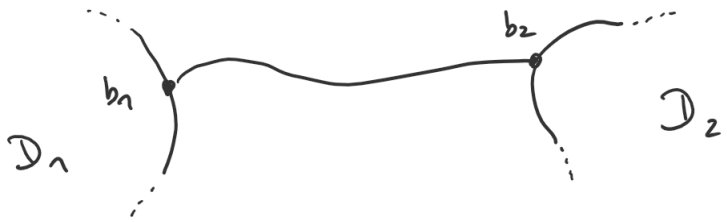
2.9 Zusammenhängende Summe

dfn:consum

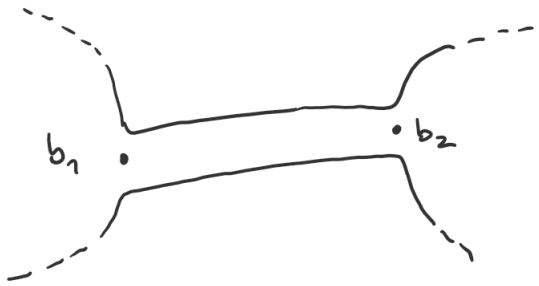
Definition 128. Es seien $D_1, D_2 \in \mathcal{V}_d$ virtuelle Knotendiagramme, die durch eine Gerade getrennt voneinander liegen:



Es seien b_1 und b_2 Punkte auf den Schatten von D_1 bzw. D_2, die keine Doppelpunkte sind und die sich durch eine Kurve verbinden lassen, die keine der beiden Schatten schneidet.



Die zusammenhängende Summe von D_1 mit D_2 wird mit $D_1 \# D_2$ bezeichnet und wird wie folgt gebildet:



Bemerkung 129. Für klassische Knoten hängt der Knotentyp der zusammenhängenden Summe nicht von der Auswahl der Punkte auf den Schatten ab (ohne Beweis). Für Knoten mit virtuellen Kreuzungen gilt das im allgemeinen nicht.

Für das f-Polynom erhalten wir folgenden zentralen

thm:fpolconsum

Satz 130. *Für virtuelle Knotendiagramme $D_1, D_2 \in \mathcal{V}_d$ gilt $f_{D_1 \# D_2}(A) = f_{D_1}(A) \cdot f_{D_2}(A)$.*

Beweis □

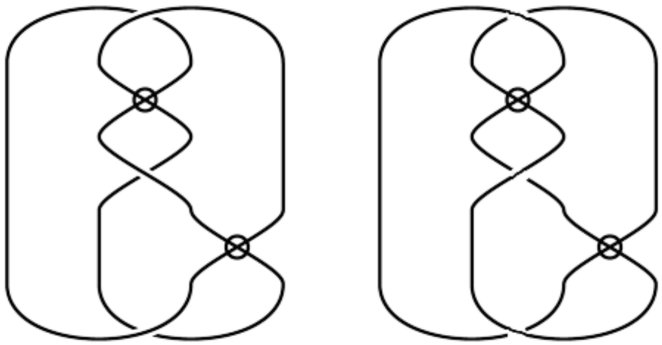
Beispiel 131. Kishinos Knoten ist die zusammenhängende Summe zweier trivialer Knoten. Daher gilt $f_{Kishino}(A) = 1 \cdot 1 = 1$.

2.10 Spiegelbilder

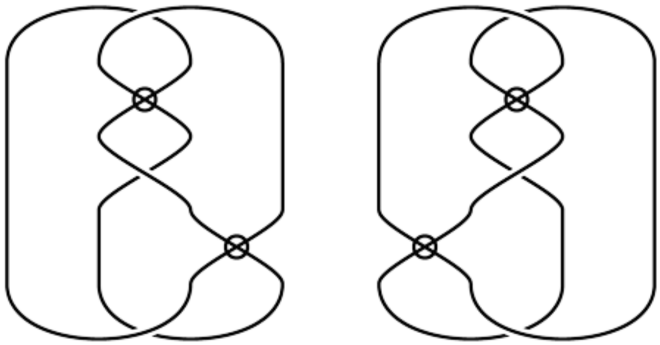
dfn:vkspiegel

Definition 132. Das vertikale Spiegelbild D^v eines Diagramms $D \in \mathcal{V}_d$ entsteht durch Abändern aller Vorzeichen der klassischen Kreuzungen. Das horizontale Spiegelbild D^h entsteht durch Spiegelung des Diagramms an einer Geraden, die den Schatten des Diagramms nicht schneidet.

Beispiel 133. Der virtuelle Knoten 3.4 links und rechts sein vertikales Spiegelbild:



Der virtuelle Knoten 3.4 links und rechts sein horizontales Spiegelbild:



Hier gelten $D \neq D^v$, $D \neq D^h$ und $D^v = D^h$ (ohne Beweis).

Bemerkung 134. Für klassische Verkettungen gilt stets $D^v = D^h$. Der klassische Kleeblattknoten ist nicht äquivalent zu seinem Spiegelbild (Übung). Der Achterknoten indes ist äquivalent zu seinem Spiegelbild:

thm:fpolspiegel

Satz 135. *Für $D \in \mathcal{V}_d$ gelten:*

1. $f_D(A) = f_{D^v}(A^{-1})$
2. $f_D(A) = f_{D^h}(A^{-1})$

Beweis Ausgelassen □

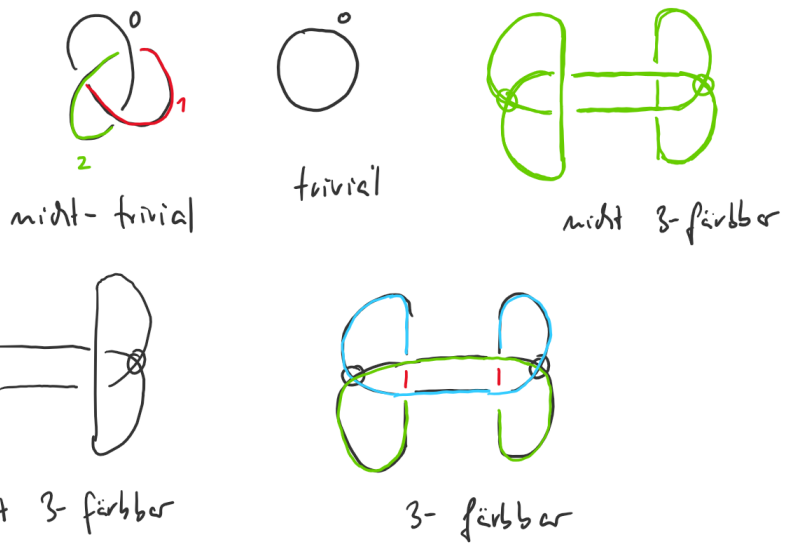
Bemerkung 136. Nach Satz 135 kann das f-Ploynom Spiegelbeilder nicht voneinander unterscheiden, denn es gilt $f_{D^v}(A) = f_D(A^{-1}) = f_{D^h}(A)$.

