Vorlesung "Mathematische Strukturen"

Sommersemester 2015

Prof. Barbara König
Übungsleitung: Dennis Nolte

Monoide, Gruppen, Körper

Wir betrachten nun grundlegende "Rechenstrukturen". Das sind Strukturen, mit denen man rechnen kann wie mit (natürlichen/rationalen/reellen) Zahlen, die aber möglicherweise andere Elemente enthalten.

Dabei beantworten u.a. wir folgende Fragen:

- Welche (gemeinsamen) Eigenschaften haben Addition und Multiplikation?
- Wie unterscheiden sich $\mathbb{N}_0$ und $\mathbb{Z}$?
- Kann man auch mit endlichen Mengen von Objekten rechnen?
- Was sind mögliche Anwendungen in der Kryptographie?

Monoide, Gruppen, Körper

Monoid

Gegen sei eine Menge M und eine zweistellige Abbildung $\circ\colon M \times M \to M$. Wir benutzen meist die Infix-Schreibweise: $\circ((m_1, m_2)) = m_1 \circ m_2$ und bezeichnen $\circ$ als zweistelligen Operator.

$(M, \circ)$ heißt Monoid, falls folgendes gilt:

- $\circ$ ist assoziativ, d.h., es gilt $m_1 \circ (m_2 \circ m_3) = (m_1 \circ m_2) \circ m_3$ für alle $m_1, m_2, m_3 \in M$.
- Es gibt ein neutrales Element $e \in M$, für das gilt: $e \circ m = m \circ e = m$ für alle $m \in M$.

Monoide, Gruppen, Körper

(Gegen-)Beispiele für Monoide

- $(\mathbb{N}_0, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ sind Monoide
  (neutrales Element: 0)
- $(\mathbb{N}_0, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$ sind Monoide
  (neutrales Element: 1)
- $(\mathbb{Z}, -)$ ist kein Monoid
  (fehlende Assoziativität)

Monoide, Gruppen, Körper

Modulo-Rechnen

Wir definieren $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ mit folgender Addition $+_n$ und Multiplikation $\cdot_n$. Seien $k, \ell \in \mathbb{Z}_n$, dann gilt:

$$k +_n \ell = (k + \ell) \bmod n \qquad k \cdot_n \ell = (k \cdot \ell) \bmod n$$

$(\mathbb{Z}_n, +_n)$ und $(\mathbb{Z}_n, \cdot_n)$ sind Monoide
(mit neutralen Elementen 0 bzw. 1)

Sie spielen eine große Rolle u.a. in der Kryptographie und Kodierungstheorie.

Monoide, Gruppen, Körper

Bemerkungen:

Bei Modulo-Rechnungen kann man Addition/Multiplikation und Modulo-Rechnung beliebig tauschen. Es gilt nämlich:

Modulo-Gesetze

- $(a + b) \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n$
- $(a \cdot b) \bmod n = ((a \bmod n) \cdot (b \bmod n)) \bmod n$
- $a^k \bmod n = (a \bmod n)^k \bmod n$

Statt $(x \bmod n) = (a \bmod n)$ schreibt man oft auch:

$$x \equiv a \pmod{n}.$$

Monoide, Gruppen, Körper

Additions-/Multiplikationstabellen für $\mathbb{Z}_5$:

$+_n$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot_n$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Monoide, Gruppen, Körper

In vielen Fällen (z.B. zum Lösen von Gleichungssystemen) benötigt man beim Rechnen etwas mehr Struktur: man braucht sogenannte Inverse.

Gruppe

Ein Monoid $(G, \circ)$ mit neutralem Element e heißt Gruppe, wenn zusätzlich zu den Monoid-Eigenschaften noch folgendes gilt:

- für jedes $g \in G$ gibt es ein $g^{-1} \in G$ mit $g \circ g^{-1} = e$.

Dabei heißt g^{-1} das Inverse von g.

$(G, \circ)$ heißt kommutative Gruppe (oder abelsche Gruppe), falls außerdem $g_1 \circ g_2 = g_2 \circ g_1$ für alle $g_1, g_2 \in G$ gilt.

Bemerkung: In jeder Gruppe gilt nicht nur $g \circ g^{-1} = e$, sondern auch $g^{-1} \circ g = e$ für alle $g \in G$.

Monoide, Gruppen, Körper

(Gegen-)Beispiele für Gruppen

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ sind Gruppen
  (Inverses zu x ist $-x$)
- $(\mathbb{N}_0, +)$ ist keine Gruppe
  (fehlende Inverse)
- $(\mathbb{Q}\backslash\{0\}, \cdot)$, $(\mathbb{R}\backslash\{0\}, \cdot)$ sind Gruppen
  (Inverses zu x ist $\frac{1}{x}$)
- $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$ sind keine Gruppen
  (0 hat kein Inverses)
- $(\mathbb{Z}, \cdot)$, $(\mathbb{Z}\backslash\{0\}, \cdot)$ sind keine Gruppen
  (fehlende Inverse)

Monoide, Gruppen, Körper

(Gegen-)Beispiele für Gruppen (Fortsetzung)

- $(\mathbb{Z}_n, +_n)$ ist eine Gruppe
- $(\mathbb{Z}_n, \cdot_n)$ ist keine Gruppe
  (0 hat kein Inverses)
- $(\mathbb{Z}_n \backslash \{0\}, \cdot_n)$ ist genau dann eine Gruppe, wenn n eine Primzahl ist.
  (Ein Element $m \in \mathbb{Z}_n$ hat genau dann ein Inverses, wenn m, n teilerfremd sind.)

