

sprechend  $y < p$ ; A schickt  $u = a^x \bmod p$  an B und erhält dafür  $v = a^y \bmod p$ .

Sodann berechnet A die Zahl

$$v^x \bmod p = (a^y)^x \bmod p = a^{xy} \bmod p$$

und B entsprechend

$$u^y \bmod p = (a^x)^y \bmod p = a^{xy} \bmod p;$$

beide haben also auf verschiedene Weise dieselbe Zahl berechnet, die sie nun als Schlüssel in einem klassischen Kryptosystem verwenden können: Beispielsweise könnten die letzten 128, 196 oder 256 Bit der Zahl als AES-Schlüssel dienen.

Ein Gegner, der den Datenaustausch abgehört hat, kennt die Zahlen  $p, a, u$  und  $v$ ; um  $a^{xy} \bmod p$  zu finden, muß er den diskreten Logarithmus von  $u$  oder  $v$  berechnen.

Mit den besten heute bekannten Algorithmen ist die möglich, wenn  $p$  eine Primzahl von bis zu etwa 512 Bit ist, also ungefähr 155 Dezimalstellen hat; auch in diesem Fall dauert die Berechnung allerdings selbst bei massiver Parallelisierung über das Internet mehrere Monate, gefolgt von einer Schlußrechnung auf einem Supercomputer.

Da diskrete Logarithmen auch für die in Deutschland rechtlich bindenden digitalen Unterschriften verwendet wird, veröffentlicht die Regulierungsbehörde für Telekommunikation und Post jedes Jahr einen Bericht über sichere Kryptoverfahren. Nach ihrem neuesten Bericht vom August 2001 gelten Verfahren mit diskreten Logarithmen, egal ob in Körpern  $\mathbb{F}_p$  von Primzahlordnung oder Körpern  $\mathbb{F}_{2^n}$  von Zweierpotenzordnung bis Ende 2005 als sicher, wenn die Elementanzahl des Körpers mindestens 1024 Bit ab; für die Zeit bis Ende 2006 werden 2048 Bit empfohlen, aber nicht gefordert. Der Bericht ist zu finden unter [www.regtp.de/imperia/md/content/tech\\_reg\\_t/digisign/39.pdf](http://www.regtp.de/imperia/md/content/tech_reg_t/digisign/39.pdf).

Natürlich gibt es keine Garantie, daß kein Gegner mit einem besseren als den bislang bekannten Verfahren diskrete Logarithmen auch in weitaus größeren Körpern berechnen kann. Dazu bräuchte er allerdings einen

Durchbruch entweder auf der mathematischen oder auf der technischen Seite, für den weit und breit keine Grundlage zu sehen ist.

Falls sich allerdings die sogenannten *Quantencomputer* realisieren lassen, werden alle heute bekannten Verfahren der Kryptographie mit öffentlichen Schlüsseln, egal ob mit diskreten Logarithmen, RSA oder elliptischen Kurven, unsicher sein. Bislang können Quantencomputer kaum mit drei Bit rechnen, und nicht alle Experten sind davon überzeugt, daß es je welche geben wird, die mit mehreren Tausend Bit rechnen können.

### §3: Matrizen und lineare Gleichungssysteme

Die abstrakte Art und Weise, wie wir Vektoren und lineare Abbildungen bisher betrachtet haben, hat zwar den Vorteil, daß wir damit viele Probleme behandeln können, die nichts mit den gewohnten anschaulichen Vektoren zu tun haben; sie hat aber auch den Nachteil, daß wir bislang noch sehr wenige nichttriviale Beispiele konkret durchrechnen können. Dieser Paragraph soll die wichtigsten Hilfsmittel zum Rechnen in endlichdimensionalen Vektorräumen bereitstellen.

#### a) Abbildungsmatrizen

Basen sind nicht nur nützlich, um Vektoren darzustellen, sie können auch den Umgang mit linearen Abbildungen vereinfachen. Der Grund liegt im folgenden Lemma:

**Lemma:**  $V$  und  $W$  seien  $k$ -Vektorräume, und  $\mathcal{B}$  sei eine Basis von  $V$ . Dann ist jede lineare Abbildung  $\varphi: V \rightarrow W$  eindeutig bestimmt durch die Bilder  $\varphi(\vec{b})$  der Basisvektoren  $\vec{b} \in \mathcal{B}$ . Umgekehrt läßt sich auch jede Abbildung  $\varphi: \mathcal{B} \rightarrow W$  fortsetzen zu einer linearen Abbildung  $\varphi: V \rightarrow W$

*Beweis:* Jeder Vektor  $\vec{v} \in V$  läßt sich in eindeutiger Weise als Linearkombination

$$\vec{v} = \lambda_1 \vec{b}_1 + \dots + \lambda_n \vec{b}_n \quad \text{mit} \quad \vec{b}_1, \dots, \vec{b}_n \in \mathcal{B}$$

darstellen, und für eine lineare Abbildung  $\varphi$  muß dann

$$\varphi(\vec{v}) = \lambda_1 \varphi(\vec{b}_1) + \dots + \lambda_n \varphi(\vec{b}_n)$$

sein.

Besonders nützlich ist dies im Fall endlichdimensionaler Vektorräume.

Sei etwa  $V$  ein  $m$ -dimensionaler  $k$ -Vektorraum und  $W$  ein  $n$ -dimensionaler;

$$\mathcal{B} = \{\vec{b}_1, \dots, \vec{b}_m\} \subset V \quad \text{und} \quad \mathcal{C} = \{\vec{c}_1, \dots, \vec{c}_n\} \subset W$$

seien Basen.

Eine lineare Abbildung  $\varphi: V \rightarrow W$  ist, wie wir gerade gesehen haben, eindeutig bestimmt durch die Bilder der Basisvektoren  $\vec{b}_j$ ; diese wiederum lassen sich als Linearkombinationen der Basisvektoren  $\vec{c}_i$  schreiben:

$$\varphi(\vec{b}_j) = a_{1j}\vec{c}_1 + a_{2j}\vec{c}_2 + \dots + a_{nj}\vec{c}_n \quad \text{mit} \quad a_{ij} \in k.$$

Wenn wir die Basen  $\mathcal{B}$  und  $\mathcal{C}$  als *geordnete* Mengen auffassen, ist  $\varphi$  somit eindeutig bestimmt durch die  $n \cdot m$  Skalare  $a_{ij}$ ; wir fassen diese zusammen zu einer *Matrix*:

**Definition:** a) Eine  $n \times m$ -Matrix  $A$  über dem Körper  $k$  ist eine zweidimensionale Anordnung von Körperelementen  $a_{ij} \in k$  in  $n$  Zeilen und  $m$  Spalten, d.h.

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nm} \end{pmatrix}.$$

b) Die Menge aller  $n \times m$ -Matrizen  $A$  über  $k$  bezeichnen wir mit  $k^{n \times m}$ .

Die Matrix  $A$  zur linearen Abbildung  $\varphi$  bezeichnen wir als *Abbildungsmatrix* von  $\varphi$  bezüglich der (geordneten) Basen  $\mathcal{B}$  und  $\mathcal{C}$ ; wenn  $\mathcal{B}$  und  $\mathcal{C}$  vorgegeben sind, gibt es offensichtlich für jede Matrix  $A \in k^{n \times m}$  eine

lineare Abbildung  $\varphi: V \rightarrow W$  mit  $A$  als Abbildungsmatrix, nämlich diejenige lineare Abbildung, für die

$$\varphi(\vec{b}_j) = a_{1j}\vec{c}_1 + a_{2j}\vec{c}_2 + \dots + a_{nj}\vec{c}_n$$

ist. Bei gegebenen (geordneten) Basen entsprechen sich lineare Abbildungen und Matrizen also eindeutig (d.h. umkehrbar eindeutig): Zu jeder linearen Abbildung gibt es *genau* eine Matrix und zu jeder Matrix *genau* eine lineare Abbildung).

Matrizen als zweidimensionale Zahlenschemata sind natürlich erheblich älter als Vektorräume und lineare Abbildungen; erste Spuren aus dem zweiten vorchristlichen Jahrhundert finden sich bereits in den *Neun Büchern der Rechenkunst* 九章算術 aus der chinesischen Han-Dynastie. Rechenregeln für den Umgang mit Matrizen tauchen ab dem 16. Jahrhundert bei verschiedenen Autoren auf.