2.11 Färbungen

2.11.1 3-Färbungen

Definition 137. Eine Färbung eines Diagramms $D \in \mathcal{V}_d$ mit Farben aus einer Menge $\mathcal{F}$ ist eine Etikettierung jedes Bogens des Diagramms mit einer Farbe aus $\mathcal{F}$. Ein Diagramm heißt 3-gefärbt, wenn es eine Färbung mit Farben aus $\mathcal{F} = \{0, 1, 2\}$ gibt, bei der an jeder klassischen Kreuzung genau eine oder alle drei Farben auftreten. Eine Färbung mit nur einer Farbe für jeden Bogen nennt man trivial. Ein Diagramm $D \in \mathcal{V}_d$ heißt 3-färbbar, wenn es eine nicht-triviale Färbung von D gibt.

Beispiel 138. 3-Färbungen lassen sich gut mit Farben darstellen.



Satz 139. *3-Färbbarkeit ist eine Inavariante virtueller Verkettungen.*

Beweis □

Korollar 140. *Der klassische Kleeblattknoten ist nicht äquivalent zum trivialen Knoten.*

Beispiel 141. Der Achterknoten läßt sich nicht nicht-trivial 3-färben. Also ist er nicht äquivalent zum Kleeblattknoten.

2.11.2 Färbungen modulo n

Wir betrachten $\mathbb{Z}_n := \{0, 1, 2, \ldots, n-1\}$ zusammen mit der modularen Arithmetik. In $\mathbb{Z}_4$ gilt zum Beispiel $6 \equiv 2 \mod 4$ oder $-1 \equiv 3 \mod 4$.

Definition 142. Ein Diagramm $D \in \mathbb{V}_d$ heißt färbbar modulo n, falls es eine nicht-triviale Färbung der Bögen von D mit Farben aus $\mathbb{Z}_n$ gibt, so dass an jeder klassischen Kreuzung

die Bedingung $2z \equiv x + y \mod n$ gilt.

Beispiel 143. Eine Färbung modulo 3 des Kleeblattknotens kann so aussehen:

Korollar 144. *Ist D färbbar modulo n, dann tauchen an jeder klassischen Kreuzung drei verschiedene oder drei gleiche Farben auf.*

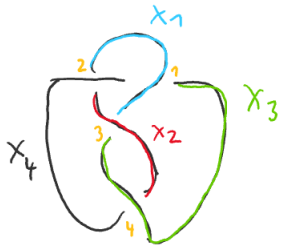
Beweis □

Satz 145. *Färbbarkeit modulo n ist eine Invariante virtueller Verkettungen.*

Beweis □

Bemerkung 146. Um eine Färbung modulo n zu erhalten, muss man ein LGS in $\mathbb{Z}_n$ lösen. Dabei ist die Anzahl der Gleichungen gleich der Anzahl der Kreuzungen von D und die Anzahl der Variablen gleich der Anzahl der Bögen. Die Anzahl der Bögen ist gleich der Anzahl der Kreuzungen (Übung), daher ist das LGS quadratisch.

Beispiel 147. Wir versuchen Färbungen des Achterknotens zu finden. Dazu stellen wir zunächst das LGS auf.



1 $2x_1 \equiv x_4 + x_3 \ (n)$
2 $2x_4 \equiv x_1 + x_2 \ (n)$
3 $2x_2 \equiv x_1 + x_3 \ (n)$
4 $2x_3 \equiv x_2 + x_4 \ (n)$

liefert Koeff matrix

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

Zunächst suchen wir Lösungen modulo 3.

Betrachte Modulo 3 : $\begin{pmatrix} 0 & 2 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 2 \\ 0 & 1 & 1 & 1 \end{pmatrix}$

$\Rightarrow x_3 \equiv -2x_4 \equiv x_4 \Rightarrow x_2 \equiv -2x_3 \equiv x_3 \overset{\text{mod } 3}{\Rightarrow} x_1 \equiv x_2$

$\Rightarrow x_1 \equiv x_2 \equiv x_3 \equiv x_4$ (nicht-triviale)

$\Rightarrow$ Es gibt keine 3-Färbung

Dann Lösungen modulo 4.

Betrachte Modulo 4

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

$$= \begin{pmatrix} 0 & 0 & 1 & 3 \\ 1 & 0 & 2 & 1 \\ 0 & 0 & 3 & 1 \\ 0 & 1 & 2 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & -5 \\ 0 & 0 & 1 & 3 \\ 0 & 1 & 0 & -5 \end{pmatrix}$$

$\Rightarrow$ $x_1 \equiv 5x_4 \equiv x_4$, $x_2 \equiv 5x_4 \equiv x_4$, $x_3 \equiv -3x_4 \equiv x_4$

$\Rightarrow$ $x_1 \equiv x_2 \equiv x_3 \equiv x_4$ $\Rightarrow$ nur triviale 4-Färbung möglich

Und Lösungen modulo 5.