Monoide, Gruppen, Körper

Am Beispiel $\mathbb{Z}_4$ ($n = 4$):

Es gilt $n = 4 = 2 \cdot 2$, d.h., 4 ist keine Primzahl.

$m = 2$ hat kein multiplikatives Inverses in $\mathbb{Z}_4$, denn $ggT(2, 4) = 2 \neq 1$.

Insbesondere hat die Gleichung $2 \cdot_4 x = (2 \cdot x) \bmod 4 = 1$ keine Lösung: $2 \cdot x$ ist für alle $x \in \mathbb{Z}$ eine gerade Zahl und $(2 \cdot x) \bmod 4$ ist daher ebenfalls eine gerade Zahl. D.h., man kann niemals das Ergebnis 1 erhalten.

Die Zahlen 1 und 3 sind allerdings teilerfremd zu n und besitzen multiplikative Inverse in $\mathbb{Z}_4$.

Monoide, Gruppen, Körper

Inversenbildung in $(\mathbb{Z}_n, +_n)$

Das Inverse zu $m \in \mathbb{Z}_n$ bezüglich der Addition $+_n$ ist $-_n m = (-m) \bmod n = (n - m) \bmod n$. Es gilt:

$$m +_n (-_n m) = (m + (-m)) \bmod n = 0 \bmod n = 0$$

Monoide, Gruppen, Körper

Für die Bildung von multiplikativen Inversen in $\mathbb{Z}_n$ benötigen wir folgenden Satz:

Satz von Euler-Fermat

Für teilerfremde Zahlen $m, n \in \mathbb{N}_0$ mit $n > 1$ gilt:

$$m^{\varphi(n)} \bmod n = 1$$

▸ Eulersche φ-Funktion

Monoide, Gruppen, Körper

Inversenbildung in $(\mathbb{Z}_n, \cdot_n)$ (Methode 1)

Mit dem Satz von Euler-Fermat:

$$m^{-1} = m^{\varphi(n)-1} \bmod n$$

Denn es gilt

$$m \cdot_n m^{-1} = (m \cdot m^{\varphi(n)-1}) \bmod n = m^{\varphi(n)} \bmod n = 1$$

Bemerkung: Inversenbildung funktioniert nur dann, wenn m, n teilerfremd sind. (Ansonsten hat m kein multiplikatives Inverses.) Diese Bedingung ist immer erfüllt, falls $m \neq 0$ und n eine Primzahl ist.

Monoide, Gruppen, Körper

Beispiel: Wir berechnen das multiplikative Inverse von 3 in $\mathbb{Z}_5$.

$3^{-1} = 3^{\varphi(5)-1} \bmod 5 = 3^3 \bmod 5 = 27 \bmod 5 = 2$

Test: $3 \cdot_5 2 = (3 \cdot 2) \bmod 5 = 6 \bmod 5 = 1$.

Monoide, Gruppen, Körper

Inversenbildung in $(\mathbb{Z}_n, \cdot_n)$ (Methode 2)

Das Inverse zu $m \in \mathbb{Z}_n$ bezüglich der Multiplikation $\cdot_n$ kann auch folgendermaßen bestimmt werden:

- Diophantische Gleichung $m \cdot x + n \cdot y = 1$ lösen.
- Bestimme Inverses $m^{-1} = x \bmod n$.

Denn es gilt:

$$m \cdot_n m^{-1} = m \cdot_n (x \bmod n) = (m \cdot x) \bmod n = (1 - n \cdot y) \bmod n = 1$$

Diese Methode funktioniert auch dann, wenn der Wert $\varphi(n)$ nicht einfach berechnet werden kann (z.B. wenn n sehr groß ist).

Monoide, Gruppen, Körper

Beispiel: Wir berechnen wieder das multiplikative Inverses von 3 in $\mathbb{Z}_5$.

Löse $3 \cdot x + 5 \cdot y = 1$:

$$ggT(3,5) = ggT(5,3) = ggT(2,3) = ggT(3,2) = ggT(1,2)$$
$$= ggT(2,1) = ggT(1,1) = ggT(0,1) = 1$$

Rückwärts einsetzen: $1 = 3 - 2 = 3 - (5 - 3) = 3 \cdot 2 + 5 \cdot (-1)$

Wir erhalten die Lösungen $x = 2$, $y = -1$

Bestimme $m^{-1} = x \bmod n = 2 \bmod 5 = 2$.

Monoide, Gruppen, Körper

Tabelle der Inversen in $(\mathbb{Z}_5 \setminus \{0\}, \cdot_5)$:

m	1	2	3	4
m^{-1}	1	3	2	4

Monoide, Gruppen, Körper

Nun betrachten wir noch eine Rechenstruktur, die zwei (miteinander kompatible) Operationen (normalerweise $+$ und $\cdot$) vereint.

Körper

Sei $(K, +, \cdot)$ ein Tupel, das aus einer Menge K und zwei zweistelligen Operationen $+$ und $\cdot$ auf K besteht.