Als Beispiel betrachten wir den Vektorraum  $V$  aller reeller Polynome vom Grad höchstens vier und den Vektorraum  $W$  aller reeller Polynome vom Grad höchstens drei zusammen mit der linearen Abbildung

$$\varphi: V \rightarrow W; \quad f \mapsto f'.$$

Bevor wir eine Abbildungsmatrix berechnen können, brauchen wir zunächst Basen der beiden Vektorräume; am einfachsten nehmen wir dazu (mit der angegebenen Ordnung)

$$\mathcal{B} = \{1, X, X^2, X^3, X^4\} \subset V \quad \text{und} \quad \mathcal{C} = \{1, X, X^2, X^3\} \subset W.$$

Dann ist

$$\begin{aligned} \varphi(1) &= 0 &= 0 \cdot 1 + 0 \cdot X + 0 \cdot X^2 + 0 \cdot X^3 \\ \varphi(X) &= 1 &= 1 \cdot 1 + 0 \cdot X + 0 \cdot X^2 + 0 \cdot X^3 \\ \varphi(X^2) &= 2X &= 0 \cdot 1 + 2 \cdot X + 0 \cdot X^2 + 0 \cdot X^3 \\ \varphi(X^3) &= 3X^2 &= 0 \cdot 1 + 0 \cdot X + 3 \cdot X^2 + 0 \cdot X^3 \\ \varphi(X^4) &= 4X^3 &= 0 \cdot 1 + 0 \cdot X + 0 \cdot X^2 + 4 \cdot X^3, \end{aligned}$$

die Abbildungsmatrix ist also

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 4 \end{pmatrix} \in \mathbb{R}^{4 \times 5}.$$

Hier wie auch im allgemeineren Fall stehen in den *Spalten* der Abbildungsmatrix die Koeffizienten der Bilder der Basisvektoren von  $V$ , ausgedrückt bezüglich der Basis von  $W$ .

### b) Rechenregeln für Matrizen

Wir haben Matrizen eingeführt, um mit linearen Abbildungen konkret rechnen zu können; als erstes sollten wir uns dazu überlegen, wie man mit *Matrizen* rechnen kann.

Zu zwei  $n \times m$ -Matrizen

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nm} \end{pmatrix} \quad \text{und} \quad B = \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1m} \\ b_{21} & b_{22} & \dots & b_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \dots & b_{nm} \end{pmatrix}$$

können wir deren Summe

$$A + B \stackrel{\text{def}}{=} \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} & \dots & a_{1m} + b_{1m} \\ a_{21} + b_{21} & a_{22} + b_{22} & \dots & a_{2m} + b_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} + b_{n1} & a_{n2} + b_{n2} & \dots & a_{nm} + b_{nm} \end{pmatrix}$$

definieren, und für einen Skalar  $\lambda \in k$  auch das Produkt

$$\lambda A \stackrel{\text{def}}{=} \begin{pmatrix} \lambda a_{11} & \lambda a_{12} & \dots & \lambda a_{1m} \\ \lambda a_{21} & \lambda a_{22} & \dots & \lambda a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda a_{n1} & \lambda a_{n2} & \dots & \lambda a_{nm} \end{pmatrix}.$$

Das legt die Vermutung nahe, daß  $k^{n \times m}$  mit diesen beiden Verknüpfungen ein Vektorraum sein könnte, und in der Tat gilt:

**Lemma:**  $k^{n \times m}$  ist ein  $k$ -Vektorraum der Dimension  $nm$ .

*Beweis:* Beide Rechenoperationen sind so definiert, daß, wenn wir den  $ij$ -Eintrag für sich alleine betrachten, dort die entsprechende Rechenoperation im Grundkörper  $k$  ausgeführt wird. Da für die Rechenoperationen im Grundkörper alle bei der Definition eines Vektorraums geforderten Rechenregeln gelten, gelten sie auch in  $k^{n \times m}$ .

Beispielsweise ist also

$$A + B = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} & \dots & a_{1m} + b_{1m} \\ a_{21} + b_{21} & a_{22} + b_{22} & \dots & a_{2m} + b_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} + b_{n1} & a_{n2} + b_{n2} & \dots & a_{nm} + b_{nm} \end{pmatrix} = \begin{pmatrix} b_{11} + a_{11} & b_{12} + a_{12} & \dots & b_{1m} + a_{1m} \\ b_{21} + a_{21} & b_{22} + a_{22} & \dots & b_{2m} + a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} + a_{n1} & b_{n2} + a_{n2} & \dots & b_{nm} + a_{nm} \end{pmatrix} = B + A$$

und

$$\begin{aligned} \lambda(\mu A) &= \lambda \begin{pmatrix} \mu a_{11} & \mu a_{12} & \dots & \mu a_{1m} \\ \mu a_{21} & \mu a_{22} & \dots & \mu a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ \mu a_{n1} & \mu a_{n2} & \dots & \mu a_{nm} \end{pmatrix} \\ &= \begin{pmatrix} \lambda(\mu a_{11}) & \lambda(\mu a_{12}) & \dots & \lambda(\mu a_{1m}) \\ \lambda(\mu a_{21}) & \lambda(\mu a_{22}) & \dots & \lambda(\mu a_{2m}) \\ \vdots & \vdots & \ddots & \vdots \\ \lambda(\mu a_{n1}) & \lambda(\mu a_{n2}) & \dots & \lambda(\mu a_{nm}) \end{pmatrix} \\ &= \begin{pmatrix} (\lambda\mu)a_{11} & (\lambda\mu)a_{12} & \dots & (\lambda\mu)a_{1m} \\ (\lambda\mu)a_{21} & (\lambda\mu)a_{22} & \dots & (\lambda\mu)a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ (\lambda\mu)a_{n1} & (\lambda\mu)a_{n2} & \dots & (\lambda\mu)a_{nm} \end{pmatrix} = (\lambda\mu)A. \end{aligned}$$

Nullelement der Addition ist natürlich die Nullmatrix

$$\begin{pmatrix} 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 \end{pmatrix},$$

deren sämtliche Einträge null sind, und

$$- \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nm} \end{pmatrix} = \begin{pmatrix} -a_{11} & -a_{12} & \dots & -a_{1m} \\ -a_{21} & -a_{22} & \dots & -a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \dots & -a_{nm} \end{pmatrix}.$$

Schließlich müssen wir uns noch überlegen, daß  $k^{n \times m}$  die Dimension  $nm$  hat; wir wir am Ende von §1h) gesehen haben, ist das gleichbedeutend damit, daß es eine Basis aus  $nm$  Matrizen gibt.

Als eine solche Basis wählen wir die Menge aller Matrizen  $E_{ij}$ , die so definiert sind, daß  $E_{ij}$  an der Stelle  $ij$  eine Eins stehen hat und sonst lauter Nullen.

$$\text{In } k^{4 \times 5} \text{ wäre also etwa } E_{23} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

In einem beliebigen  $k^{n \times m}$  läßt sich jede Matrix eindeutig als Linearkombination der  $E_{ij}$  schreiben, denn

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nm} \end{pmatrix} = \sum_{i=1}^n \sum_{j=1}^m a_{ij} E_{ij},$$

und ist

$$\sum_{i=1}^n \sum_{j=1}^m \lambda_{ij} E_{ij} = \begin{pmatrix} \lambda_{11} & \lambda_{12} & \dots & \lambda_{1m} \\ \lambda_{21} & \lambda_{22} & \dots & \lambda_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_{n1} & \lambda_{n2} & \dots & \lambda_{nm} \end{pmatrix}$$

die Nullmatrix, so müssen offensichtlich alle  $\lambda_{ij}$  verschwinden, die  $E_{ij}$  sind also auch linear unabhängig. Damit bilden sie eine Basis von  $k^{n \times m}$ , und  $\dim_k k^{n \times m} = nm$ . ■

Die Basis mit den Matrizen  $E_{ij}$  ist zwar sicherlich die einfachste Basis für den Vektorraum aller  $n \times m$ -Matrizen, aber nicht immer die beste: Matrizen bieten sich beispielsweise auch an, um digitalisierte Bilder darzustellen, und zumindest in digitalen Kameras oder Scannern entsteht das Bild wirklich als eine Matrix von Grauwerten  $b_{zw}$  als drei Matrizen von Farb- oder sonstigen Werten, dargestellt in der Basis aus den  $E_{ij}$ . Für die Übertragung oder Speicherung ist das aber selten optimal, da hier für jede Komponente der Basisdarstellung dieselbe Genauigkeit

erforderlich ist. Daher werden die Bilder etwa für die Speicherung im JPEG-Format zunächst in eine andere Basis umgerechnet, bezüglich derer viele Koeffizienten nahe bei Null liegen. Bei der Diskretisierung und Quantisierung entstehen dann viele Koeffizienten, für die nur wenige oder gar keine Bit benötigt werden, was im Zusammenspiel mit anderen Verfahren wie *run length encoding* und HUFFMAN-Codierung zu Komprimierungsfaktoren um die zwanzig oder dreißig ohne nennenswerten Qualitätsverlust führt.

Auch für zwei lineare Abbildungen  $\varphi, \psi: V \rightarrow W$  können wir eine Summe definieren, und für  $\lambda \in k$  auch ein Produkt  $\lambda\varphi$  durch

$$\varphi + \psi: \begin{cases} V \rightarrow W \\ \vec{v} \mapsto \varphi(\vec{v}) + \psi(\vec{v}) \end{cases} \quad \text{und} \quad \lambda\varphi: \begin{cases} V \rightarrow W \\ \vec{v} \mapsto \lambda\varphi(\vec{v}) \end{cases};$$

sind  $V$  und  $W$  endlichdimensional und sind  $A, B$  die Abbildungsmatrizen von  $\varphi, \psi$ , so hat  $\varphi + \psi$  offenbar die Abbildungsmatrix  $A + B$  und  $\lambda A$  ist die von  $\lambda\varphi$ .

Auch hier ist klar, daß die sämtlichen linearen Abbildungen  $V \rightarrow W$  einen Vektorraum bilden, da einfach für jeden Vektor  $\vec{v} \in V$  die Vektoroperationen von  $W$  auf die Bildvektoren angewendet werden; dieser Vektorraum wir mit  $\text{Hom}_k(V, W)$  bezeichnet nach dem Wort *Homomorphismus*, das man gelegentlich anstelle von *lineare Abbildung* gebraucht.