Betrachte Modulo 5

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

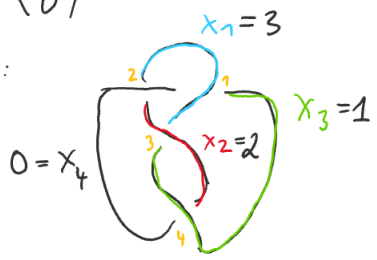
$\Rightarrow$ $x_3 =: \lambda$, $x_4 =: \mu$ $\Rightarrow$ $x_1 = 3\lambda + 3\mu$, $x_2 = 2\lambda + 4\mu$

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 3\lambda + 3\mu \\ 2\lambda + 4\mu \\ \lambda \\ \mu \end{pmatrix} = \lambda \begin{pmatrix} 3 \\ 2 \\ 1 \\ 0 \end{pmatrix} + \mu \begin{pmatrix} 3 \\ 4 \\ 0 \\ 1 \end{pmatrix}, \lambda, \mu \in \mathbb{Z}_5$$

Zum Beispiel $\lambda = 1$ liefert:

oder $\lambda = 2$ liefert

$x_1 = 1$, $x_2 = 4$, $x_3 = 2$, $x_4 = 0$



eine andere Färbung Modulo 5!

Kapitel 3

Zahlentheorie und ihre Anwendungen

3.1 Division mit Rest

In den ganzen Zahlen $\mathbb{Z}$ rechnen wir im üblichen Sinn $\cdot$ und $+$. Es gibt eine Division mit Rest, das bedeutet: zu $m, n \in \mathbb{Z}$ gibt es $q, r \in \mathbb{Z}$ mit $0 \leq r \leq n$, so dass $m = qn + r$ gilt. Für $n = 10$ und $n = 10$ zum Beispiel $43 = 4 \cdot 10 + 3$. Im Fall $r = 0$ sagen wir n teilt m und schreiben $n|m$.

Definition 148. Zu $n, m \in \mathbb{Z}$ heißt $\mathrm{ggT}(m, n) := \max\{x \in \mathbb{Z} \mid x|m \text{ und } x|n\}$ der größte gemeinsame Teiler von m und n.

lem:ggt

Lemma 149. *Es sei $m = qn + r$ mit $q \neq 0$. Dann gilt $\mathrm{ggT}(m, n) = \mathrm{ggT}(n, r)$.*

Beweis □

Satz 150 (Bezout)**.** *Zu $m, n \in \mathbb{Z}$ gibt es $a, b \in \mathbb{Z}$, so dass $\mathrm{ggT}(m, n) = am + bn$ gilt.*

Beweis □

Bemerkung 151. Euklidischer Algorithmus. Wir berechnen $\mathrm{ggT}(101, 35)$.

$$\begin{aligned} 101 &= 2 \cdot 35 + 31 \\ 35 &= 1 \cdot 31 + 4 \\ 31 &= 7 \cdot 4 + 3 \\ 4 &= 1 \cdot 3 + 1 \\ 3 &= 1 \cdot 3 + 0 \end{aligned}$$

Nach Lemma 149 ist $\mathrm{ggT}(101, 35) = \mathrm{ggT}(3, 1) = 1$. Rückwarts einsetzen ergibt

$$1 = 4 - 1 \cdot 3 = 4 - (31 - 7 \cdot 4) = 8 \cdot 4 - 31 = 8(35 - 1 \cdot 31) - 31 = 8 \cdot 35 - 9 \cdot 31 = (-9) \cdot 101 + 26 \cdot 35.$$

cor:ggt

Korollar 152. *Sind $a, b \in \mathbb{Z}$ teilerfremde Zahlen, dann existiert ein $a' \in \{0, \ldots, b-1\}$, so dass $aa' \equiv 1 \mod b$ gilt.*

Beweis □

3.2 Primzahlen

Sei $n \in \mathbb{N}$, $n \geq 2$. Die Menge der Restklassen auf $\mathbb{Z}$, die bei Division durch n entstehen, nennen wir $\mathbb{Z}_n := \{[0]_n, \ldots, [n-1]_n\}$. Eine Restklasse enthält die Menge der Zahlen $[a]_n = \{k \cdot n + a \,|\, k \in \mathbb{Z}\}$. Dabei heißt a der Repräsentant von $[a]_n$. Eine Addition und eine Multiplikation kann man auf $\mathbb{Z}_n$ wie folgt einführen

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

Man muss dann allerdings noch zeigen, dass diese Verknüpfungen nicht von der Wahl der Repräsentanten abhängen (das machen wir hier nicht). Es gilt

$$[a]_n = [b]_n \Leftrightarrow [a-b]_n = [0]_n \Leftrightarrow \{kn + (a-b) \,|\, k \in \mathbb{Z}\} = \{kn \,|\, k \in \mathbb{Z}\} \Leftrightarrow \exists l \in \mathbb{Z} : b - a = ln.$$

Das ergibt

$$[a]_n = [b]_n \quad \Leftrightarrow \quad a \equiv b \mod n.$$

Beispiel 153. Wir betrachten die Verknüpfungstafel für $\mathbb{Z}_4 = \{0,1,2,3\}$. Dabei schreiben wir zur Abkürzung a für $[a]_4$.

$+$	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

Man erkennt, dass die 2 kein multiplikatives Inverses Element besitzt.

Der größte gemeinsame Teiler charakterisiert die multiplikativen Inversen in $\mathbb{Z}_n$. Diese Aussgae steht in dem

Satz 154. *Es sei $[a]_n \in \mathbb{Z}_n$. Es gilt folgende Äquivalenz:*

$$\exists\, a' \in \mathbb{Z} \;:\; [a]_n \cdot [a']_n = [1]_n \quad \Leftrightarrow \quad \mathrm{ggT}(a,n) = 1.$$

Beweis □

Es sei $(K, +, \cdot)$ eine Menge mit einer Addition und einer Multiplikation. Das neutrale Element der Addition sei 0 , das neutrale Element Multiplikation sei 1. Man nennt K einen Körper, falls $(K,+)$ und $(K\backslash\{0\}, \cdot)$ abelsche Gruppen sind und die Distributivgesetze gelten. Das bedeutet insbesondere, dass in K jedes Element außer der 0 ein multiplikatives Inverses besitzt.

Als Faustregel kann man sich merken, dass man in Körpern rechnen kann wie in $\mathbb{R}$ oder $\mathbb{Q}$.

thm:Zp

Satz 155. *Ist $p \in \mathbb{Z}$ eine Primzahl, dann ist $\mathbb{Z}_p$ ein Körper.*

Wir wollenzeigen, dass es unendlich viele Primzahlen gibt. Dazu brauche wir den folgenden Hauptsatz der Zahlentheorie, den wir nicht beweisen wollen.

thm:haupt

Satz 156 (Primfaktorzerelgung)**.** *Jede Zahl $n \in \mathbb{N}$, $n \geq 2$, läßt sich als Produkt von Primzahlpotenzen schreiben, also $n = p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}$. Diese Darstellung ist eindeutig bis auf die Reihenfolge der Faktoren.*

Satz 157. *Es gibt unendlich viele Primzahlen.*

Beweis □

Beispiel 158.

