Mathematik für InformatikerInnen 2

Frank-Olaf Schreyer

Universität des Saarlandes, SS 2020

Ziel heute: Matrizen und Basiswechsel

- Charakeristik und Kardinalität von endlichen Körpern
- Die Matrix zu einer linearen Abbildung zwischen Vektorräumen mit Basen
- Kern, Bild und Rang
- Dimensionsformel für Untervektorräume
- Invertierbare Matrizen und die Berechnung der Inversen

In der letzten Vorlesung hatten wir gezeigt, dass jeder endlich–dimensionale K–Vektorraum V zu einem der Vektorräume K^n isomorph ist. Dabei ist $n = \dim V$. Allerdings gibt es viele Isomorphismen: Jede Basis $\mathcal{B} = \{v_1, \ldots, v_n\}$ von V induziert einen Isomorphismus

$$\varphi_{\mathcal{B}} : K^n \to V, e_j \mapsto v_j.$$

Ziel dieser Vorlesung ist es zu verstehen, wie sich Basiswechsel auswirken.

Charakeristik und Kardinalität von endlichen Körpern

Sei $\mathbb{F}$ ein endlicher Körper. Dann ist die kanonische Abbildung

$$\chi : \mathbb{N} \to \mathbb{F}, n \mapsto n \cdot 1_K = \sum_{j=1}^{n} 1_K$$

nicht injektiv. Im letzten Semester hatten wir gezeigt, dass

$$p = \min\{n \geq 1 \mid \chi(n) = 0\}$$

eine Primzahl ist, und somit $\mathbb{F}_p = \text{Bild}(\chi) \subset \mathbb{F}$ ein Unterkörper von $\mathbb{F}$ ist.

Definition. Man nennt die Primzahl p die **Charakteristik** von $\mathbb{F}$, in Zeichen, $\text{char}(\mathbb{F}) = p$.

Charakeristik und Kardinalität von endlichen Körpern, 2

Satz. *Sei $\mathbb{F}$ ein endlicher Körper der Charakteristik p. Dann gilt*

$$|\mathbb{F}| = p^e,$$

wobei $e = \dim_{\mathbb{F}_p} \mathbb{F}$ die Dimension von $\mathbb{F}$ als $\mathbb{F}_p$-Vektorraum ist.

Beweis. Als $\mathbb{F}_p$–Vektorraum ist $\mathbb{F} \cong \mathbb{F}_p^e$, und $|\mathbb{F}_p^e| = p^e$, da wir für jede Koordinate p Wahlmöglichkeiten haben. □

Bemerkung. Man kann zeigen, dass es zu jeder Primzahlpotenz $q = p^e$ einen Körper $\mathbb{F}_q$ mit genau q Elementen gibt.

Beispiel. $\mathbb{F}_4$ konstruiert man wie folgt. Wir betrachten den Polynomring $\mathbb{F}_p[x]$ und das Polynom $f = x^2 + x + 1$. Für $g \in \mathbb{F}_2[x]$ bezeichne $\overline{g}$ den Rest von g bei der Division mit Rest nach f. Dann ist

$$\mathbb{F}_4 = \{0 = \overline{0}, 1 = \overline{1}, \overline{x}, \overline{x+1}\}$$

die Menge aller möglichen Reste, und die Verknüpfungen sind durch

$$\overline{a} + \overline{b} = \overline{a+b}, \overline{a} \cdot \overline{b} = \overline{a \cdot b}$$

definiert.

Erinnerung: Homomorphismen

Letzte Stunde hatten wir lineare Abbildungen definiert: Eine Abbildung $f : V \to W$ zwischen K-Vektorräumen ist K-linear, wenn

$$f(\lambda_1 v_1 + \lambda_2 v_2) = \lambda_1 f(v_1) + \lambda_2 f(v_2) \quad \forall \lambda_1, \lambda_2 \in K \; \forall v_1, v_2 \in V$$

gilt. Eine (K-)lineare Abbildung $f : V \to W$ nennt man auch (Vektorraum)–**Homomorphismus**, da die Vektoraumstrukturen von linearen Abbildungen respektiert werden. Ein **Monomomorphismus** ist ein injektiver Homomorphismus, ein **Epimorphismus** ist ein surjektiver Homomorphismus, und schließlich **Isomorphismus** ist ein bijektiver Homomorphismus.