Im endlichdimensionalen Fall hat  $\text{Hom}_k(V, W)$  wegen der eindeutigen Entsprechung von linearen Abbildungen und Matrizen als Dimension das Produkt der Dimensionen von  $V$  und von  $W$ . Die Basismatrix  $E_{ij} \in k^{n \times m}$  entspricht dabei bezüglich der Basen  $\mathcal{B}$  von  $V$  und  $\mathcal{C}$  von  $W$  jener linearen Abbildung, die alle Vektoren aus  $\mathcal{B}$  mit Ausnahme des  $j$ -ten auf den Nullvektor abbildet; der  $j$ -te Basisvektor geht auf den  $i$ -ten Basisvektor aus  $\mathcal{C}$ . Bei den linearen Abbildungen  $k^5 \rightarrow k^4$  etwa entspräche obige Matrix  $E_{23}$  der linearen Abbildung

$$k^5 \rightarrow k^4; \quad \begin{pmatrix} u \\ v \\ w \\ x \\ y \end{pmatrix} \mapsto \begin{pmatrix} 0 \\ w \\ 0 \\ 0 \end{pmatrix}.$$

Lineare Abbildungen lassen sich nicht nur addieren und mit Skalaren multiplizieren; sie lassen sich auch, wie alle Abbildungen, hintereinanderausführen: Sind  $\psi: U \rightarrow V$  und  $\varphi: V \rightarrow W$  lineare Abbildungen, so ist auch

$$\varphi \circ \psi: U \rightarrow W; \quad \vec{v} \mapsto \varphi(\psi(\vec{v}))$$

eine lineare Abbildung.

Falls alle beteiligten Vektorräume endlichdimensional sind, können wir endliche Basen wählen; das seien etwa

$$\mathcal{B} = \{\vec{b}_1, \dots, \vec{b}_m\} \subset U, \quad \mathcal{C} = \{\vec{c}_1, \dots, \vec{c}_n\} \subset V$$

und

$$\mathcal{D} = \{\vec{d}_1, \dots, \vec{d}_p\} \subset W,$$

d.h.

$$\dim_k U = m, \quad \dim_k V = n \quad \text{und} \quad \dim_k W = p.$$

Dann haben wir Abbildungsmatrizen  $A \in k^{p \times n}$  von  $\varphi$  und  $B \in k^{n \times m}$  von  $\psi$ ; wir wollen die Abbildungsmatrix  $C \in k^{p \times m}$  von  $\varphi \circ \psi: U \rightarrow W$  berechnen.

Nach Definition der Abbildungsmatrizen  $A = (a_{i\ell})$  von  $\varphi$  und  $B = (b_{j\ell})$  von  $\psi$  ist

$$\begin{aligned} \varphi \circ \psi(\vec{b}_i) &= \varphi\left(\psi(\vec{b}_i)\right) = \varphi\left(\sum_{j=1}^n b_{ji} \vec{c}_j\right) = \sum_{j=1}^n b_{ji} \varphi(\vec{c}_j) \\ &= \sum_{j=1}^n b_{ji} \sum_{\ell=1}^p a_{\ell j} \vec{d}_\ell = \sum_{\ell=1}^p \left(\sum_{j=1}^n a_{\ell j} b_{ji}\right) \vec{d}_\ell. \end{aligned}$$

Für die Abbildungsmatrix  $C = (c_{i\ell})$  von  $\varphi \circ \psi$  ist nach Definition

$$\varphi \circ \psi(\vec{b}_i) = \sum_{\ell=1}^p c_{\ell i} \vec{d}_\ell,$$

also ist

$$c_{\ell i} = \sum_{j=1}^n a_{\ell j} b_{ji}.$$

**Definition:** Für zwei Matrizen  $A = (a_{i\ell}) \in k^{p \times n}$  und  $B = (b_{\ell j}) \in k^{n \times m}$  bezeichnen wir die Matrix  $C = (c_{ij}) \in k^{p \times m}$  mit

$$c_{ij} = \sum_{\ell=1}^n a_{i\ell} b_{\ell j}$$

als *Produktmatrix*  $C = AB$  von  $A$  und  $B$ .

Für praktische Rechnungen empfiehlt es sich als Eselsbrücke, den zweiten Faktor des Produkts höher zu stellen nach dem Schema

$$\begin{pmatrix} \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{i1} & \dots & a_{im} & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix} \begin{pmatrix} \dots & b_{1j} & \dots \\ \vdots & \vdots & \vdots \\ \dots & b_{mj} & \dots \end{pmatrix} = \begin{pmatrix} \dots & \sum_{\ell=1}^m a_{i\ell} b_{\ell j} & \dots \\ \vdots & \vdots & \vdots \\ \dots & \vdots & \dots \end{pmatrix};$$

dadurch behält man den Überblick, welcher Rechenschritt jeweils als nächster auszuführen ist.

Im Gegensatz zu den meisten bislang aufgetretenen Produkten ist dieses Matrixprodukt im allgemeinen *nicht* kommutativ: Falls nicht zufälligerweise  $n = p$  sein sollte, ist das Matrixprodukt  $BA$  nicht einmal definiert, geschweige denn gleich  $AB$ . Allgemein ist Kommutativität bei der Hintereinanderausführung von Abbildungen eine sehr seltene Ausnahmeerscheinung; schließlich ist auch  $\sin(x^2) \neq \sin^2 x$  für fast jedes  $x$ , und so ist auch bei Matrizen, selbst wenn beide Produkte definiert sind, im allgemeinen  $AB \neq BA$ . Beispielsweise ist

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

aber

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

Ansonsten gelten aber doch die meisten bekannten Rechenregeln, beispielsweise das *Assoziativitätsgesetz*

$$A(BC) = (AB)C \quad \text{für alle } A \in k^{n \times m}, B \in k^{m \times p}, C \in k^{p \times q}.$$

Es ist durchaus möglich (und verglichen mit manch anderen Dingen sogar nicht einmal so extrem aufwendig), dieses Gesetz nach obiger Formel explizit nachzurechnen. Bevor wir uns das antun, sollten wir uns aber daran erinnern, wo das Matrixprodukt eigentlich herkommt: Matrizen entsprechen umkehrbar eindeutig linearen Abbildungen, und das Matrixprodukt entspricht deren Hintereinanderausführung. Für die Hintereinanderausführung von Abbildungen (egal ob linear oder nicht) ist das Assoziativgesetz aber trivial: Sind etwa

$$\varphi: k^m \rightarrow k^n, \quad \psi: k^n \rightarrow k^p \quad \text{und} \quad \omega: k^q \rightarrow k^p$$

drei lineare Abbildungen mit Abbildungsmatrizen  $A, B, C$ , so ist für jeden Vektor  $\vec{v} \in k^q$  sowohl

$$(\varphi \circ (\psi \circ \omega))(\vec{v}) = \varphi(\psi \circ \omega)(\vec{v}) = \varphi(\psi(\omega(\vec{v})))$$

als auch

$$((\varphi \circ \psi) \circ \omega)(\vec{v}) = (\varphi \circ \psi)(\omega(\vec{v})) = \varphi(\psi(\omega(\vec{v}))),$$

d.h. für die Hintereinanderausführung von Abbildungen (egal ob linear oder nicht) ist das Assoziativgesetz

$$\varphi \circ (\psi \circ \omega) = (\varphi \circ \psi) \circ \omega$$

automatisch erfüllt.

Da nun  $A(BC)$  die Abbildungsmatrix von  $\varphi \circ (\psi \circ \omega)$  ist und  $(AB)C$  die von  $(\varphi \circ \psi) \circ \omega$ , und da diese beiden Abbildungen übereinstimmen, müssen auch die Abbildungsmatrizen gleich sein, wir haben also gezeigt, daß

$$A(BC) = (AB)C \quad \text{für alle } A \in k^{n \times m}, B \in k^{m \times p}, C \in k^{p \times q},$$

ohne daß wir ein einziges Matrixprodukt explizit ausrechnen mußten.