1. Die Mersenne-Primzahlen sind von der Form $2^n - 1$ für $n \geq 2$.
2. Die Fermat'schen Zahlen (Fermat 1640) sind von der Form $2^{2^n} + 1$. Für $n \in \{0, 1, 2, 3, 4\}$ sind das Primzahlen. Für $n = 5$ hat Euler (etwa 1732) gezeigt, dass es sich nicht um eine Primzahl handelt. Für $n > 5$ ist das unbekannt.

Satz 159 (Primzahlsatz)**.** *Es sei $\pi(x)$ die Anzahl der Primzahlen $\leq x$. Dann wächst $\pi(x)$ für $x \to \infty$ wie $\frac{x}{\ln x}$.*

Beweis Ausgelassen □

Bemerkung 160 (Sieb des Eratosthenes)**.** Wir notieren die natürlichen Zahlen aufsteigend von links nach rechts bis zu einer frei wählbaren maximalen Zahl M. Dann streicht man die Vielfachen der ersten nicht gestrichenen Zahl von links. Die nächste nicht gestrichene Zahl ist eine Primzahl. Streiche deren Vielfache. die nächste nicht gestrichene Zahl ist die nächste Primzahl. So fährt man fort und erhält eine Liste von Primzahlen.

3.3 Teilbarkeitsregeln

Lemma 161. *Es seien $a \equiv b \mod n$ und $c \equiv d \mod n$. Dann gelten $a + b \equiv c + d \mod n$ und $ac \equiv bd \mod n$.*

Beweis □

Im 10er-System kann man eine Zahl $n \in \mathbb{N}$ darstellen durch

$$n = \sum_{i=0}^{k} a_i \cdot 10^i, \quad a_i \in \{0, 1, \ldots, 9\}.$$

Also hat n die Stellen $a_k a_{k-1} \cdots a_0$.

Satz 162. *Es sei $n = \sum_{i=0}^{k} a_i \cdot 10^i$ mit $a_i \in \{0, 1, \ldots, 9\}$. Es gelten die folgenen Teilbarkeitsregeln.*

1. $10|n \Leftrightarrow a_0 = 0$
2. $5|n \Leftrightarrow a_0 \in \{0, 5\}$
3. $2|n \Leftrightarrow a_0 \in \{0, 2, 4, 6, 8\}$

4. $4|n \Leftrightarrow 4|10a_1 + a_0$

5. $8|n \Leftrightarrow 8|100a_2 + 10a_1 + a_0$

6. $d \in \{3, 9\}: \quad d|n \Leftrightarrow d|Q(n) := \sum_{i=0}^{k} a_i$. *Man nennt* $Q(n)$ *die* Quersumme *von* n

7. $11|n \Leftrightarrow d|Q*(n) := \sum_{i=0}^{k}(-1)^i a_i$. *Man nennt* $Q*(n)$ *die* alternierende Quersumme *von* n

Beweis □

3.4 Fehlererkennung

Es sei V eine Menge. Eine Teilmenge $C \subset V$ heißt fehlererkennender Code, falls er folgende Prozedur ermöglicht: ein Sender übermittelt $c \in C$, ein Empfänger erhält ein möglicherweise verändertes $c' \in V$ und prüft, ob $c' \in C$ gilt. Der Code C ist so angelegt, dass eine Prüfprozedur durchgeführt werden kann.

3.4.1 Paritätscodes

eztdfn:pc

Definition 163. Es sei $q \in \mathbb{N}$, $q \geq 2$. Für $V := \{a_1a_2 \cdots a_n \,|\, a_1, \ldots, a_n \in \{0, \ldots, q-1\}\}$ heißt $C := \{a_1a_2 \cdots a_n \in V \,|\, a_1 + \cdots + a_n \equiv 0 \mod q\}$ Paritätscode zur Basis q der Länge n.

eztbsp:pc

Beispiel 164. Wir wählen $q = 10$ und $n = 5$. Also $V := \{a_1a_2a_3a_4a_5 \,|\, a_1, \ldots, a_5 \in \{0, \ldots, 9\}\}$ und $C := \{a_1a_2a_3a_4a_5 \in V \,|\, a_1 + \cdots + a_5 \equiv 0 \mod 10\}$. Dabei ist $a_1a_2a_3a_4$ die Information und a_5 die Prüfziffer. Zum Beispiel ist $12340 \in C$, also 0 die Prüfziffer für 1234. Dagegen ist zum BEispiel $12341 \notin C$.

Definition 165. Es sei C ein fehlererkennender Code. Ein Element $c \in C$ wird Codewort genannt. Wird ein Codewort an einer Stelle verändert, so nennt man dies einen Einzelfehler. Werden zwei verschiedene Stellen eines Codewortes vertauscht, nennt man dies einen Vertauschungsfehler.

Beispiel 166. Der Code aus 163 erkennt keine Vertauschungsfehler.

Satz 167. *Der Code aus 163 erkennt Einzelfehler.*

Beispiel 168. Um Vertauschungsfehler zu erkennen, stattet man Paritätscodes mit Gewichen aus. Zum Beispiel bei Kontonnummern:

Nummer	1	8	9	8	2	0	1	8
Gewicht	1	2	1	2	1	2	1	2
Produkt	1	16	9	16	2	0	1	16

Die Summe der Produkte ergibt 61. Aufrunden auf 10er ergibt die Prüfziffer 9. Die Kontonummer mit Prüfziffer lautet also 189820189. Der Code lautet formal: $C := \{a_1 \cdots a_9 \,|\, a_1, \ldots a_9 \in \{0, \ldots, 9\}, 1 \cdot a_1 + 2 \cdot a_2 \cdots + 2 \cdot a_8 + 1 \cdot a_9 \equiv 0 \mod 10\}$.

eztdfn:pcg

Definition 169. Eine Menge $C := \{a_1 \cdots a_n \,|\, a_1, \ldots a_n \in \{0, \ldots, q-1\}, \sum_{i=1}^{n} g_i a_i \equiv 0 \mod q\}$ heißt Paritätscode der Länge n zur Basis q mit Gewichten $g_1, \ldots, g_n \in \mathbb{Z}$.