$(K, +, \cdot)$ heißt Körper, falls folgendes gilt:

- $(K, +)$ ist eine kommutative Gruppe mit neutralem Element 0.
- $(K \backslash \{0\}, \cdot)$ ist eine kommutative Gruppe mit neutralem Element 1.
- Das Distributivgesetz gilt: das heißt, für alle $a, b, c \in K$ gilt: $a \cdot (b + c) = a \cdot b + a \cdot c$.

Monoide, Gruppen, Körper

Körperaxiome (Zusammenfassung, Teil 1)

Für einen Körper $(K, +, \cdot)$ muss gelten:

- $+ \colon K \times K \to K$ und $\cdot \colon K \times K \to K$ sind zweistellige Operationen auf K.
- $+$ und $\cdot$ sind assoziativ, d.h., es gilt für alle $x, y, z \in K$:

$$(x + y) + z = x + (y + z) \quad \text{und} \quad (x \cdot y) \cdot z = x \cdot (y \cdot z)$$

- $+$ hat ein neutrales Element, welches mit 0 bezeichnet wird und $\cdot$ hat ein neutrales Element, welches mit 1 bezeichnet wird.

Monoide, Gruppen, Körper

Körperaxiome (Zusammenfassung, Teil 2)

- Jedes Element hat ein additives Inverses und jedes Element, außer 0, hat ein multiplikatives Inverses.
- $+$ und $\cdot$ sind kommutativ, d.h., es gilt für alle $x, y \in K$:

$$x + y = y + x \qquad \text{und} \qquad x \cdot y = y \cdot x$$

- Es gilt das Distributivgesetz, d.h., für alle $x, y, z \in K$ gilt

$$x \cdot (y + z) = x \cdot y + x \cdot z \quad \text{und} \quad (x + y) \cdot z = x \cdot z + y \cdot z$$

(Das zweite Distributivgesetz folgt aus dem ersten aufgrund der Kommutativität von $\cdot$.)

Monoide, Gruppen, Körper

(Gegen-)Beispiele für Körper

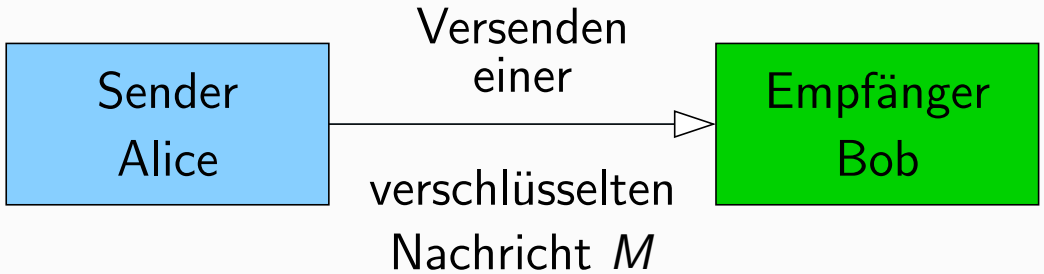
- $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ sind Körper
- $(\mathbb{Z}_n, +_n, \cdot_n)$ ist ein Körper, falls n eine Primzahl ist

Weitere Beispiele für Körper (auf die wir nicht mehr weiter eingehen): komplexe Zahlen, endliche Körper (mit $4, 8, 9, \ldots$ Elementen), ...

Anwendungsbeispiel: RSA

Wir betrachten eine Anwendung im Bereich der asymmetrischen Verschlüsselung (public-key cryptography).

Das sogenannte RSA-Verfahren (benannt nach Rivest, Shamir, Adleman) ist die Grundlage von wichtigen Kommunikationsprotokollen im Internet. Außerdem bildet es die Basis von elektronischen Signaturen.



- Alice will eine Nachricht M an Bob verschicken.
- Alice verwendet den öffentlichen Schlüssel von Bob zum Verschlüsseln.
- Bob verwendet seinen privaten Schlüssel zum Entschlüsseln.

Anwendungsbeispiel: RSA

1. Schritt: Schlüsselerzeugung

- Bob generiert zwei große Primzahlen p, q mit $p \neq q$ und setzt $n = p \cdot q$.
- Bob bestimmt $\varphi(n)$
  (in diesem Fall gilt $\varphi(n) = (p-1) \cdot (q-1)$).
- Bob bestimmt d, e mit $(d \cdot e) \bmod \varphi(n) = 1$
  (d.h., d, e sind in $\mathbb{Z}_{\varphi(n)}$ zueinander multiplikativ invers)
- (e, n) ist der öffentliche Schlüssel, den Bob bekanntgibt.
- (d, n) ist der private Schlüssel, den Bob geheimhält.

Anwendungsbeispiel: RSA

2. Schritt: Verschlüsselung

- Alice will eine Nachricht M an Bob verschlüsseln. Sie kodiert diese Nachricht als eine Zahl $m \in \mathbb{Z}_n$ (z.B. durch Binärkodierung).
- Alice rechnet $c = m^e \bmod n$ und schickt c an Bob.

Hier wird also in $\mathbb{Z}_n$ gerechnet.

3. Schritt: Entschlüsselung

- Bob empfängt c.
- Er rechnet $m = c^d \bmod n$ und erhält damit wieder die ursprüngliche Nachricht.

Wie bei der Verschlüsselung wird hier wieder in $\mathbb{Z}_n$ gerechnet.