Genauso folgen auch die Rechenregeln

$$A(B_1 + B_2) = AB_1 + AB_2 \quad \text{und} \quad (A_1 + A_2)B = A_1B + A_2B$$

aus den entsprechenden Rechenregeln

$$\varphi \circ (\psi_1 + \psi_2) = \varphi \circ \psi_1 + \varphi \circ \psi_2 \quad \text{und} \quad (\varphi_1 + \varphi_2) \circ \psi = \varphi_1 \circ \psi + \varphi_2 \circ \psi,$$

die sich wiederum leicht und ohne Rechnung überprüfen lassen:

$$\begin{aligned} (\varphi \circ (\psi_1 + \psi_2))(\vec{v}) &= \varphi(\psi_1(\vec{v}) + \psi_2(\vec{v})) = \varphi(\psi_1(\vec{v})) + \varphi(\psi_2(\vec{v})) \\ &= (\varphi \circ \psi_1)(\vec{v}) + (\varphi \circ \psi_2)(\vec{v}) = (\varphi \circ \psi_1 + \varphi \circ \psi_2)(\vec{v}) \end{aligned}$$

und

$$\begin{aligned} ((\varphi_1 + \varphi_2) \circ \psi)(\vec{v}) &= (\varphi_1 + \varphi_2)(\psi(\vec{v})) = \varphi_1(\psi(\vec{v})) + \varphi_2(\psi(\vec{v})) \\ &= (\varphi_1 \circ \psi)(\vec{v}) + (\varphi_2 \circ \psi)(\vec{v}) = (\varphi_1 \circ \psi + \varphi_2 \circ \psi)(\vec{v}). \end{aligned}$$

Da in der obigen Formel für die Matrixmultiplikation alle  $b_{ij}$  linear in den Ausdrücken für  $e_{ij}$  vorkommen usw., hätten sich die beiden letzten Rechenregeln auch einfach direkt nachrechnen lassen. Ebenfalls durch direktes Nachrechnen überzeugt man sich von der Formel

$$(\lambda A)B = \lambda(AB) = A(\lambda B) \quad \text{für alle } \lambda \in k,$$

und auch für die *Einheitsmatrix*

$$E = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix} \in k^{n \times n}$$

folgt sowohl durch Nachrechnen als auch durch Interpretation von  $E$  als Abbildungsmatrix der identischen Abbildung  $k^n \rightarrow k^n$ , die jeden Vektor auf sich selbst abbildet, daß

$$A \cdot E = A \quad \text{für alle } A \in k^{m \times n}$$

und

$$E \cdot A = A \quad \text{für alle } A \in k^{n \times m}$$

ist. Den Eintrag an der Stelle  $ij$  der Einheitsmatrix bezeichnet man als das **KRONECKER- $\delta$** :

$$\delta_{ij} = \begin{cases} 1 & \text{falls } i = j \\ 0 & \text{falls } i \neq j \end{cases}.$$



LEOPOLD KRONECKER (1823–1891) ist heute zwar vielen nur im Zusammenhang mit dem KRONECKER- $\delta$  bekannt, er war aber einer der bedeutendsten deutschen Mathematiker seiner Zeit. Seine Arbeiten befaßten sich mit Algebra, Zahlentheorie und Analysis, wobei er insbesondere die Verbindungen zwischen der Analysis und den beiden anderen Gebieten erforschte. Bekannt ist auch seine Ablehnung jeglicher mathematischer Methoden, die, wie die Mengenlehre oder Teile der Analysis, unendliche Konstruktionen verwenden. Er war deshalb mit vielen anderen bedeutenden Mathematikern seiner Zeit verfeindet, z.B. mit CANTOR und mit WEIERSTRASS.

Bei den reellen Zahlen und auch sonst in jedem Körper gibt es zu jedem Element  $a \neq 0$  ein inverses Element  $a^{-1}$ , so daß  $aa^{-1} = a^{-1}a = 1$  ist. Bei Matrizen muß es das selbst für quadratische Matrizen nicht geben:

Für eine beliebige Matrix  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  ist

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$$

und

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix},$$

was beides offensichtlich nie die Einheitsmatrix sein kann.

**Definition:** Eine  $n \times n$ -Matrix  $A \in k^{n \times n}$  heißt *invertierbar*, wenn es eine Matrix  $B \in k^{n \times n}$  gibt, so daß  $AB = BA = E$  ist.  $B$  heißt *inverse Matrix* von  $A$ ; in Zeichen  $B = A^{-1}$ .

(Es wäre theoretisch möglich, Invertierbarkeit auch für nicht-quadratische Matrizen zu definieren, aber das hat keinen sonderlichen Nutzen.)

Um zu sehen, wann eine Matrix  $A \in k^{n \times n}$  invertierbar ist, betrachten wir wieder die Situation bei den linearen Abbildungen: Zu einer linearen Abbildung  $\varphi: k^n \rightarrow k^n$  gibt es genau dann eine Umkehrabbildung  $\psi: k^n \rightarrow k^n$ , so daß  $\varphi \circ \psi$  und  $\psi \circ \varphi$  beide die identische Abbildung sind, wenn  $\varphi$  bijektiv ist. Nach dem Korollar am Ende von §17) ist dies genau dann der Fall, wenn  $\varphi$  surjektiv ist, wenn also das Bild von  $\varphi$  Dimension  $n$  hat. Dieses Bild wird aber erzeugt von den Bildern der

Einheitsvektoren, und das sind gerade die Spalten der Abbildungsmatrix. Diese  $n$  Vektoren erzeugen genau dann ganz  $k^n$ , wenn sie linear unabhängig sind.

**Definition:** Der (Spalten-)Rang einer Matrix  $A \in k^{n \times m}$  ist die maximale Anzahl linear unabhängiger Spaltenvektoren von  $A$ .

Nach obiger Diskussion gilt daher

**Lemma:** Eine Matrix  $A \in k^{n \times n}$  ist genau dann invertierbar, wenn sie Rang  $n$  hat. Die inverse Matrix  $B = A^{-1}$  ist sowohl durch die Bedingung  $AB = E$  als auch durch die Bedingung  $BA = E$  eindeutig bestimmt.

Die Eindeutigkeit der inversen Matrix folgt dabei natürlich aus der Eindeutigkeit der Umkehrabbildung.

### c) Matrixdarstellung der komplexen Zahlen

Die komplexen Zahlen bilden mit ihrer üblichen Addition und der Einschränkung der üblichen Multiplikation zu einer Abbildung

$$\cdot: \begin{cases} \mathbb{R} \times \mathbb{C} \rightarrow \mathbb{C} \\ (r, z) \mapsto rz \end{cases}$$

einen  $\mathbb{R}$ -Vektorraum, und die Abbildung

$$\mathbb{C} \rightarrow \mathbb{C}; \quad z \mapsto cz$$

ist für jede komplexe Zahl  $c = a + ib \in \mathbb{C}$  insbesondere eine lineare Abbildung von  $\mathbb{R}$ -Vektorräumen. Wählen wir  $\{1, i\}$  als  $\mathbb{R}$ -Basis von  $\mathbb{C}$ , so bildet sie die beiden Basisvektoren 1 und  $i$  ab auf

$$c \cdot 1 = a + bi \quad \text{und} \quad c \cdot i = ai + bi^2 = -b + ai;$$

sie hat also die Abbildungsmatrix

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

Die Hintereinanderausführung zweier solcher Abbildungen entspricht der Multiplikation der entsprechenden komplexen Zahlen; insbesondere

gehört also das Produkt  $(a + ib)(a' + ib')$  zweier komplexer Zahlen zur Produktmatrix

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} a' & -b' \\ b' & a' \end{pmatrix}.$$

Der Körper der komplexen Zahlen kann damit auch identifiziert werden mit der Menge aller reeller  $2 \times 2$ -Matrizen der obigen Form mit der Matrixaddition und dem Matrixprodukt. Man beachte, daß das Produkt zweier Matrizen dieser speziellen Form kommutativ ist, denn die Multiplikation komplexer Zahlen ist kommutativ.

Ganz entsprechend kann man auch die Elemente der Körper  $\mathbb{F}_{2^n}$  mit  $n \times n$ -Matrizen über  $\mathbb{F}_2$  identifizieren; nimmt man  $1, \alpha$  als Basisvektoren, entsprechen beispielsweise die vier Elemente  $0, 1, \alpha$  und  $\alpha + 1$  des Körpers  $\mathbb{F}_4$  den Matrizen

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \text{ und } \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix},$$

und für  $\mathbb{F}_{32}$  mit  $\mathbb{F}_2$ -Basis  $1, \alpha, \alpha^2, \alpha^3, \alpha^4$  und Relation  $\alpha^5 = \alpha^2 + 1$  entspricht  $\alpha$  der Matrix

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

#### d) Das Gaußsche Eliminationsverfahren

Die meisten kennen wohl aus der Schule zumindest Verfahren zur Lösung linearer Gleichungssysteme in bis zu drei Unbekannten, teilweise vielleicht auch für Systeme aus beliebig vielen Gleichungen in beliebig vielen Unbekannten.

Der GAUSS-Algorithmus, mit dem wir uns hier beschäftigen wollen, bestimmt die Lösungsmenge eines beliebigen linearen Gleichungssystems, und falls das Gleichungssystem nicht gerade eine spezielle Gestalt hat, liefert er sie im allgemeinen auf die effizienteste Art und Weise.

Die Grundidee seines Verfahrens zur Lösung linearer Gleichungssysteme ist sehr einfach: Im Falle einer einzigen Gleichung mit einer einzigen Unbekannten  $x$  können wir das „Gleichungssystem“

$$ax = b$$

sofort lösen: Für  $a \neq 0$  ist  $x = -b/a$ , d.h.  $\mathcal{L} = \{-b/a\}$ ; ansonsten gibt es für  $b \neq 0$  keine Lösung, d.h.  $\mathcal{L} = \emptyset$ , und für  $a = b = 0$  ist jedes  $x$  aus  $k$  eine Lösung, d.h.  $\mathcal{L} = k$ .