Kern und Bild

Definition. Sei $f : V \to W$ ein Homorphimus zwischen K-Vektorräumen. Dann heißt

$$\ker f = \{v \in V \mid f(v) = 0\}$$

der **Kern** von f und

$$\text{Bild}\, f = f(V) = \{w \in W \mid \exists v \in V \text{ mit } f(v) = w\}$$

das **Bild** von f.

Satz. *Sei $f : V \to W$ ein Vektorraumhomomorphismus.*

1. $\ker f$ *ist ein Untervektorraum von* V.
2. $\text{Bild}\, f$ *ist ein Untervektorraum von* W.
3. f *ist ein Monomorphismus (also injektiv) genau dann, wenn* $\ker f = 0$.

Beweis.

Satz. *Sei $f : V \to W$ ein Vektorraumhomomorphismus.*

1. $\ker f = \{v \in V \mid f(v) = 0\}$ *ist ein Untervektorraum von V.*
2. $\text{Bild } f = f(V)$ *ist ein Untervektorraum von W.*
3. *f ist ein Monomorphismus (also injektiv) genau dann, wenn* $\ker f = 0$.

Beweis. Zu 3.: Angenommen $\ker f = 0$, $v_1, v_2 \in V$ und $f(v_1) = f(v_2)$

$$\begin{aligned} &\Rightarrow \quad f(v_1 - v_2) = f(v_1) - f(v_2) = 0 \\ &\Rightarrow \quad v_1 - v_2 \in \ker f = \{0\} \\ &\Rightarrow \quad v_1 - v_2 = 0 \\ &\Rightarrow \quad v_1 = v_2 \end{aligned}$$

Also f ist injektiv.
Die umgekehrte Richtung ist klar, da bei einer injektiven Abbildung nur die 0 auf 0 abgebildet wird.

□

Ende Teil 1

Sei V ein K-Vektorraum und $\mathcal{B} = \{v_1, \dots v_n\}$ eine Basis. Wir fassen $\mathcal{B}$ nicht als eine Menge auf, sondern als eine **Liste** auf! Dies ist notwendig, damit der Isomorphimus

$$\varphi_{\mathcal{B}} : K^n \to V, f\left(\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}\right) = \sum_{i=1}^{n} a_i v_i$$

wohldefiniert ist.
Also $\mathcal{B} = \{v_1, v_2, \dots, v_n\}$ und die Basis $\mathcal{B}' = \{v_2, v_1, \dots, v_n\}$, die wir durch Vertauschen von v_1 mit v_2 erhalten sind von einander verschieden.
Wieviele Basen hat $\mathbb{F}_2^2$? Da $\dim \mathbb{F}_2^2 = 2$ gilt, besteht jede Basis aus zwei Vektoren.

Matrixdarstellungen einer linearen Abbildung

Definition. Seien V, W zwei endlich–dimensionale K-Vektorräume und $\mathcal{A} = \{v_1, \ldots, v_n\}$ bzw. $\mathcal{B} = \{w_1, \ldots, w_m\}$ Basen. Ist $f : V \to W$ eine lineare Abbildung, dann betrachten wir die Skalare $a_{ij} \in K$, definiert durch

$$f(v_j) = a_{1j}w_1 + a_{2j}w_2 + \cdots + a_{mj}w_m = \sum_{i=1}^{m} a_{ij}w_i \in W.$$

Dann heißt die Matrix

$$A = (a_{ij}) = M_{\mathcal{B}}^{\mathcal{A}}(f) \in K^{m \times n}$$

die **Matrixdarstellung** von f bezüglich der Basen $\mathcal{A}$ und $\mathcal{B}$.

Merkregel. Die j-te Spalte von A sind die Koeffizienten von $f(v_j)$ bzgl. der Basis $\mathcal{B}$ von W.

Beispiel. Sei $V = \mathbb{R}[x]_{\leq d}$, und seien $\alpha_1, \ldots, \alpha_{d+1} \in \mathbb{R}$. Die Abbildung

$$f \colon V \to \mathbb{R}^{d+1}, \quad p \mapsto \begin{pmatrix} p(\alpha_1) \\ \vdots \\ p(\alpha_{d+1}) \end{pmatrix}$$

ist $\mathbb{R}$-linear. Um die Darstellung von f bezüglich der Basen $\mathcal{A} = \{1, t, \ldots, t^d\}$ und $\mathcal{E} = \{e_1, \ldots, e_{d+1}\} \subset \mathbb{R}^{d+1}$ zu berechnen, betrachten wir für $j = 0, 2, \ldots, d$:

$$f(t^j) = \begin{pmatrix} \alpha_1^j \\ \vdots \\ \alpha_{d+1}^j \end{pmatrix} = \sum_{i=1}^{d+1} \alpha_i^j e_j.$$