Anwendungsbeispiel: RSA

Rechenbeispiel RSA

- $p = 5$, $q = 11$, $n = 5 \cdot 11 = 55$
- $\varphi(n) = (p-1) \cdot (q-1) = 4 \cdot 10 = 40$
- Wähle $e = 3$ und berechne das Inverse (Methode 2):
  - Löse $3 \cdot x + 40 \cdot y = 1$, ergibt Lösungen $x = -13$, $y = 1$
  - Setze $d = x \bmod 40 = (-13) \bmod 40 = 27$
- Nachricht $m = 9$ soll übertragen werden. Alice berechnet die Kodierung $c = 9^3 \bmod 55 = 729 \bmod 55 = 14$.
- Code $c = 14$ kommt an. Bob rechnet

$$
\begin{aligned}
& 14^{27} \bmod 55 = (14^3 \bmod 55)^9 \bmod 55 \\
&= (2744 \bmod 55)^9 \bmod 55 = 49^9 \bmod 55 \\
&= (49^3 \bmod 55)^3 \bmod 55 = (117649 \bmod 55)^3 \bmod 55 \\
&= 4^3 \bmod 55 = 64 \bmod 55 = 9 = m
\end{aligned}
$$

Anwendungsbeispiel: RSA

Warum funktioniert RSA?

Korrektheit: Warum erhält Bob wieder die ursprüngliche Nachricht?

Das kann mit dem Satz von Euler-Fermat nachgewiesen werden.

Es gilt $(e \cdot d \bmod \varphi(n)) = 1$ und damit gibt es eine Zahl z mit $e \cdot d = z \cdot \varphi(n) + 1$. Also entsteht beim Verschlüsseln und anschließenden Entschlüsseln:

$$(m^e \bmod n)^d \bmod n = m^{e \cdot d} \bmod n = m^{z \cdot \varphi(n)+1} \bmod n$$
$$= (m \cdot (m^{\varphi(n)})^z) \bmod n = m \cdot 1^z \bmod n = m \bmod n = m$$

Diese Argumentation funktioniert nicht, falls m, n nicht teilerfremd sind. In diesem Fall kann man aber anders nachweisen, dass man trotzdem das richtige Ergebnis erhält.

Anwendungsbeispiel: RSA

Warum funktioniert RSA? (Fortsetzung)

Sicherheit: Warum ist es für andere Teilnehmer (außer Bob) schwierig, die Nachricht zu entschlüsseln?

Das liegt daran, dass man d nur dann leicht aus e berechnen kann, wenn man $\varphi(n)$ kennt. Um $\varphi(n)$ zu berechnen, müsste man die Primfaktorzerlegung von großen Zahlen n (ca. 1024–2048 Bits) bestimmen, was sehr schwer ist.

Vektorräume und Matrizen

Wir betrachten nun Vektoren, die Tupel von Elementen eines Körpers sind. Mengen von Vektoren bilden einen sogenannten Vektorraum.

Vektoren sind wichtig für die Darstellung geometrischer Objekte. Matrizen werden dazu verwendet, um (lineare) Funktionen in Vektorräumen zu beschreiben. Sie spielen auch eine wichtige Rolle beim Lösen von Gleichungssystemen.

Vektorräume und Matrizen

Vektor

Sei $n \in \mathbb{N}_0$ eine natürliche Zahl und $(K, +, \cdot)$ ein Körper. Ein Vektor $\vec{u}$ der Dimension n über K besteht aus n Elementen $u_1, \ldots, u_n \in K$ des Körpers.

Ein Vektor wird im allgemeinen folgendermaßen dargestellt und heißt daher auch Spaltenvektor.

$$\vec{u} = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}$$

Vektorräume und Matrizen

Vektorraum

Die Menge aller Vektoren der Dimension n über K heißt n-dimensionaler Vektorraum über K und wird mit K^n bezeichnet.

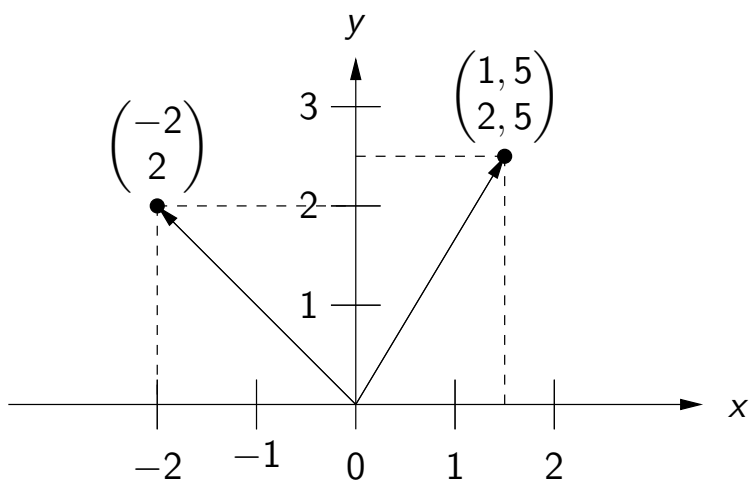
Hinweis: es gibt noch allgemeinere Definitionen eines Vektorraums (ähnlich zu den Definitionen von Monoid, Gruppe, Körper), die wir hier aber nicht betrachten.

Die Operationen auf einem Vektorraum sind Addition von Vektoren und Skalarmultiplikation, die im Folgenden betrachtet werden.