Lemma 170. *Ist in Definition 169 die Zahl g_n teilerfremd zu q, dann lässt sich die Prüfziffer a_n aus $a_1, \ldots, a_{n-1}$ und den Gewichten berechnen.*

Satz 171. *Ein Paritätscode aus Definition 169 erkennt*

1. *Vertauschungen an den Stellen $i < j$ genau dann, wenn $g_j - g_i$ teilefremd zu q ist.*
2. *Einzelfehler an der Stelle i genau dann, wenn g_i teilerfremd zu q ist.*

Beispiel 172. Der ISBN-10-Code. Es ei $q = 11$ und $a_i \in \{0, 1, \ldots, 9, X\}$ für $1 \leq i \leq 10$.

3	–	528	–	12345	–	1
Sprache		Verlag		Buch		Prüfziffer

Die Gewichte seien $g_i := 11 - i$. Damit erkennt der gewichtete Paritätscode C sowohl Einzel- als auch Vertauschungsfehler. Berechnung der Prüfziffer:

1. 3-528-06783-a_{10} liefert Prüfziffer $a_{10} = 7$.
2. 3-528-06786-a_{10} liefert $a_{10} \equiv 10 \mod 11$ also $a_{10} = X$.

3.4.2 Codes über Gruppen

Im folgenden sei $(G, \cdot)$ eine (möglicherweise nicht-kommutative) Gruppe, mit neutralem Element 1 und inversen Elementen g^{-1} zu $g \in G$. Als Beispiele kenn wir $(\mathbb{Q}, +), (\mathbb{Z}_n, +)$ oder auch $(\mathbb{Z}_p \backslash \{0\}, \cdot)$ für eine Primzahl p.

eztdfn:gc

Definition 173. Ein Code über eine Gruppe $(G, \cdot)$ der Länge n mit Kontrollsymbol $c \in G$ ist gegeben durch

$$C := \{(g_1, \ldots, g_n) \in G^n \,|\, g_1 g_2 \cdot \ldots \cdot g_n = c\}.$$

Beispiel 174. Die Gruppe $(G, \cdot) := (\mathbb{Z}_{10}, \cdot)$ mit $c = 0$ liefert den Paritätscode aus Beispiel 164 mit $n = 5$.

eztthm:gcef

Satz 175. *Jeder Code aus Definiton 173 erkennt Einzelfehler.*

Bemerkung 176. Der Beweis von Satz 175 zeigt, dass die Wahl des Kontrollsymbols unerheblich ist. Der Vorteil von Gruppencodes ist, dass die Gruppen nicht kommutativ sein müssen. Man erhält die folgende Verallgemeinerung um Vertauschungsfehler zu erkennen:

eztdfn:gcperm

Definition 177. Ein Code über eine Gruppe $(G, \cdot)$ der Länge n mit Kontrollsymbol $c \in G$ und Permutationen $\pi_1, \ldots, \pi_n \in S_G := \{\pi : G \to G \,|\, \pi \text{ bijektiv}\}$ ist gegeben durch

$$C := \{(g_1, \ldots, g_n) \in G^n \,|\, \pi_1(g_1)\pi_2(g_2) \cdot \ldots \cdot \pi_n(g_n) = c\}.$$

Beispiel 178. Es sei $(G, \cdot) = (\mathbb{Z}_{10}, +)$ und C ein Paritätscode mit Gewichten $s_1, \ldots, s_n$, die jeweils teilerfremd zu 10 sind. Dann ist durch $\pi_i : \mathbb{Z}_{10} \to \mathbb{Z}_{10}$ gegeben durch $x \mapsto s_i x$ eine Permutation gegeben. Wir zeigen dazu, dass π_i bijektiv ist:

1. injektiv: $\pi_i(x) = \pi_i(y) \Longrightarrow s_i x \equiv s_i y \mod 10 \Longrightarrow s_i(x-y) \equiv 0 \mod 10 \Longrightarrow 10 | x - y \Longrightarrow x = y \in \{0, \ldots, 9\}$.

2. surjektiv: sei $x \in \mathbb{Z}_{10}$ vorgelegt. Nach dem Satz von Bezout gilt $1 = 10a + s_i b$ für gewisee $a, b \in \mathbb{Z}$. Also $x \equiv s_i x b \mod 10$ und daher folgt $\pi_i(xb) = s_i x b \equiv x \mod 10$.

Insgesamt ist C also ein Gruppencode mit Permutationen.

eztthm:gcpermfehl

Satz 179. *Ein Gruppencode wie in Definition 177 erkennt*

1. *Einzelfehler und*

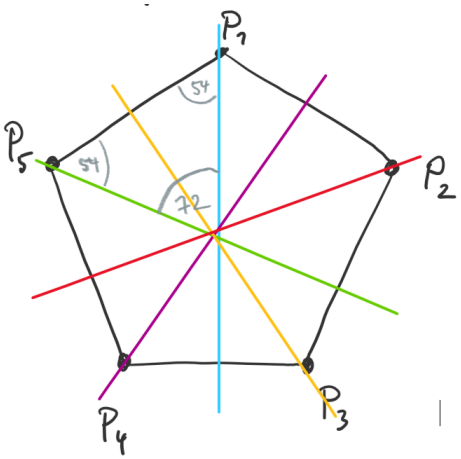
2. *Vertauschungen an den Stellen $i, i+1$ für $i \in \{1, \ldots, n-1\}$, falls für alle $g, h \in G$ gilt:*

$$\pi_i(g)\pi_{i+1}(h) \neq \pi_i(h)\pi_{i+1}(g).$$

Bemerkung 180. In $\mathbb{Z}_{10}$ kann meine keine Permutationen derart wählen, dass die Bedingung aus Satz 179.2 erfüllt ist. Soll die Prüfziffer aus 10 Elementen wählbar sein, braucht man eine nicht-kommutative Gruppe mit 10 Elementen. Das führt uns zur Betrachtung der Diedergruppe D_5.