Daher hat f die Matrixdarstellung

$$M_{\mathcal{E}}^{\mathcal{A}}(f) = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \ldots & \alpha_1^d \\ 1 & \alpha_2 & \ldots & \ldots & \alpha_1^d \\ \vdots & \vdots & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & \vdots \\ 1 & \alpha_{d+1} & \cdots & \cdots & \alpha_{d+1}^d \end{pmatrix} \in \mathbb{R}^{(d+1)\times(d+1)}.$$

Satz. *Sei $f : V \to W$ eine lineare Abbildung zwischen zwei Vektorräumen V und W. Ist $A = (a_{ij}) = M_{\mathcal{B}}^{\mathcal{A}}(f) \in K^{m\times n}$ die Matrixdarstellung bzgl. der Basen $\mathcal{A} = \{v_1, \ldots, v_n\}$ und $\mathcal{B} = \{w_1, \ldots, w_m\}$, so gilt:*

1. *Das Diagramm*

$$\begin{array}{ccc} V & \xrightarrow{f} & W \\ {\scriptstyle \varphi_{\mathcal{A}}}\uparrow & & \uparrow{\scriptstyle \varphi_{\mathcal{B}}} \\ K^n & \xrightarrow{A} & K^m \end{array}$$

   kommutiert, *das heißt*

$$f(\varphi_{\mathcal{A}}(x)) = \varphi_{\mathcal{B}}(Ax) \quad \forall x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in K^n.$$

2. *Jede Matrix $A \in K^{m\times n}$ liefert eine Abbildung f, so dass das Diagramm kommutiert.*

Beweis. Zu 1.: Der untere Pfeil ist

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \overset{A}{\mapsto} Ax = \begin{pmatrix} \sum_{j=1}^{n} a_{1j}x_j \\ \vdots \\ \sum_{j=1}^{n} a_{mj}x_j \end{pmatrix} \in K^m.$$

Unter $\varphi_{\mathcal{B}}$ (rechter Pfeil) geht dies über in:

$$\varphi_{\mathcal{B}}(Ax) = \varphi_{\mathcal{B}} \begin{pmatrix} \sum_{j=1}^{n} a_{1j}x_j \\ \vdots \\ \sum_{j=1}^{n} a_{mj}x_j \end{pmatrix} = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} a_{ij}x_j \right) w_i$$

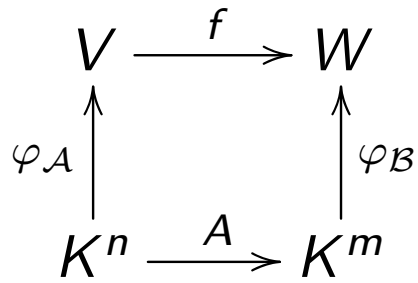
Betrachten wir nun den anderen Weg: Der linke Pfeil ist

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \overset{\varphi_{\mathcal{A}}}{\mapsto} \sum_{j=1}^{n} x_j v_j.$$

Unter f geht dies über in (oberer Pfeil):

$$f(\varphi_{\mathcal{A}}(x)) = f\left(\left(\sum_{j=1}^{n} x_j v_j \right) \right) = \sum_{j=1}^{n} x_j f(v_j) = \sum_{j=1}^{n} x_j \left(\sum_{i=1}^{m} a_{ij} w_i \right).$$

Zu 2.: Die Abbildung ist: $f = \varphi_{\mathcal{B}} \circ A \circ \varphi_{\mathcal{A}}^{-1}$.



Wir können lineare Abbildungen zwischen endlich–dimensionalen Vektorräumen also vollständig auf Matrixebene verstehen und die Abbildungen $\varphi_{\mathcal{A}}$ und $\varphi_{\mathcal{B}}$ benutzen, um zwischen den ursprünglichen Vektorräumen und dem K^n bzw. dem K^m hin- und herzuwechseln.