Vektorräume und Matrizen

Klassisches Beispiel: Sei $n = 2$ und $K = \mathbb{R}$, d.h., wir betrachten den Vektorraum $\mathbb{R}^2$.

Dann handelt es sich bei den Vektoren um Punkte im zweidimensionalen Raum. Diese werden auch durch Pfeile – ausgehend vom Ursprung des Koordinatensystems – dargestellt.



Die erste Koordinate bezeichnet man dabei – wie üblich – als x-Koordinate, die zweite als y-Koordinate.

Vektorräume und Matrizen

In Vektorräumen sind verschiedene Operationen definiert:

Addition von Vektoren

Die Addition auf Vektoren ist eine zweistelligen Operation $+ \colon K^n \times K^n \to K^n$, die folgendermaßen definiert ist:

$$\begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} + \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} u_1 + v_1 \\ \vdots \\ u_n + v_n \end{pmatrix}$$

Dabei werden die einzelnen Körperelemente mit Hilfe der $+$-Operation des Körpers verknüpft.

Vektorräume und Matrizen

Vektorraum als Gruppe

Ein Vektorraum mit der Addition ist eine kommutative Gruppe. Das neutrale Element ist der Nullvektor $\vec{0}$ und das additive Inverse zu $\vec{u}$ wird mit $-\vec{u}$ bezeichnet:

$$\vec{0} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \qquad \text{Falls } \vec{u} = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}, \text{ dann ist } -\vec{u} = \begin{pmatrix} -u_1 \\ \vdots \\ -u_n \end{pmatrix}.$$

Dabei sind $-u_1, \ldots, -u_n$ die additiven Inversen im Körper.

Vektorräume und Matrizen

Multiplikation mit einem Skalar

Ein Vektor $\vec{u} \in K^n$ kann mit einem einzelnen Körperelement $k \in K$ multipliziert werden. Das Element k nennt man dann auch Skalar.

$$k \cdot \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} = \begin{pmatrix} k \cdot u_1 \\ \vdots \\ k \cdot u_n \end{pmatrix}$$

Dabei entstehen $k \cdot u_1, \ldots, k \cdot u_n$ durch die Multiplikationsoperation im Körper.

Vektorräume und Matrizen

Eigenschaften der Multiplikation mit einem Skalar

Seien $\vec{u}, \vec{v} \in K^n$ Vektoren und $k, \ell \in K$ Skalare. Dann gilt:

$$\begin{aligned} k \cdot (\ell \cdot \vec{u}) &= (k \cdot \ell) \cdot \vec{u} \\ k \cdot (\vec{u} + \vec{v}) &= k \cdot \vec{u} + k \cdot \vec{v} \\ (k + \ell) \cdot \vec{u} &= k \cdot \vec{u} + \ell \cdot \vec{u} \\ 1 \cdot \vec{u} &= \vec{u} \end{aligned}$$

Dabei ist 1 das neutrale Element der Multiplikation im Körper.

Vektorräume und Matrizen

Wir betrachten nun bestimmte Abbildungen auf Vektorräumen: sogenannte lineare Abbildungen.

Lineare Abbildung

Seien K^n, K^m zwei Vektorräume. Eine Funktion $\psi\colon K^n \to K^m$ heißt lineare Abbildung, falls folgendes gilt:

$$\psi(\vec{u}+\vec{v}) = \psi(\vec{u}) + \psi(\vec{v}) \qquad \text{für alle } \vec{u}, \vec{v} \in K^n$$
$$\psi(k \cdot \vec{u}) = k \cdot \psi(\vec{u}) \qquad \text{für alle } \vec{u} \in K^n, k \in K$$

Die Multiplikation mit einem Skalar ist eine lineare Abbildung.

Auch viele der interessanten Abbildungen in der Geometrie sind linear (z.B. Drehungen, Spiegelungen).

Vektorräume und Matrizen

Wir betrachten nun Matrizen, mit denen solche linearen Abbildungen beschrieben werden können:

Matrix

Seien $m, n \in \mathbb{N}_0$ und K ein Körper. Eine $m \times n$-Matrix A über K besteht aus $m \cdot n$ Einträgen

$$A_{i,j} \in K \qquad \text{für } i \in \{1, \ldots, m\},\ j \in \{1, \ldots, n\}$$

Sie wird folgendermaßen dargestellt:

$$A = \begin{pmatrix} A_{1,1} & \cdots & A_{1,n} \\ \vdots & \ddots & \vdots \\ A_{m,1} & \cdots & A_{m,n} \end{pmatrix}$$

Vektorräume und Matrizen

Bemerkungen:

Eine $m \times n$-Matrix besteht also aus m Zeilen der Länge n, oder – anders ausgedrückt – aus n Spalten der Länge m.

Dabei heißt m Zeilendimension und n Spaltendimension der Matrix.

Bei einem Eintrag $A_{i,j}$ bezeichnet der erste Index i die Zeile, der zweite Index j die Spalte.

Eine Matrix, für die $m = n$ gilt, heißt quadratisch.

Vektorräume und Matrizen

Matrizen können mit Vektoren muliplizierт werden.