3.4.3 Die Diedergruppe

Die Elemente der Diedergruppe $D_5 := \{0, 1, 2, \ldots, 9\}$ sind Isometrien des regulären 5-Ecks. Das sind Drehungen und Spiegelungen. Die Verknüpfung $\circ$ ist die Hintereinanderausführung dieser Abbildungen. Genauer gilt



Für $k \in \{0, \ldots, 4\}$

$k :=$ Drehung um $k \cdot 72°$

gegen den Uhrzeigersinn

$k \in \{5, 6, 7, 8, 9\}$ = Spiegelung an Geraden durch:

P1 P3 P5 P2 P4

MAn rechnet nach, dass $5 \circ 1 = 1^4 \circ 5$ gilt. Damit erhält man folgende Verknüpfungstabelle:

*	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	0	6	7	8	9	5
2	2	3	4	0	1	7	8	9	5	6
3	3	4	0	1	2	8	9	5	6	7
4	4	0	1	2	3	9	5	6	7	8
5	5	9	8	7	6	0	4	3	2	1
6	6	5	9	8	7	1	0	4	3	2
7	7	6	5	9	8	2	1	0	4	3
8	8	7	6	5	9	3	2	1	0	4
9	9	8	7	6	5	4	3	2	1	0

Satz 181. *Die Diedergruppe $(D_5, \circ)$ bildet eine nicht-kommutative Gruppe.*

Beispiel 182. Der Banknotencode für Deutsche Mark. Wir betrachten nun die Permutation

$$\pi_1 := \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 7 & 6 & 2 & 8 & 3 & 0 & 9 & 4 \end{pmatrix}$$

und definieren $\pi_k := \pi_1^k$ für $k \in \mathbb{N}$. Auf den Scheinen kommen 10 Buchstaben vor, die wie folgt durch Zahlen ersetzt werden:

$$\begin{array}{cccccccccc} A & D & G & K & L & N & S & U & V & Z \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{array}.$$

Wir betrachten den Gruppencode zur Diedergruppe mit Kontrollsymbol $c = 0$, $n = 11$, Permutationen π^k für $1 \leq k \leq 10$ und $\pi_{11} = id$. Die Prüfziffer berechnet sich damit wie folgt:

$$\pi_1(g_1) \circ \pi_2(g_2) \circ \ldots \circ \pi_{10}(g_{10}) \circ g_{11} = 0 \;\Rightarrow\; g_{11} = (\pi_1(g_1) \circ \pi_2(g_2) \circ \ldots \circ \pi_{10}(g_{10}))^{-1}.$$

Als Beispiel sei AU1210706Z eine Banknotennummer. Ohne Buchstaben ergibt das 0712107069. Man berechnet $\pi_1(0) = 1,\ \pi_2(7) = 1, \ldots, \pi_{10}(9) = 2$ und daraus $g_{11}^{-1} = 2$ also $g_{11} = 3$. Somit ist AU1210706Z3 die Geldscheinnummer mit Prüfziffer. Der Code erkennt nach Satz 179 alle Einzelfehler. Dass Vertauschungen erkannt werden muss für alle Elemente und Permutationen nachgerechnet werden. Immerhin sieht man sofort, dass Vertauschungen der letzten beiden Stellen erkannt werden.

3.5 Kryptologie

ist die Wissenschaft, die sich mit Ver- und Entschlüsselung von Informationen und damit mit der Informationssicherheit beschäftigt. Arbeitsfelder sind Verschlüsselungsverfahren und digitale Signaturen (Authentifizierung). Man unterteilt die Kryptologie in

1. Kryptographie (Symmetrische Kryptographie, Asymmetrische Kryptographie = Public-Key-Verfahren)

2. Kryptoanalyse (Sicherheitsanalyse von Verfahren)

Ver- und Entschlüsselung von Informationen dient dazu, Nachrichten zu übertragen ohne dass Dritte die Informationen abfangen können, beziehungsweise die abgefangenen Informationen nicht ohne weiteres lesen können. Bei *symmetrischen* Verschlüsselungsverfahren besitzen Sender und Empfänger denselben Schlüssel S. Der Sender verschlüsselt eine Nachricht mit S und verschickt sie. Der Empfänger entschlüsselt daraufhin auch mit S. Bei dr *asymmetrischen* Verschlüsselung erzeugt der Empfänger einen öffentlichen und einen privaten Schlüssel. Den Privaten hält er geheim. Der öffentliche wird bekannt gegeben. Mit diesem verschlüsselt der Sender seine Nachricht. Der Empfänger entschlüsselt sie mit seinem privaten Schlüssel.

3.5.1 Public-Key-Verschlüsselung

Wir beschreiben das allgemeine Verfahren: jeder Teilnehmer T erhält einen öffentlichen Schlüssel E_T und einen privaten Schlüssel D_T mit den Eigenschaften

1. Entschlüsselungseigenschaft: für jede NAchricht m gilt $D_T(E_T(m)) = m$. Der Geheimtext ist also $E_T(m)$.

2. Public-Key Eigenschaft: der private Schlüssel lässt sich in der Praxis nicht aus dem öffentlchen Schlüssel ermitteln.

Der Vorteil dieser Konstruktion ist, dass keine Schlüssel ausgetauscht werden müssen. Dieses Verfahren eigent sich daher auch gut für mehrere Teilnehmende.

Möchte man nicht Nachrichten übertragen sondern Sender authentifizieren, so ersetzt man die erste Bedingung durch die

1') Authentifizierungseigenschaft: $E_T(D_T(m)) = m$ für alle Nachrichten m.

Das Authentifizierungsverfahren läuft dann so ab:

- Sender verschlüsselt m zu $D_T(m)$ und verschickt m und $D_T(m)$
- Empfänger entschlüsselt zu $E_T(D_T(m))$ und vergleicht mit m

Eine Kombination beider Verfahren gibt folgendes Beispiel einer zu verschickenden Mail.
Sender:

s1) Mail und Anlage werden mit einem Kennwort m verschlüsselt (zum Beispiel mit einem symmetrischen Verfahren)

s2) Kennwort m wird mit dem öffentlichen Schlüssel des Empfängers zu $E_{T'}(m)$ verschlüsselt

s3) Prüfsumme s der Mail wird mit eigenem privaten Schlüssel zu $D_T(s)$ verschlüsselt.

s4) Verschicken von s, $D_T(s)$ und $E_{T'}(m)$.