Das GAUSSsche Eliminationsverfahren führt ein allgemeines lineares Gleichungssystem sukzessive zurück auf solche lineare Gleichungen in einer Unbekannten, ausgehend von zwei trivialen Beobachtungen:

1. Die Lösungsmenge eines linearen Gleichungssystems ändert sich nicht, falls wir zwei Gleichungen miteinander vertauschen.
2. Die Lösungsmenge ändert sich auch dann nicht, wenn wir ein Vielfaches einer Gleichung zu einer anderen addieren, d.h. wenn wir die Gleichung

$$\ell_j(x_1, \dots, x_m) \stackrel{\text{def}}{=} a_{j1}x_1 + \dots + a_{jm}x_m = b_j$$

ersetzen durch

$$\ell_j(x_1, \dots, x_m) + \lambda \ell_i(x_1, \dots, x_m) = b_j + \lambda b_i, \quad (*)$$

denn unter der Nebenbedingung

$$\ell_i(x_1, \dots, x_m) = b_i$$

ist (\*) äquivalent zu  $\ell_j(x_1, \dots, x_m) = 0$ .

Mit Hilfe dieser beiden Beobachtungen läßt sich nun die Variablenanzahl wie folgt sukzessive reduzieren: Beginnen wir mit der Elimination von  $x_1$ . Falls  $x_1$  im Gleichungssystem überhaupt nicht vorkommt, falls also alle  $a_{i1} = 0$  sind, gibt es nichts zu tun: Wir haben ein Gleichungssystem in  $x_2, \dots, x_m$ , und für jede Lösung  $(x_2, \dots, x_m)$  dieses Systems sowie jedes beliebige  $x_1 \in k$  ist  $(x_1, x_2, \dots, x_m)$  eine Lösung des ursprünglichen Systems.

Ansonsten können wir, indem wir nötigenfalls zwei Gleichungen miteinander vertauschen, annehmen, daß  $a_{11} \neq 0$  ist. Dann lassen wir die



erste Gleichung so stehen, wie sie ist, und ersetzen jede weitere Gleichung  $\ell_j(x_1, \dots, x_m) = b_j$  durch

$$\ell_j(x_1, \dots, x_m) - \frac{a_{j1}}{a_{11}} \ell_1(x_1, \dots, x_m) = b_j - \frac{a_{j1}}{a_{11}} b_1;$$

in diesen Gleichungen kommt  $x_1$  offenbar nicht mehr vor. Wir haben somit ein Gleichungssystem in einer Variablen weniger, plus der Gleichung

$$a_{11}x_1 + a_{12}x_2 + \dots + a_{1m}x_m = b_1.$$

Sobald wir das Gleichungssystem für  $x_2, \dots, x_m$  gelöst haben, wird diese Gleichung nach Einsetzen einer Lösung  $(x_2, \dots, x_m)$  zu einer linearen Gleichung für  $x_1$ , die wir lösen können:

$$x_1 = \frac{b_1 - (a_{12}x_2 + \dots + a_{1m}x_m)}{a_{11}}.$$

Das Gleichungssystem für  $x_2, \dots, x_m$  wird nun, falls  $m > 2$  ist, nach genau derselben Methode weiterreduziert: Falls  $x_2$  in keiner der Gleichungen vorkommt, haben wir tatsächlich ein Gleichungssystem in  $x_3, \dots, x_m$ , andernfalls können wir durch Vertauschen zweier Gleichungen annehmen, daß  $x_2$  in der ersten Gleichung mit einem von Null verschiedenen Vorfaktor auftritt, und wir können wie oben  $x_2$  aus allen weiteren Gleichungen eliminieren usw.

Da in jedem Eliminationsschritt ein Nenner auftritt, können die Nenner vor allem bei großem  $m$  gelegentlich schnell unübersichtlich groß werden. Obwohl es *im Prinzip* nicht notwendig ist, kann man um dies zu vermeiden noch als dritte Operation die Multiplikation einer Gleichung mit einem Körperelement (z.B. einem Hauptnenner der Koeffizienten) zulassen. Dies ist gleichbedeutend damit, daß man anstelle der Operation (\*) allgemeiner die Ersetzung von  $\ell_j(x_1, \dots, x_m)$  durch

$$\mu \ell_j(x_1, \dots, x_m) + \lambda \ell_i(x_1, \dots, x_m)$$

mit beliebigem  $\mu \neq 0$  aus  $k$  zuläßt. ( $\mu = 0$  muß hier natürlich unbedingt ausgeschlossen werden, denn sonst läßt sich die Gleichung  $\ell_j(x_1, \dots, x_m) = 0$  aus dem neuen Gleichungssystem nicht mehr herleiten, d.h. wir erhalten auch „Lösungen“, die diese Gleichung nicht erfüllen.)



CARL FRIEDRICH GAUSS (1777–1855) leistete wesentliche Beiträge zur Zahlentheorie, zur nichteuklidischen Geometrie, zur Differentialgeometrie und Kartographie, zur Fehlerrechnung und Statistik, zur Astronomie und Geophysik usw. Als Direktor der Göttinger Sternwarte baute er zusammen mit dem Physiker Weber den ersten Telegraphen. Er leitete die erste Vermessung und Kartierung des Königreichs Hannover und zeitweise auch den Witwenfond der Universität Göttingen; seine hierbei gewonnene Erfahrung benutzte er für erfolgreiche Spekulationen mit Aktien. Sätze und Verfahren von Gauß werden uns im Laufe der Vorlesung noch häufig begegnen.

### e) Erste Beispiele

Betrachten wir dazu einige Beispiele; der Grundkörper  $k$  sei dabei jeweils der Körper der reellen Zahlen oder einer seiner Teilkörper, etwa  $k = \mathbb{Q}$ .

Sei zunächst

$$\begin{aligned} 3x_1 + 2x_2 + x_3 &= 5 \\ x_1 + 2x_2 + 4x_3 &= 3 \\ 5x_1 - 3x_2 + 7x_3 &= 19 \end{aligned}$$

das zu lösende Gleichungssystem. Da  $x_1$  in der ersten Gleichung tatsächlich vorkommt, müssen wir nichts vertauschen; allerdings müssen wir ein Drittel der ersten Gleichung von der zweiten und fünf Drittel der ersten Gleichung von der dritten subtrahieren, um  $x_2$  aus diesen beiden Gleichungen zu eliminieren, was auf das etwas unangenehme Gleichungssystem

$$\begin{aligned} 3x_1 + 2x_2 + x_3 &= 5 \\ \frac{4}{3}x_2 + \frac{11}{3}x_3 &= \frac{4}{3} \\ -\frac{19}{3}x_2 + \frac{16}{3}x_3 &= \frac{32}{3} \end{aligned}$$

führt. Solche Gleichungssysteme sind zwar nicht immer vermeidbar, aber hier hätten wir es auch einfacher haben können: Wenn wir im ursprünglichen Gleichungssystem die ersten beiden Gleichungen vertauschen, wird es zu

$$\begin{aligned} x_1 + 2x_2 + 4x_3 &= 3 \\ 3x_1 + 2x_2 + x_3 &= 5 \\ 5x_1 - 3x_2 + 7x_3 &= 19, \end{aligned}$$

und hier müssen wir stattdessen das Dreifache  $b_{2W}$ . Fünffache der ersten Gleichung von der zweiten  $b_{2W}$ , dritten subtrahieren, was auf das deutlich angenehmere Gleichungssystem

$$\begin{array}{r} x_1 + 2x_2 + 4x_3 = 3 \\ -4x_2 - 11x_3 = -4 \\ -13x_2 - 13x_3 = 4 \end{array}$$

führt. Etwas ähnliches hätten wir auch bekommen, wenn wir die letzten beiden Gleichungen des anderen Systems einfach mit drei multipliziert hätten, aber grundsätzlich ist es meistens günstiger, die Gleichung mit dem einfachsten führenden Koeffizienten an erster Stelle zu haben. Auch hier wird das Gleichungssystem zumindest optisch etwas angenehmer, wenn wir die zweite und die dritte Gleichung mit  $(-1)$  multiplizieren:

$$\begin{array}{r} x_1 + 2x_2 + 4x_3 = 3 \\ 4x_2 + 11x_3 = 4 \\ 13x_2 + 13x_3 = -4 \end{array}$$

Uns interessieren zunächst nur die letzten beiden Zeilen. Diese bilden ein lineares Gleichungssystem in  $x_2$  und  $x_3$ , aus dem wir  $x_2$  in einer der beiden Gleichungen eliminieren möchten.

Da  $x_2$  in der zweiten Gleichung wirklich vorkommt, subtrahieren wir  $13/4$  mal diese Gleichung von der dritten und erhalten als neues System

$$\begin{array}{r} 3x_1 + 2x_2 + x_3 = 5 \\ 4x_2 + 11x_3 = 4 \\ -\frac{91}{4}x_3 = -17. \end{array}$$

Hier ist die letzte Gleichung eine gewöhnliche lineare Gleichung für  $x_3$ , aus der wir sofort ablesen, daß

$$x_3 = \frac{68}{91}$$

ist. Dies setzen wir in die vorletzte Gleichung ein:

$$4x_2 + \frac{748}{91} = 4$$

ist eine lineare Gleichung für  $x_2$  mit Lösung

$$x_2 = -\frac{96}{91}.$$

Dies sowie  $x_3$  setzen wir schließlich in die erste Gleichung ein:

$$x_1 + \frac{80}{91} = 3$$

hat die Lösung

$$x_1 = \frac{193}{91},$$

so daß insgesamt

$$\left( \frac{193}{91}, \frac{96}{91}, \frac{68}{91} \right)$$

die (einzige) Lösung des Gleichungssystems ist.