Multiplikation einer Matrix mit einem Vektor

Sei A eine $m \times n$-Matrix und $\vec{u} \in K^n$ ein Vektor der Dimension n. Dann ist $A \cdot \vec{u}$ folgender Vektor aus K^m:

$$A \cdot \vec{u} = \begin{pmatrix} A_{1,1} & \dots & A_{1,n} \\ \vdots & \ddots & \vdots \\ A_{m,1} & \dots & A_{m,n} \end{pmatrix} \cdot \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} = \begin{pmatrix} A_{1,1} \cdot u_1 + \dots + A_{1,n} \cdot u_n \\ \dots \\ A_{m,1} \cdot u_1 + \dots + A_{m,n} \cdot u_n \end{pmatrix}$$

Das heißt, in der i-ten Zeile des Spaltenvektors steht der Eintrag

$$\sum_{j=1}^{n} A_{i,j} \cdot u_j$$

Vektorräume und Matrizen

Bemerkung:

Wir verwenden das Summenzeichen Σ als abkürzende Schreibweise:

$$\sum_{j=1}^{n} a_j = a_1 + a_2 + \cdots + a_n$$

Rechenregeln für Summen

$$\sum_{j=1}^{n} (a_j + b_j) = \sum_{j=1}^{n} a_j + \sum_{j=1}^{n} b_j$$

$$\sum_{j=1}^{n} (k \cdot a_j) = k \cdot \sum_{j=1}^{n} a_j$$

Vektorräume und Matrizen

Beispiel: Multiplikation von Matrix und Vektor in $\mathbb{R}$

Multiplikation einer 2×3-Matrix mit einem Vektor der Dimension 3:

$$\begin{pmatrix} 3 & 4 & -1 \\ -2 & 2 & -3 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0,5 \\ -2 \end{pmatrix} = \begin{pmatrix} 3+2+2 \\ -2+1+6 \end{pmatrix} = \begin{pmatrix} 7 \\ 5 \end{pmatrix}$$

Vektorräume und Matrizen

Merkregel:

- Die Multiplikation einer $m \times n$-Matrix mit einem Vektor der Dimension n ergibt einen Vektor der Dimension m.
- Multipliziere die Zeilen der Matrix nacheinander mit der Spalte des Vektors (und addiere jeweils die Multiplikationsergebnisse auf).

Vektorräume und Matrizen

Matrix als lineare Abbildung

Eine $m \times n$-Matrix A über K beschreibt eine lineare Abbildung $\psi_A \colon K^n \to K^m$ wie folgt:

$$\psi_A(\vec{u}) = A \cdot \vec{u}$$

Durch Nachrechnen stellt man fest, dass tatsächlich die Eigenschaften einer linearen Abbildung erfüllt sind. Insbesondere gilt für eine Matrix A, Vektoren $\vec{u}, \vec{v}$ und einen Skalar k:

$$A \cdot (\vec{u} + \vec{v}) = A \cdot \vec{u} + A \cdot \vec{v} \qquad A \cdot (k \cdot \vec{u}) = k \cdot (A \cdot \vec{u})$$

Außerdem gibt es zu jeder linearen Abbildung $\psi \colon K^n \to K^m$ eine Matrix A mit $\psi = \psi_A$.

Vektorräume und Matrizen

Beispiel: wir betrachten folgende 2×2-Matrix als lineare Abbildung:

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

Es gilt:

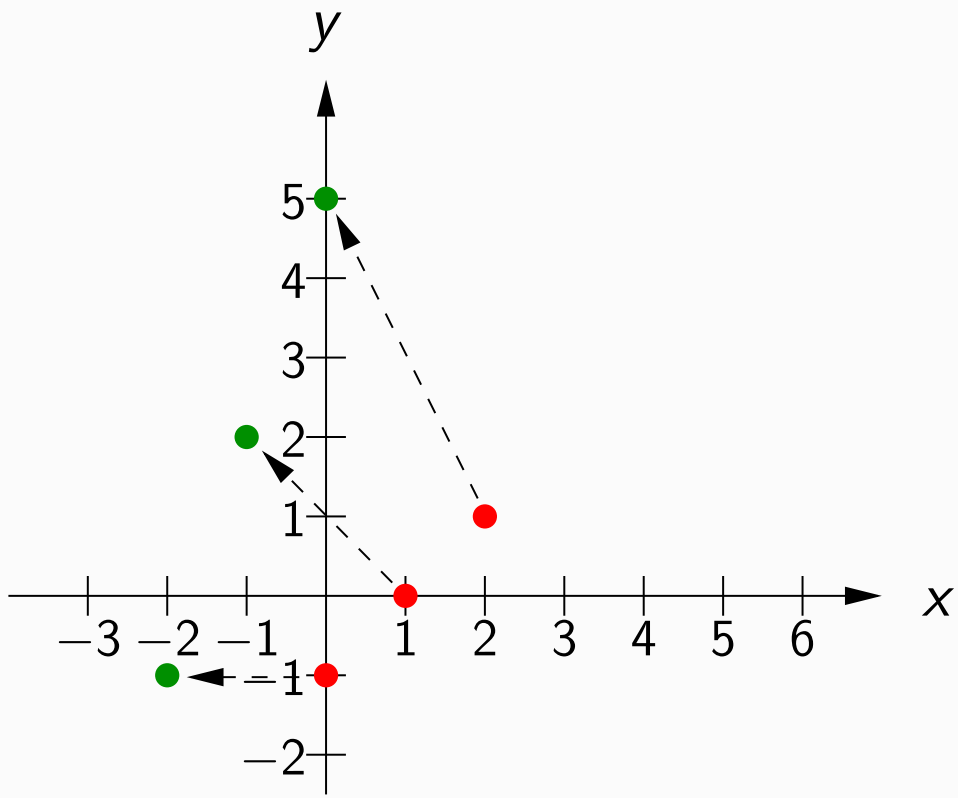
$$A \cdot \begin{pmatrix} 0 \\ -1 \end{pmatrix} = \begin{pmatrix} -1 & 2 \\ 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ -1 \end{pmatrix} = \begin{pmatrix} -2 \\ -1 \end{pmatrix}, \text{ d.h. } \psi_A(\begin{pmatrix} 0 \\ -1 \end{pmatrix}) = \begin{pmatrix} -2 \\ -1 \end{pmatrix}$$