Empfänger:

e1) Entschlüsselt s3) mit Public-Key des Senders zu $E_T(D_T(s))$ und vergleicht mit der Signatur s.

e2) Entschlüsselt Einmalkennwort mit seinem privaten Schlüssel zu $D_{T'}(E_{T'}(m) = m$.

e3) DEcodiert die Mail mit Kennwort aus e3).

3.5.2 Das RSA-Verfahren

Dieses Verfahren ist benannt nach Riverst, Shamir, Adleman (1978). Für sehr große Primzahlen $p, q \in \mathbb{N}$, $p \neq q$ ist es einfach $n = pq$ zu berechnen. Aber aus $n \in \mathbb{N}$ die Primfaktorzerlegung zu bestimmen ist sehr aufwändig. Dieser Umstand liefert die Grundlage für die Sicherheit dieses Verfahrens.

Satz 183 (Kleiner Satz von Fermat)**.** *Für $m \in \mathbb{N}$ und jede Primzahl $p \in \mathbb{N}$ gilt:*

$$m^{p-1} \equiv 1 \mod p.$$

Beweis □

Definition 184. Die Euler'sche ϕ-Funktion ist die Abbildung $\phi : \mathbb{N} \to \mathbb{N}$ gegeben durch

$$\phi(n) = |\{a \in \mathbb{N} \mid \text{ggT}(a, n) = 1\}|.$$

Zu $n \in \mathbb{N}$ ist $\phi(n)$ also die Anzahl der zu n teilerfremden Zahlen $< n$.

Satz 185. *Für teilerfremde Zahlen $m, n \in \mathbb{N}$ gilt $\phi(nm) = \phi(n)\phi(m)$.*

Beweis ausgelassen □

Lemma 186. *Es seien p, q Primzahlen, $x \equiv 1 \mod p$ und $x \equiv 1 \mod q$. Dann gilt $x \equiv 1 \mod pq$.*

Beweis □

Satz 187 (Euler)**.** *Es seien p, q verschiedene Primzahlen und $n = pq$. Für alle $m, n \in \mathbb{N}$ gilt*

$$m^{k \cdot \phi(n)+1} \equiv 1 \mod n.$$

Beweis □

Beschreibung des RSA-Algorithmus:

1. Wähle einen RSA-Modul $n = pq$ mit sehr großen verschiedenen Primzahlen p und q. Berechne $\phi(n) = \phi(p)\phi(q) = (p-1)(q-1)$.

2. Wähle ein $e \in \mathbb{N}$ mit $\text{ggT}(e, \phi(n)) = 1$. Berechne mit dem erweiterten Euklidischen Algorithmus ein $d \in \mathbb{N}$ mit $de \equiv 1 \mod \phi(n)$. Dann gilt also $ed = 1 + k \cdot \phi(n)$ für ein $k \in \mathbb{Z}$.

3. Veröffentliche (e, n) als öffentllichen Schlüssel. Behalte (d, n) als privaten Schlüssel geheim.

4. Stelle die zu verschlüsselnde Nachricht als Zahl m mit $m < n$ dar.

5a) Zur Nachrichtenverschlüsselung wendet man auf m das RSA-Verschlüsselungsverfahren an: der Sender verschlüsselt m mit Hilfe des öffentlichen Schlüssles des Empfängers zu $c := m^e \mod n$. Dann versendet er die Nachricht c. Diese wird vom Empfänger mit seinem privaten Schlüssel (d, n) entschlüsselt, indem er $c^d \mod n$ berechnet:

$$c^d \equiv (m^e)^d \equiv m^{ed} \equiv m^{k\phi(n)+1} \equiv m \mod n.$$

Also ergibt sich wegen $m < n$ der Klartext.

5b) Zur Authentifizierung wendet man das RSA-Signaturschema an: der Signieredne erstellt seinen privaten Schlüssel (d, n) und die signierte Nachricht $sig(m) := m^d \mod n$. Dann übermittelt er m und $sig(m)$. Der Empfänger prüft die Signatur, indem er $(sig(m))^e \mod n$ berechnet und mit m vergleicht. Stimmen diese überein, so wurde m mit dem privaten Schlüssel erschlüsselt, denn:

$$(sig(m))^e = (m^d)^e \equiv m^{de} \equiv m^{k\phi(n)+1} \equiv m \mod n\ .$$

Beispiel 188. Es soll eine Nachricht von B nach A verschickt werden.

1. A
   (a) wählt $p = 11$, $q = 7 \Rightarrow n = 55, \phi(n) = 40$
   (b) wählt $e = 7$, das ist wegen $\text{ggT}(7, 40) = 1$ erlaubt
   (c) $(7, 55)$ ist der öffentliche Schlüssel
   (d) veröffentlicht den öffentlichen Schlüssel
2. B
   (a) wählt Nachricht $m = 8 < 55$.
   (b) verschlüsselt $m = 8$ mit $(7, 55)$ zu

$$c \equiv 8^7 \mod 55 \equiv 64^3 \cdot 8 \equiv 9^3 \cdot 8 \equiv 81 \cdot 72 \equiv 26 \cdot 17 \equiv 442 \equiv 2 \mod 55\ .$$

   (c) übermittel $c = 2$ an B
3. B
   (a) bestimmt privaten Schlüssel $(d, 55)$ aus $7e \equiv 1 \mod 40$ mit Hilfe des erweiterten Euklidischen Algorithmus. Es ergibt sich $d \equiv 23 \mod 40$. Daher ist $(23, 55)$ der private Schlüssel.

(b) entschlüsselt $c = 2$ zu

$$c^d \equiv 23^2 \equiv 64^3 \cdot 32 \equiv 9^3 \cdot 32 \equiv 81 \cdot 288 \equiv 26 \cdot 13 \equiv 338 \equiv 8 \equiv m \mod 55 .$$

Bemerkung 189. Theoretisch kann man beim RSA-Verfahren den Privaten aus dem öffentlichen Schlüssel berechnen. Dazu muss man $\phi(n)$ aus n berechnen. Wegen $n = pq$ und p, q unbekannt ist das genauso schwierig wie p, q aus n zu berechnen.