Als nächstes Beispiel betrachten wir

$$\begin{array}{r} 5x_3 - 2x_6 = 3 \\ 4x_2 + 2x_4 - 3x_6 - 7x_7 = -2 \\ x_1 - 3x_4 + x_5 = 0 \end{array}$$

Hier kommt  $x_1$  in der ersten Gleichung nicht vor, wohl aber in der dritten. Wir vertauschen daher die erste Gleichung mit der dritten und erhalten

$$\begin{array}{r} x_1 - 3x_4 + x_5 = 0 \\ 4x_2 + 2x_4 - 3x_6 - 7x_7 = -2 \\ 5x_3 - 2x_6 = 3. \end{array}$$

In diesem Gleichungssystem kommt  $x_1$  nur in der ersten Gleichung vor,  $x_2$  nicht mehr hinter der zweiten und  $x_3$  (natürlich) nicht mehr hinter der dritten, wir haben also bereits die Treppengestalt erreicht.

Die dritte Gleichung  $5x_3 - 2x_6 = 3$  hat offensichtlich keine eindeutig bestimmte Lösung: Wir können entweder nach  $x_3$  oder nach  $x_6$  auflösen, so daß eine der beiden Unbekannten beliebig gewählt werden kann. Wählen wir etwa für  $x_6$  irgendein Element  $\alpha \in k$ , so wird

$$x_6 = \alpha, \quad x_3 = \frac{2}{5}\alpha + \frac{3}{5}.$$

Die zweite Gleichung wird nach Einsetzen von  $x_6 = \alpha$  zu

$$4x_2 + 2x_4 - 3\alpha - 7x_7 = -2,$$

also zu einer Beziehung zwischen  $x_2, x_4$  und  $x_7$ , denn  $\alpha$  ist ein bereits fest gewähltes und somit bekanntes Element des Grundkörpers  $k$ . Wieder

können wir eine der beiden Variablen willkürlich festlegen, etwa  $x_7$  auf ein  $\beta \in k$  setzen und  $x_4$  auf ein  $\gamma \in k$ ; wir erhalten

$$x_7 = \beta, \quad x_4 = \gamma, \quad x_2 = \frac{3}{4}\alpha + \frac{7}{4}\beta - \frac{\gamma}{2} - \frac{1}{2}.$$

In der ersten Gleichung schließlich müssen wir alle bereits berechneten oder festgelegten Unbekannten einsetzen und erhalten dann die Gleichung

$$x_1 - 3\gamma + x_5 = 0.$$

Hier können wir noch  $x_5 = \delta$  beliebig festlegen und erhalten dann für die letzte noch verbleibende Variable

$$x_1 = 3\gamma - \delta.$$

Insgesamt hängt die Lösung dieses Gleichungssystems also ab von vier willkürlich wählbaren Körperelementen  $\alpha, \beta, \gamma, \delta \in k$  oder, wie wir auch sagen werden, von vier *Parametern*. Die *Lösungsmenge*  $\mathcal{L}$  ist daher die Menge

$$\left\{ \left( 3\gamma - \delta, \frac{3}{4}\alpha + \frac{7}{4}\beta - \frac{\gamma}{2} - \frac{1}{2}, \frac{3}{5}\alpha + \frac{3}{5}\gamma, \gamma, \delta, \alpha, \beta \right) \mid \alpha, \beta, \gamma, \delta \in k \right\}.$$

Im ersten Beispiel brauchten wir von den beiden Operationen des GAUSS-Algorithmus nur den Eliminationsschritt, im zweiten nur den Vertauschungsschritt. Als nächstes betrachten wir ein Beispiel, in dem beide notwendig sind, das lineare Gleichungssystem

$$\begin{array}{r} x_2 \\ 2x_1 + 2x_2 \\ 6x_1 - 3x_2 + x_3 \\ 4x_1 + x_2 \\ 6x_1 - 6x_2 + x_3 \end{array} + \begin{array}{r} 5x_4 - 2x_5 + x_6 = 10 \\ -4x_4 - 6x_5 + 2x_6 = 12 \\ 5x_4 - 3x_6 = 15 \\ -3x_4 + x_6 = 0 \\ 10x_4 + 12x_5 - 6x_6 = -8 \end{array}$$

Hier kommt  $x_1$  ausgerechnet in der ersten Gleichung nicht vor, dafür aber in allen folgenden; wir müssen also die erste Gleichung mit einer der anderen vertauschen, etwa der zweiten:

$$\begin{array}{r} 2x_1 + 2x_2 \\ 6x_1 - 3x_2 + x_3 \\ 4x_1 - 7x_2 + x_3 \\ 2x_1 - 7x_2 + x_3 \end{array} + \begin{array}{r} -4x_4 - 6x_5 + 2x_6 = 12 \\ 5x_4 - 2x_5 + x_6 = 10 \\ 5x_4 - 3x_6 = 15 \\ -3x_4 + x_6 = 0 \\ 13x_4 + 12x_5 - 6x_6 = -8 \end{array}$$

Nun kommt  $x_1$  in der zweiten Gleichung nicht mehr vor; aus der dritten, vierten bzw. fünften Gleichung kann  $x_1$  eliminiert werden, indem man dreimal, zweimal bzw. einmal die erste Gleichung subtrahiert:

$$\begin{array}{r} 2x_1 + 2x_2 \\ x_2 \\ -9x_2 + x_3 \\ -3x_2 \\ -12x_2 + x_3 \end{array} + \begin{array}{r} -4x_4 - 6x_5 + 2x_6 = 12 \\ 5x_4 - 2x_5 + x_6 = 10 \\ 17x_4 + 18x_5 - 9x_6 = -21 \\ 5x_4 + 12x_5 - 3x_6 = -24 \\ 22x_4 + 30x_5 - 12x_6 = -44 \end{array}$$

Als nächstes muß  $x_2$  aus der dritten bis fünften Gleichung eliminiert werden; da  $x_2$  in der zweiten Gleichung mit Koeffizient eins vorkommt, müssen wir einfach jenes Vielfache der zweiten Gleichung subtrahieren, das dem jeweiligen  $x_2$ -Koeffizienten entspricht. Da hier alle diese Koeffizienten negativ sind, bedeutet dies, daß wir dasjenige Vielfache der zweiten Gleichung *addieren*, das dem Betrag des Koeffizienten entspricht:

$$\begin{array}{r} 2x_1 + 2x_2 \\ x_2 \\ x_3 \\ x_3 \\ x_3 \end{array} + \begin{array}{r} -4x_4 - 6x_5 + 2x_6 = 12 \\ 5x_4 - 2x_5 + x_6 = 10 \\ 62x_4 \\ 20x_4 + 6x_5 = 6 \\ 82x_4 + 6x_5 = 76. \end{array}$$

Hier muß  $x_3$  aus der letzten Gleichung eliminiert werden; dazu muß offenbar einfach die dritte Gleichung subtrahiert werden:

$$\begin{array}{r} 2x_1 + 2x_2 \\ x_2 \\ x_3 \\ x_3 \end{array} + \begin{array}{r} -4x_4 - 6x_5 + 2x_6 = 12 \\ 5x_4 - 2x_5 + x_6 = 10 \\ 62x_4 \\ 20x_4 + 6x_5 = 6 \\ 20x_4 + 6x_5 = 7. \end{array}$$

Eigentlich sollte man hier schon sehen, was los ist, aber wir rechnen zur Veranschaulichung des GAUSS-Algorithmus trotzdem stur weiter nach Schema F: Danach muß  $x_4$  aus der letzten Gleichung eliminiert werden durch Subtraktion der vorletzten:

$$\begin{array}{r} 2x_1 + 2x_2 \\ x_2 \\ x_3 \\ x_3 \end{array} + \begin{array}{r} -4x_4 - 6x_5 + 2x_6 = 12 \\ 5x_4 - 2x_5 + x_6 = 10 \\ 62x_4 \\ 20x_4 + 6x_5 \\ 0 = 1. \end{array}$$

Damit wird endgültig klar, daß jede Lösung  $(x_1, \dots, x_6)$  des gegebenen Gleichungssystems insbesondere auch die Gleichung  $0 = 1$  erfüllen muß, d.h. die Lösungsmenge ist leer.