$$A \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} -1 & 2 \\ 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} -1 \\ 2 \end{pmatrix}, \text{ d.h. } \psi_A(\begin{pmatrix} 1 \\ 0 \end{pmatrix}) = \begin{pmatrix} -1 \\ 2 \end{pmatrix}$$

$$A \cdot \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} -1 & 2 \\ 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 5 \end{pmatrix}, \text{ d.h. } \psi_A(\begin{pmatrix} 2 \\ 1 \end{pmatrix}) = \begin{pmatrix} 0 \\ 5 \end{pmatrix}$$

Vektorräume und Matrizen

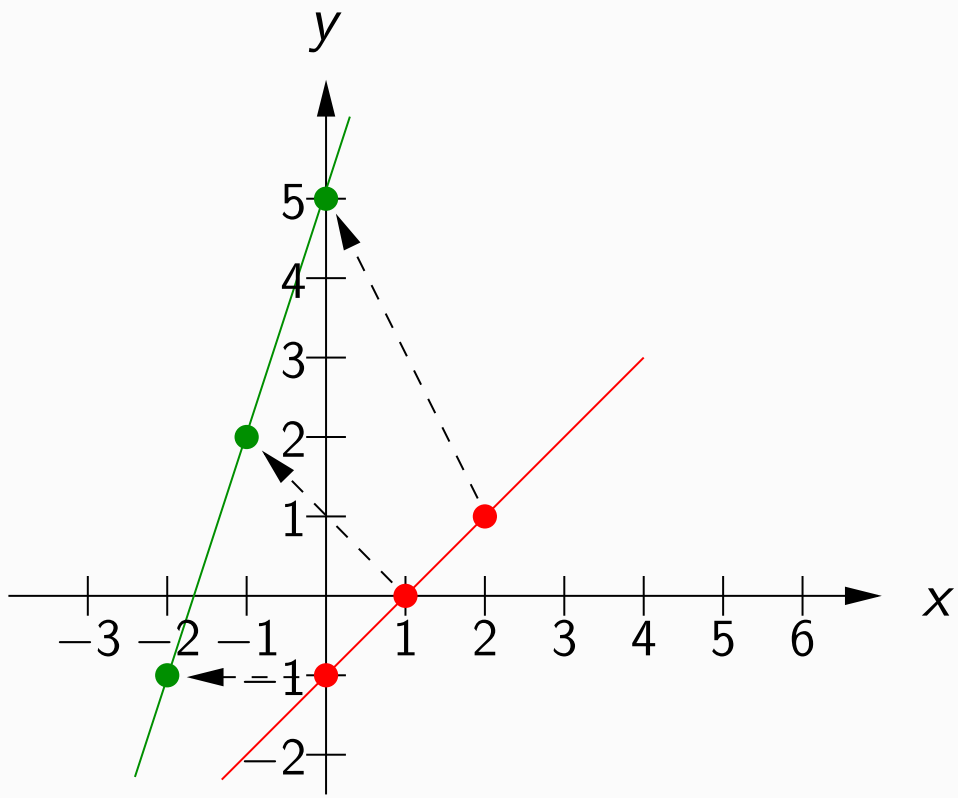
Graphische Darstellung:



Rote Punkte/Vektoren werden auf grüne Punkte/Vektoren abgebildet. Darstellung der Abbildungsvorschrift durch gestrichelte Pfeile.

Vektorräume und Matrizen

Graphische Darstellung:



Lineare Abbildungen bilden Geraden auf Geraden ab. Linien werden also erhalten. Daher stammt der Name!

Vektorräume und Matrizen

Zwei Matrizen gleicher Zeilen- und Spaltendimension können addiert werden:

Addition von Matrizen

Seien A, B $m \times n$-Matrizen. Dann hat $C = A + B$ folgendes Aussehen:

$$\begin{pmatrix} A_{1,1} & \dots & A_{1,n} \\ \vdots & \ddots & \vdots \\ A_{m,1} & \dots & A_{m,n} \end{pmatrix} + \begin{pmatrix} B_{1,1} & \dots & B_{1,n} \\ \vdots & \ddots & \vdots \\ B_{m,1} & \dots & B_{m,n} \end{pmatrix} = \begin{pmatrix} C_{1,1} & \dots & C_{1,n} \\ \vdots & \ddots & \vdots \\ C_{m,1} & \dots & C_{m,n} \end{pmatrix}$$

mit $C_{i,j} = A_{i,j} + B_{i,j}$.
Die Addition erfolgt komponentenweise.