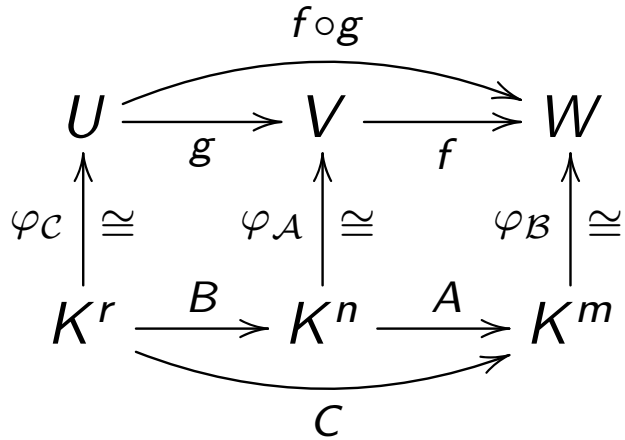
Ende Teil 2

Matrixprodukt

Korollar. *Es seien U, V, W drei K-Vektorräume jeweils mit Basen $\mathcal{C} = \{u_1, \ldots, u_r\}, \mathcal{A} = \{v_1, \ldots, v_n\}, \mathcal{B} = \{w_1, \ldots, w_m\}$. Es seien $g : U \to V$, $f : V \to W$ zwei lineare Abbildungen. Dann gilt für die Matrixdarstellungen $A = M_{\mathcal{B}}^{\mathcal{A}}(f), B = M_{\mathcal{A}}^{\mathcal{C}}(g)$ und $C = M_{\mathcal{B}}^{\mathcal{C}}(f \circ g)$, dass*

$$C = A \cdot B.$$

Mit anderen Worten: Das Diagramm



kommutiert; insbesondere heißt dies, dass das Matrixprodukt der Komposition von linearen Abbildungen entspricht.

Beweis. Wir betrachten die Hintereinanderausführung $f \circ g \colon U \to W$. Für einen Vektor u_k der Basis von U gilt:

$$\begin{aligned}(f \circ g)(u_k) &= f(g(u_k)) = f\Big(\sum_{j=1}^{n} b_{jk} v_j\Big) \\ &= \sum_{j=1}^{n} b_{jk} \cdot f(v_j) = \sum_{j=1}^{n} b_{jk} \cdot \sum_{i=1}^{m} a_{ij} w_i \\ &= \sum_{i=1}^{m} \Big(\sum_{j=1}^{n} a_{ij} b_{jk}\Big) \cdot w_i .\end{aligned}$$

Also:

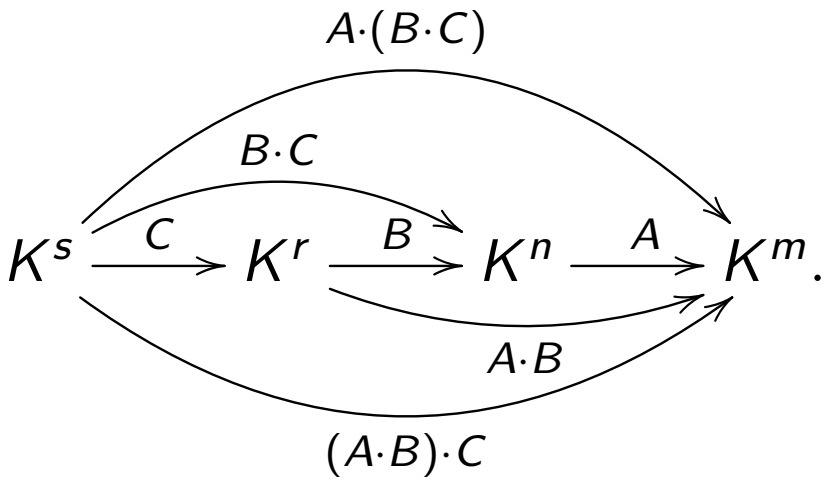
$$C = (c_{ik}) \in K^{m \times r} \text{ mit } c_{ik} = \sum_{j=1}^{n} a_{ij} b_{jk}$$

ist die Matrixdarstellung von $f \circ g$. □

Korollar. *Das Matrixprodukt ist assoziativ, das heißt:*

$$(A \cdot B) \cdot C = A \cdot (B \cdot C) \quad \forall A \in K^{m \times n} \; \forall B \in K^{n \times r} \; \forall C \in K^{r \times s}.$$

Beweis. Die Komposition von linearen Abbildungen ist assoziativ:



□

Invertierbare Matrizen

Definition. Eine quadratische Matrix $A \in K^{n\times n}$ heißt **invertierbar**, wenn die lineare Abbildung $f : K^n \to K^n$, $x \mapsto f(x) = Ax$, ein Isomorphismus ist. Die Matrixdarstellung der Umkehrabbildung $B = M_{\mathcal{E}}^{\mathcal{E}}(f^{-1}) \in K^{n\times n}$ erfüllt

$$B \cdot A = E = (\delta_{k\ell}).$$

Hierbei bezeichnet

$$\delta_{k\ell} := \begin{cases} 1, & \text{falls } k = \ell \\ 0, & \text{sonst} \end{cases}$$

das **Kroneckersymbol**; E ist also die **Einheitsmatrix**:

$$E = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix} \in K^{n\times n}.$$

Wir definieren die **inverse** Matrix von A durch $A^{-1} := B$.