Nachdem wir soviel Arbeit in dieses Beispiel investiert haben, sollten wir zumindest einen Teil der Rechnungen recyceln zu einem Beispiel, in dem es Lösungen gibt. Dazu muß nur die letzte der fünf ursprünglichen Gleichungen auf der rechten Seite leicht abgeändert werden: Wir betrachten nun das System

$$\begin{array}{rcccccccc} & x_2 & + & 5x_4 & - & 2x_5 & + & x_6 & = & 10 \\ 2x_1 & + & 2x_2 & & - & 4x_4 & - & 6x_5 & + & 2x_6 & = & 12 \\ 6x_1 & - & 3x_2 & + & x_3 & + & 5x_4 & & - & 3x_6 & = & 15 \\ 4x_1 & + & x_2 & & - & 3x_4 & & & + & x_6 & = & 0 \\ 6x_1 & - & 6x_2 & + & x_3 & + & 10x_4 & + & 12x_5 & - & x_6 & = & -9. \end{array}$$

Hierauf lassen sich genau dieselben Umformungen anwenden wie oben, anstelle des Systems mit fünfter Gleichung  $0 = 1$  führen diese nun aber auf

$$\begin{array}{rcccccccc} & 2x_1 & + & 2x_2 & & - & 4x_4 & - & 6x_5 & + & 2x_6 & = & 12 \\ & & & & & & x_2 & + & 5x_4 & - & 2x_5 & + & x_6 & = & 10 \\ & & & & & & & & x_3 & + & 62x_4 & & & = & 69 \\ & & & & & & & & & & 20x_4 & + & 6x_5 & & = & 6 \\ & & & & & & & & & & & & & & 0 & = & 0. \end{array}$$

Diese letzte Gleichung ist natürlich für jedes Tupel  $(x_1, \dots, x_6)$  erfüllt. Die vorletzte gibt eine Beziehung zwischen  $x_4$  und  $x_5$ , wir können also

$$x_5 = \alpha \in k$$

beliebig wählen und erhalten dann

$$x_4 = -\frac{3}{10}\alpha + \frac{3}{10}.$$

Wenn wir dies in die dritte Gleichung einsetzen, bleibt dort nur noch  $x_3$  als Variable stehen, und aus

$$x_3 - \frac{93}{5}\alpha + \frac{93}{5} = 69$$

lesen wir sofort ab, daß

$$x_3 = \frac{93}{5}\alpha + \frac{252}{5}$$

ist. Damit gehen wir in die zweite Gleichung:

$$x_2 - \frac{7}{5}\alpha + x_6 + \frac{3}{2} = 10.$$

Hier können wir wieder eine der beiden noch verbliebenen Variablen auf einen beliebigen Wert setzen, etwa

$$x_6 = \beta \in k.$$

Dann wird

$$x_2 = \frac{7}{2}\alpha - \beta + \frac{17}{2},$$

was wir schließlich zusammen mit all den anderen bereits berechneten  $x_i$  in die erste Gleichung einsetzen können:

$$2x_1 + \frac{11}{5}\alpha + \frac{79}{5} = 12$$

hat die Lösung

$$x_1 = -\frac{11}{10}\alpha - \frac{19}{10}.$$

Damit hängt also die allgemeine Lösung dieses linearen Gleichungssystems von zwei frei wählbaren Parametern  $\alpha$  und  $\beta$  ab. Sie wird geringfügig übersichtlicher, wenn wir  $\alpha$  als  $\alpha = 10\gamma$  schreiben; dann ist  $\mathcal{L}$  gleich der Menge

$$\left\{ \left( -11\gamma - \frac{19}{10}, 35\gamma - \beta + \frac{17}{2}, 186\gamma + \frac{22}{5}, -3\gamma + \frac{3}{10}, 10\gamma, \beta \right) \mid \beta, \gamma \in k \right\}.$$

Als nächstes Beispiel wollen wir ein System betrachten, daß von zwar festen, aber nicht numerisch gegebenen Parametern abhängt: Wir betrachten das Gleichstromnetzwerk aus Abbildung zwölf mit bekannten Widerständen  $R_1, \dots, R_5$  und bekanntem Eingangs- und Ausgangsstrom  $I$ ; gesucht sind die Ströme  $I_1, \dots, I_5$ .

Nach den KIRCHHOFFSchen Gesetzen müssen sich zunächst an allen Knoten die eingehenden und die ausgehenden Ströme zu Null ergänzen, d.h. wir erhalten die Gleichungen

$$I_1 + I_2 = I = I_4 + I_5$$

für Anfang und Ende sowie

$$I_2 = I_3 + I_4 \quad \text{und} \quad I_1 + I_3 = I_5$$

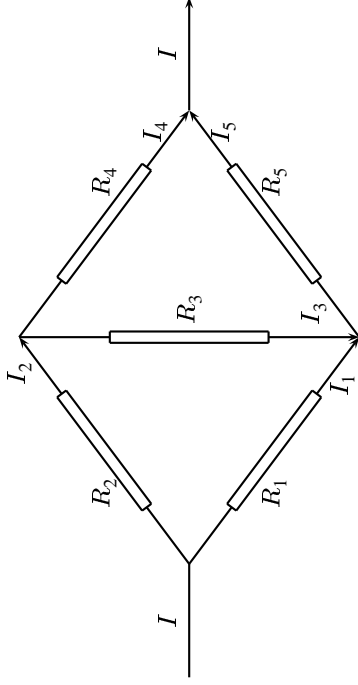


Abb. 12: Ein Gleichstromnetzwerk

für oben und unten. Außerdem müssen sich die Spannungen in den beiden Dreiecken zu Null summieren; nach dem OHMSchen Gesetz führt dies auf die beiden Gleichungen

$$R_2 I_2 + R_3 I_3 - R_1 I_1 = 0 \quad \text{und} \quad R_3 I_3 + R_5 I_5 - R_4 I_4 = 0.$$

Ordnen wir dies nach den Strömen  $I_i$ , erhalten wir also das lineare Gleichungssystem

$$\begin{aligned} I_1 + I_2 &= I \\ I_2 - I_3 + I_4 + I_5 &= I \\ -R_1 I_1 + R_2 I_2 + I_3 - I_4 &= 0 \\ -R_3 I_3 + R_3 I_3 + R_4 I_4 - R_5 I_5 &= 0. \end{aligned}$$

Die Elimination von  $I_1$  aus allen Gleichungen ab der zweiten ist einfach: Wir müssen die erste Gleichung von der vierten subtrahieren und ihr  $R_1$ -faches zur fünften addieren; das neue System ist

$$\begin{aligned} I_1 + I_2 &= I \\ I_2 - I_3 + I_4 + I_5 &= I \\ -I_2 + I_3 - I_4 &= 0 \\ (R_1 + R_2)I_2 + I_3 - I_4 - R_5 I_5 &= -R_1 I \\ -R_3 I_3 + R_4 I_4 - R_5 I_5 &= 0, \end{aligned}$$

Da  $I_2$  in der zweiten Gleichung nicht vorkommt, vertauschen wir diese mit der dritten; danach können wir letztere zur vierten addieren und ihr  $(R_1 + R_2)$ -faches von der fünften subtrahieren, um  $I_2$  aus allen weiteren Gleichungen zu eliminieren.

Damit weiterhin jede Gleichung in eine Zeile paßt, setzen wir zur Abkürzung

$$R_{12} \stackrel{\text{def}}{=} R_1 + R_2 \quad \text{und} \quad R_{123} \stackrel{\text{def}}{=} R_1 + R_2 + R_3$$

und erhalten

$$\begin{aligned} I_1 + I_2 - I_3 - I_4 + I_5 &= I \\ I_2 - I_3 - I_4 + I_5 &= 0 \\ R_{123} I_3 + R_{12} I_4 - R_3 I_5 &= R_1 I \\ -R_3 I_3 + R_4 I_4 - R_5 I_5 &= 0. \end{aligned}$$

Zur Elimination von  $I_3$  bietet sich an, die dritte Gleichung, in der  $I_3$  nicht vorkommt, mit der sechsten zu vertauschen (diese hat einen einfacheren  $I_3$ -Koeffizienten als die fünfte), und dann das  $R_{123}/R_3$ -fache dieser Gleichung zur fünften zu addieren. Dazu müssen wir uns allerdings zunächst überlegen, ob das überhaupt zulässig ist: Falls  $R_3 = 0$  ist, dürfen wir natürlich nicht durch  $R_3$  dividieren; wenn dieser Fall nicht ausgeschlossen werden kann, muß er also ab hier getrennt behandelt werden.

Im vorliegenden Beispiel wollen wir aber davon ausgehen, daß alle fünf Widerstände tatsächlich vorhanden sind, so daß alle  $R_i$  positive reelle Zahlen sind. Dann können wir durch  $R_3$  dividieren und das System wird zu

$$\begin{aligned} I_1 + I_2 - I_3 - I_4 + I_5 &= I \\ I_2 - I_3 - I_4 + I_5 &= 0 \\ -R_3 I_3 + R_4 I_4 - R_5 I_5 &= 0 \\ \alpha I_4 + \beta I_5 &= -I \\ I_4 + I_5 &= R_1 I \end{aligned}$$

mit

$$\alpha = R_{12} + \frac{R_4 R_{123}}{R_3} \quad \text{und} \quad \beta = \frac{-R_5 R_{123}}{R_3}.$$

Schließlich muß noch  $I_4$  aus den letzten beiden Gleichungen eliminiert werden; wir addieren also die vierte Gleichung unverändert zur letzten und ihr  $\alpha$ -faches zur vorletzten:

$$\begin{aligned} I_1 + I_2 &= I \\ I_2 - I_3 - I_4 &= 0 \\ -R_3 I_3 + R_4 I_4 - R_5 I_5 &= 0 \\ -I_4 + R_5 I_5 &= -I \\ (\beta - \alpha) I_5 &= (R_1 - \alpha) I \\ 0 &= 0 \end{aligned}$$

Damit können wir nacheinander

$$I_5 = \frac{R_1 - \alpha}{\beta - \alpha} \cdot I, \quad I_4 = I - I_5, \quad I_3 = \frac{R_4 I_4 - R_5 I_5}{R_3},$$

$$I_2 = I_3 + I_4 \quad \text{und} \quad I_1 = I - I_2$$

bestimmen, wobei sich der Leser noch überlegen sollte, warum die Division durch  $\beta - \alpha$  unproblematisch ist.