3.5.3 Symmetrische Verschlüsselungsverfahren

Der Polybios-Code

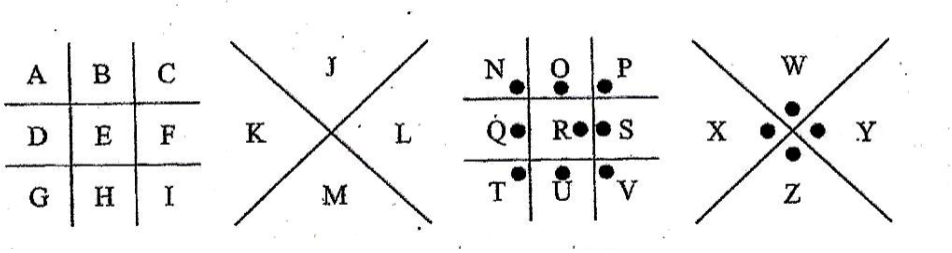
Die Nachricht wird mit Hilfe einer 5×5-Matrix zu Zahlen codiert:

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I, J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Das Wort LIEBE zum Beispiel wird zu 3124151215 .

Der Freimaurer-Code

Nach folgendem Schema wir jeder Buchstabe durch ein Zeichen ersetzt:



Cäsar-Code

Schreibe das Klartext-Alphabet auf und darunter um einige Stellen versetzt nochmals dieses Alphabet.

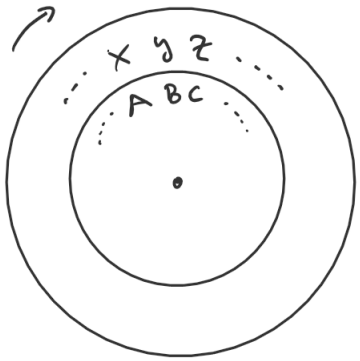
Klartext Alphabet Geheimtext Alphabet

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
V W X Y Z A B C D E F G H I J K L M N O P Q R S T U

Ersetze dann wie fdgt: A ↦ V, B ↦ W usw.

um Beispiel: LIEBE ⟷ GDZWZ

Später ($\approx$ 1500) wurde die Cäsar-Scheibe erfunden:



Der "Schlüssel" bei diesen Verschlüsselungen ist die Zuordnung eines beliebigen Buchstabens (zB A).

Das Vignère-Verfahren

Polyalphabetischer Codes versuchen eine Gleichverteilung unter den Buchstaben zu erreichen. Nimmt man zB das Schlüsselwort DACH:

D A C H D A C H D A C H
P O L Y A L P H A B E T
↓ ↓ ↓ ↓ ... ↓ ↓ ← Vigenère-
I S O N Quadrat

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Das Vigenère-Quadrat

Das Vigenère-Verfahren ist zwar schwieriger zu "knacken"

Wie kann man einen Code knacken?

1. Systematisches Durchprobieren aller Schlüssel. Das funktioniert gut, wenn es wie beim Cäsar-Code wenige Schlüssel gibt. Als Ausweg beim Cäsar-Code kann man diesen derart modifizieren, dass man beliebige Permutationen des Alphabets als Geheimalphabet zulässt. Das ergibt 26! verschiedene Schlüssel.

2. Statistische Analyse: mache eine Häufigkeitsanalyse der vorkommenden Buchstaben. Je nach Sprache gibt es typische Häufigkeiten. In der deutschen Sprache zum Beispiel: E=18%, N=10%. Als Ausweg kann man mehrere Alphabete wie zum Beispiel beim Vigenère-Verfahren verwenden. Dies führt zu einer Einteilung der Verfahren wie folgt:

Monoalphabetische Verfahren

sind Verschlüssellungen, bei denen jedem Buchstaben genau ein Geheimbuchstabe zugeordnet wird. Beispielsweise beim Cäsar-Code.

Polyalphabetiche Verfahren

sind Verschlüssellungen, bei denen einem Buchstaben verschiedene Geheimbuchstaben zugeordnet werden können. Zum Beispiel beim Vigenère-Verfahren.

Wie kann man den Vigenère-Code knacken?

Kennt man die Schlüssellänge n, so sind die Buchstaben $\mod n$ mit demselben Alphabet verschlüsselt. Dann lässt sich eine statistische Analyse durchführen. Kennt man die Schlüssellänge nicht, wendet man das Kasiski-Prinzip an:

1. Suche im Geheimtext Buchstabenfolgen der Länge 2 oder länger, die mehrfach vorkommen.

2. Bestimme die Abstände zwischen je zwei solchen Folgen. In folgendem Beispiel ist der Abstand der zwei ABC-Folgen gleich 6:

A	B	C	D	X	F	A	B	C
1	2	3	4	5	6			

3. Bestimme den ggT der gesammelten Abstände und vermute: dieser ist ein Vielfaches der Schlüssellänge.

4. Teste alle Teiler des ggT als Schlüssellänge.

Beispiel 190. Wir betrachten den folgenden mit dem Vigenere-Code verschlüsselten Text:

SPLDZPCNXLIHYKRTRYASXXNXLI
1 2 3 4 15

Die Folge NXLI kommt mit Abstand 15 zweimal vor.

Vermutung: dieselbe Wortteil/Silbe wurde verschlüsselt.

Vermutung: Wegen 15 = 3·5 hat Schlüsselwort die Länge 3, 5 oder 15.

Statistische Analyse: testen wir die Länge n = 5, so würden wir die Folge der 1., 6., 11., 16., ... Buchstaben analysieren und (falls der Text in deutscher Sprache verfasst wurde) unterstellen, dass der häufigste Buchstabe das "E" ist. Entsprechend verfährt man mit dem 2., 7., 12., ... Buchstaben und so weiter:

SPLDZPCNXLIHYKRTRYASX
PLUTOPLUTOPLUTOPLUTOPL
DERKLARTEXTUERDEGEHEIM

↑ Vigenère

Damit diese Analyse klappt, muss der Text in Relation zur Schlüssellänge "lang" sein. Ist zB das Schlüsselwort beim Vigenère-Verfahren gleich der Länge des Klartextes, so ist der Code unknackbar.