Die allgemeine lineare Gruppe $\mathrm{GL}(n, K)$

Bemerkung. Es gilt: $f^{-1} \circ f = \mathrm{id}_{\mathbb{R}^n}$ also

$$M_{\mathcal{E}}^{\mathcal{E}}(f^{-1}) \cdot M_{\mathcal{E}}^{\mathcal{E}}(f) = M_{\mathcal{E}}^{\mathcal{E}}(\mathrm{id}_{\mathbb{R}^n}) \text{ d.h. } B \cdot A = E.$$

Da auch $f \circ f^{-1} = \mathrm{id}_{\mathbb{R}^n}$, gilt $A \cdot B = E$ ebenfalls.
A^{-1} ist durch A eindeutig bestimmt, denn es definiert die eindeutig bestimmte Umkehrabbildung

$$f : K^n \xrightarrow{A} K^n, \quad f^{-1} : K^n \xrightarrow{A^{-1}} K^n.$$

Definition. Die Menge der quadratischen invertierbaren $n \times n$–Matrizen über K bezeichnen wir mit

$$\mathrm{GL}(n, K) := \{A \in K^{n \times n} \mid A \text{ ist invertierbar}\}.$$

Vermöge des Matrizenproduktes ist $\mathrm{GL}(n, K)$ eine Gruppe im Sinne der nachfolgenden Definition.

Ende Teil 3

Die Axiome einer Gruppe

Definition. Eine **Gruppe** $(G, \cdot)$ ist eine Menge G zusammen mit einer Verknüpfung $\cdot$, das heißt einer Abbildung

$$G \times G \to G, \quad (a, b) \mapsto a \cdot b,$$

die folgenden Axiomen genügt:

G1) (Assoziativgesetz) $(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall a, b, c \in G$.

G2) (Existenz des neutralen Elements)
$\exists\, e \in G$ mit $e \cdot a = a \quad \forall a \in G$.

G3) (Existenz von Inversen)
$\forall a \in G, \exists a^{-1} \in G,$ so dass $a^{-1} \cdot a = e$.

Eine Gruppe heißt **abelsch** (nach N.H. Abel (1802-1829)) oder **kommutativ**, falls $a \cdot b = b \cdot a \; \forall a, b \in G$ gilt.

Bemerkung. Man kann aus den Axiomen folgendes herleiten:

- Das inverse Element a^{-1} zu $a \in G$ ist eindeutig bestimmt und erfüllt auch $a \cdot a^{-1} = e$
- Das neutrale Element ist eindeutig bestimmt und erfüllt auch $a \cdot e = a \; \forall a \in G$.

Beispiele.

1. $(\mathbb{Z}, +)$ ist eine abelsche Gruppe:
   $a + b \in \mathbb{Z}$, $\quad (a + b) + c = a + (b + c)$,
   $a + 0 = a \ \forall a \Rightarrow e = 0$, $\quad -a + a = 0$ (wird die Verknüpfung $+$ verwendet, dann schreibt man für a^{-1} meist $-a$).
2. $(\mathbb{Z}^*, \cdot)$ ist keine Gruppe ($\mathbb{Z}^* := \mathbb{Z} \setminus \{0\}$):
   $1 \cdot a = a \quad \forall a \in \mathbb{Z}$, 1 muß also das neutrale Element sein $(e = 1)$. Aber für $a \in \mathbb{Z}$ mit $|a| > 1$ existiert kein Inverses.
   Z.B: $\nexists b \in \mathbb{Z} : \ 2 \cdot b = 1$.
3. Sei K ein Körper. Dann sind $(K, +)$ und $(K^*, \cdot)$ abelsche Gruppen.

Bemerkung.

1. $\mathrm{GL}(n, K)$ für $n > 1$ ist nicht abelsch (siehe Übungsaufgaben).
2. Es gilt: $(A \cdot B)^{-1} = B^{-1} \cdot A^{-1}$, denn
   $A \cdot B \cdot B^{-1} \cdot A^{-1} = A \cdot E \cdot A^{-1} = A \cdot A^{-1} = E$.