Zum Berechnen der Ströme in konkreten Beispielen reicht diese Lösungsformel aus; ist man allerdings an einem symbolischen Ausdruck interessiert, muß man die Definitionen von  $\alpha, \beta, R_{12}, R_{123}$  einsetzen und nacheinander alle rechte Seiten auf Ausdrücke nur in  $I$  und den  $R_i$  reduzieren. Dies ist eine *im Prinzip* einfache Übungsaufgabe in Bruchrechnung, die man allerdings im vorliegenden Fall besser einem Computersystem überläßt. Als Ergebnis erhält man die expliziten Formeln

$$\begin{aligned} I_1 &= \frac{(R_2 R_5 + R_2 R_3 + R_2 R_4 + R_3 R_4) \cdot I}{R_1 R_5 + R_2 R_5 + R_3 R_5 + R_1 R_3 + R_2 R_3 + R_1 R_4 + R_2 R_4 + R_3 R_4} \\ I_2 &= \frac{(R_1 R_4 + R_1 R_5 + R_3 R_5 + R_1 R_3) \cdot I}{R_1 R_5 + R_2 R_5 + R_3 R_5 + R_1 R_3 + R_2 R_3 + R_1 R_4 + R_2 R_4 + R_3 R_4} \\ I_3 &= \frac{(R_1 R_4 - R_2 R_5) \cdot I}{R_1 R_5 + R_2 R_5 + R_3 R_5 + R_1 R_3 + R_2 R_3 + R_1 R_4 + R_2 R_4 + R_3 R_4} \\ I_4 &= \frac{(R_1 R_3 + R_1 R_5 + R_2 R_5 + R_3 R_5) \cdot I}{R_1 R_5 + R_2 R_5 + R_3 R_5 + R_1 R_3 + R_2 R_3 + R_1 R_4 + R_2 R_4 + R_3 R_4} \\ I_5 &= \frac{(R_2 R_3 + R_1 R_4 + R_2 R_4 + R_3 R_4) \cdot I}{R_1 R_5 + R_2 R_5 + R_3 R_5 + R_1 R_3 + R_2 R_3 + R_1 R_4 + R_2 R_4 + R_3 R_4} \end{aligned}$$

die für die meisten *konkreten* Anwendungen erheblich weniger nützlich sind als die obige Form des Ergebnisses.

Als letztes Beispiel schließlich betrachten wir eines, das auch von einem Parameter abhängt, bei dem man aber *nicht* wie im obigen Beispiel einfach durch Ausdrücke im Parameter dividieren darf. (Eigentlich hätten wir es da auch nicht immer dürfen, aber wir haben einfach angenommen, daß alle Widerstände wirklich vorhanden und damit positiv sind; da Kurzschlüsse immer wieder vorkommen, ist diese Annahme nicht hundertprozentig realistisch.) Das Gleichungssystem hänge ab von einem Parameter  $a \in k$  und habe die Form

$$\begin{aligned} x_1 + ax_2 + x_3 &= 1 \\ x_1 + x_2 &= 1 \\ -2x_1 - 2ax_2 - ax_3 &= 1. \end{aligned}$$

Ein Computeralgebrasystem findet unschwer die Lösung

$$x_1 = \frac{a^2 - 3a - 1}{a^2 - 3a + 2}, \quad x_2 = \frac{3}{a^2 - 3a + 2}, \quad x_3 = \frac{-3}{a - 2}.$$

Diese „Lösung“ hat aber für  $a = 2$  und auch für  $a = 1$  Nullen im Nenner, ist dort also nicht erklärt. Für ein Computeralgebrasystem ist das kein Problem: Wie der Name sagt, rechnet es *algebraisch*, und da ist  $a$  keine reelle Zahl, sondern ein Symbol, das nichts mit irgendwelchen Zahlen zu tun hat. Damit ist  $a - 2$  ein formaler Ausdruck, der nie null sein kann, denn das *Symbol*  $a$  ist schließlich verschieden von der *Zahl* zwei.

Dieses Rechnen in sogenannten Funktionenkörpern ist mathematisch problemlos, ist aber nicht das, was in den meisten Anwendungen gefragt ist: Dort steht  $a$  im allgemeinen für eine variable Größe, in Abhängigkeit von der das Gleichungssystem gelöst werden soll. Man kann sich beispielsweise vorstellen, daß das Gleichungssystem ein lineares Regelungsproblem beschreibt in Abhängigkeit von steuerbaren Größen  $x_1, x_2$  und  $x_3$ , wobei die zu steuernden Größen zu

$$x_1 + ax_2 + x_3, \quad x_1 + x_2 \quad \text{und} \quad -2x_1 - 2ax_2 - ax_3$$

werden. Der Parameter  $a$  wäre dann zu interpretieren als eine von außen vorgegebene Umgebungsbedingung (z.B. die Temperatur), und das lineare Gleichungssystem besagt, daß wir das System so regeln wollen,

daß die drei steuerbaren Größen allesamt eins werden – unabhängig von der Außentemperatur.

Bei einer solchen Interpretation können wir natürlich *nicht* einfach durch  $a - 2$  dividieren; ein Ergebnis, wie  $x_3 = -3/(a - 2)$  besagt in so einem Fall, daß das Ziel im Falle  $a = 2$  nicht erreichbar ist, und das ist ein sehr wichtiges Ergebnis. Bei einem System, das einen Stromkreis beschreibt, könnte das zum Beispiel bedeuten, daß beim Parameterwert  $a = 2$  ein Kurzschluß entsteht, so daß dieser Parameterwert unbedingt verhindert werden muß. Deshalb muß man bei einem Gleichungssystem, das ein reales Problem beschreibt, vor jeder Division durch einen parameterabhängigen Ausdruck garantieren, daß dieser Ausdruck von null verschieden ist, und man muß die Fälle, in denen er null wird, gesondert diskutieren.

Im vorliegenden Beispiel (einer Vordiplomaufgabe vom April 1999) führt dies auf folgende Lösung:

Subtraktion der ersten Gleichung von der zweiten sowie Addition der zweifachen ersten Gleichung zur dritten ergibt

$$\begin{aligned}(a - 1)x_2 + x_3 &= 0 \\ (2 - a)x_3 &= 3.\end{aligned}$$

Für  $a = 2$  ist die letzte dieser beiden Gleichungen unlösbar, ansonsten ist

$$x_3 = \frac{3}{2 - a} \quad \text{falls } a \neq 2.$$

Für  $a = 1$  wird die vorletzte Gleichung zu  $x_3 = 0$ , was der schon gefundenen Lösung

$$x_3 = \frac{3}{2 - a} = 1$$

widerspricht; auch dann ist also das Gleichungssystem unlösbar. In allen anderen Fällen erhalten wir

$$x_2 = \frac{3}{(a - 1)(a - 2)} \quad \text{falls } a \neq 1, 2.$$

Schließlich läßt sich noch, beispielsweise aus der zweiten Gleichung des ursprünglichen Systems,  $x_1$  berechnen und wir erhalten als Ergebnis:

Die Lösungsmenge ist

$$\mathcal{L} = \left\{ \left( 1 - \frac{3}{(a-1)(a-2)}, \frac{3}{(a-1)(a-2)}, \frac{3}{a-2} \right) \right\},$$

falls  $a \neq 1, 2$ , und

$$\mathcal{L} = \emptyset, \quad \text{falls } a = 1 \text{ oder } a = 2$$

ist.

In einem solchen Fall wird man durch die Nullstellen des Nenners gewarnt, daß hier etwas schiefgehen muß; es gibt aber auch Beispiele, in denen ein Computeralgebrasystem Lösungen schlichtweg „übersieht“: Betrachten wir etwa das lineare Gleichungssystem

$$\begin{aligned}x_1 + 2x_3 &= 9 \\ 2x_1 + 3x_2 + x_3 &= 9 \\ -x_2 + ax_3 &= a + 2.\end{aligned}$$

Ein Computer findet leicht die Lösung

$$x = 7, \quad y = -2 \quad \text{und} \quad z = 1.$$

Der GAUSSalgorithmus führt uns aber über das Gleichungssystem

$$\begin{aligned}x_1 + 2x_3 &= 9 \\ 3x_2 - 3x_3 &= -9 \\ -x_2 + ax_3 &= a + 2\end{aligned}$$

oder

$$\begin{aligned}x_1 + 2x_3 &= 9 \\ x_2 - x_3 &= -3 \\ -x_2 + ax_3 &= a + 2\end{aligned}$$

auf die Endgestalt

$$\begin{aligned}x_1 + 2x_3 &= 9 \\ x_2 - x_3 &= -3 \\ (a - 1)x_3 &= a - 1,\end{aligned}$$

in der man nur für  $a \neq 1$  aus der letzten Gleichung schließen darf, daß  $z = 1$  ist; für  $a = 1$  haben wir die immer erfüllte Gleichung  $0z = 0$ . Die Lösungsmenge ist hier also

$$\mathcal{L} = \{(7, -2, 1)\} \quad \text{für } a \neq 1$$