Zeilenstufenform einer invertierbaren Matrix

Satz. *Sei $A \in K^{n\times n}$ eine quadratische Matrix. A ist invertierbar genau dann, wenn die Zeilenstufenform von A die maximal mögliche Anzahl von n Stufen hat.*

Beweis. Sei A invertierbar. Dann ist die Abbildung

$$K^n \to K^n, x \mapsto A \cdot x$$

surjektiv, d.h., das Gleichungssystem $Ax = c$ hat für beliebige rechte Seiten c eine Lösung. Dies ist genau dann der Fall, wenn die Zeilenstufenform von A genau n Stufen hat.
Umgekehrt hat die Zeilenstufenform von A die maximale mögliche Anzahl von n Stufen, dann können wir die Matrix $B = (b_{ij})$ betrachten, deren j-te Spalte die Lösung des Gleichungssystems

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \vdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} b_{1j} \\ b_{2j} \\ \vdots \\ b_{nj} \end{pmatrix} = \begin{pmatrix} \delta_{1j} \\ \delta_{2j} \\ \vdots \\ \delta_{nj} \end{pmatrix} = e_j.$$

Die Matrix B erfüllt dann $A \cdot B = E$, ist also die Inverse $A^{-1} = B$.

Gauß–Algorithmus zur Berechnung der Inversen.
Input. Eine quadratische Matrix $A \in K^{n\times n}$.
Output. Die Antwort auf die Frage, ob A invertierbar ist, und, wenn dies der Fall ist, die inverse Matrix $A^{-1} \in K^{n\times n}$.

1. Wir bilden die um E erweiterte Matrix

$$(A \mid E) = \left(\begin{array}{cccc|cccc} a_{11} & \cdots & \cdots & a_{1n} & 1 & 0 & \cdots & 0 \\ \vdots & a_{22} & & \vdots & 0 & 1 & \ddots & \vdots \\ \vdots & & \ddots & \vdots & \vdots & \ddots & \ddots & 0 \\ a_{n1} & \cdots & \cdots & a_{nn} & 0 & \cdots & 0 & 1 \end{array}\right)$$

2. Bringen $(A \mid E)$ in Zeilenstufenform $(\tilde{A}|\tilde{B})$. Sind die Stufen nicht $j_1 = 1, \ldots, j_n = n$, dann ist A nicht invertierbar.
3. Wir dividieren die k-te Zeile jeweils durch $\tilde{a}_{kk} \in K \setminus \{0\}$ (da die Zeilenstufenform genau n Stufen hat) und erhalten die Gestalt:

$$\rightsquigarrow (\tilde{\tilde{A}} \mid \tilde{\tilde{B}}) = \left(\begin{array}{ccc|c} 1 & \cdots & \tilde{\tilde{a}}_{1n} & \\ \vdots & \ddots & \vdots & \tilde{\tilde{b}}_{ij} \\ 0 & \cdots & 1 & \end{array}\right)$$

4. Wir räumen durch Zeilenoperationen die Einträge von $\tilde{\tilde{A}}$ oberhalb der Diagonalen sukzessive aus, etwa in der Reihenfolge:

$$\begin{array}{cccc} \tilde{\tilde{a}}_{n-1,n}, & \tilde{\tilde{a}}_{n-2,n}, & \dots, & \tilde{\tilde{a}}_{1,n} \\ & \tilde{\tilde{a}}_{n-2,n-1}, & \dots, & \vdots \\ & & \ddots & \vdots \\ & & & \tilde{\tilde{a}}_{1,2}. \end{array}$$

Dann haben wir eine Matrix:

$$\left(\begin{array}{ccc|c} 1 & \cdots & 0 & \\ \vdots & \ddots & \vdots & B \\ 0 & \cdots & 1 & \end{array}\right).$$

5. **return** $A^{-1} = B$.

Beweis. Korrektheit: Die j-te Spalte $b_{\bullet j}$ von B ist eine Lösung des Gleichungssystems $A \cdot b_{\bullet j} = e_j$, also ist B die Inverse nach dem Beweis des vorangegangenen Satzes. □

Beispiel.

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 0 & 3 & 7 \end{pmatrix} \quad \rightsquigarrow$$

$$\rightsquigarrow \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & -17/3 & 5/3 & 1 \\ 0 & 1 & 0 & 28/3 & -7/3 & -2 \\ 0 & 0 & 1 & -4 & 1 & 1 \end{array}\right).$$