Vektorräume und Matrizen

Matrizen als additive Gruppe

Die Menge aller $m \times n$-Matrizen über einem Körper K bildet eine kommutative Gruppe bezüglich der Addition.
Dabei ist die Nullmatrix N das neutrale Element und das additive Inverse zu A ist $-A$:

$$N = \begin{pmatrix} 0 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 0 \end{pmatrix} \qquad -A = \begin{pmatrix} -A_{1,1} & \dots & -A_{1,n} \\ \vdots & \ddots & \vdots \\ -A_{m,1} & \dots & -A_{m,n} \end{pmatrix}$$

Vektorräume und Matrizen

Matrizen können auch miteinander multipliziert werden.

Multiplikation von Matrizen

Sei A eine $m \times n$-Matrix und B eine $n \times r$-Matrix. Dann ist $C = A \cdot B$ eine $m \times r$-Matrix und hat folgendes Aussehen:

$$\begin{pmatrix} A_{1,1} & \dots & A_{1,n} \\ \vdots & \ddots & \vdots \\ A_{m,1} & \dots & A_{m,n} \end{pmatrix} \cdot \begin{pmatrix} B_{1,1} & \dots & B_{1,r} \\ \vdots & \ddots & \vdots \\ B_{n,1} & \dots & B_{n,r} \end{pmatrix} = \begin{pmatrix} C_{1,1} & \dots & C_{1,r} \\ \vdots & \ddots & \vdots \\ C_{m,1} & \dots & C_{m,r} \end{pmatrix}$$

mit

$$C_{i,j} = \sum_{\ell=1}^{n} A_{i,\ell} \cdot B_{\ell,j}$$

Vektorräume und Matrizen

Merkregel:

- Multipliziere die Zeilen der ersten Matrix (A) mit den Spalten der zweiten Matrix (B).
- Um in der Ergebnismatrix C den Eintrag $C_{i,j}$ zu erhalten, multipliziere die i-te Zeile der ersten Matrix (A) mit der j-ten Spalte der zweiten Matrix (B) und addiere jeweils die Multiplikationsergebnisse auf.

Vektorräume und Matrizen

Alternative Beschreibung: teile B in r (Spalten-)Vektoren auf

$$B = \begin{pmatrix} \vec{b}_1 & \dots & \vec{b}_r \end{pmatrix}$$

Multipliziere diese Spaltenvektoren dann einzeln. Die entstehenden Spaltenvektoren werden dabei von links nach rechts nebeneinandergeschrieben.

$$A \cdot B = A \cdot \begin{pmatrix} \vec{b}_1 & \dots & \vec{b}_r \end{pmatrix} = \begin{pmatrix} A \cdot \vec{b}_1 & \dots & A \cdot \vec{b}_r \end{pmatrix}$$

Multiplikation einer Matrix mit einem Vektor ist daher ein Spezialfall der Matrizenmultiplikation.

Vektorräume und Matrizen

Beispiel: Matrixmultiplikation in $\mathbb{R}$

Multiplikation einer 2×3-Matrix mit einer 3×2-Matrix:

$$\begin{pmatrix} 3 & 4 & -1 \\ -2 & 2 & -3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0,5 & -3 \\ -2 & -1 \end{pmatrix}$$

$$= \begin{pmatrix} 3+2+2 & 0-12+1 \\ -2+1+6 & 0-6+3 \end{pmatrix} = \begin{pmatrix} 7 & -11 \\ 5 & -3 \end{pmatrix}$$

Vektorräume und Matrizen

Merkregel Falk-Schema: Folgende "Eselsbrücke" hilft bei der Matrizenmultiplikation $A \cdot B = C$

- Die zweite Matrix B wird nach oben verschoben.
- In dem Feld rechts von der ersten Matrix A und unterhalb der zweiten Matrix B entsteht dann die neue Matrix C.
- Ein Eintrag von C entsteht dadurch, dass die entsprechende Zeile von A und Spalte von B miteinander multipliziert werden.

$$\begin{pmatrix} 3 & 4 & -1 \\ -2 & 2 & -3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0,5 & -3 \\ -2 & -1 \end{pmatrix} = \begin{pmatrix} 7 & -11 \\ 5 & -3 \end{pmatrix}$$

			1	0
			0,5	-3
			-2	-1
3	4	-1	7	-11
-2	2	-3	5	-3

Vektorräume und Matrizen

Assoziativität der Matrizenmultiplikation

Matrixmultiplikation ist assoziativ. D.h., falls A eine $m \times n$-Matrix, B eine $n \times r$-Matrix und C eine $r \times s$-Matrix ist, dann gilt:

$$A \cdot (B \cdot C) = (A \cdot B) \cdot C$$

Es macht keinen Sinn zu fragen, ob die Menge aller Matrizen beliebiger Dimension ein Monoid oder eine Gruppe bezüglich der Multiplikation ist. Es läßt sich nicht jede Matrix mit jeder Matrix verknüpfen, da die Dimensionen übereinstimmen müssen.

Diese Frage macht nur Sinn für quadratische Matrizen fester Dimension.

Vektorräume und Matrizen

Eigenschaften quadratischer Matrizen (I)

- Die Menge aller quadratischen $n \times n$-Matrizen bildet ein Monoid mit der Multiplikationsoperation.
- Insbesondere gibt es ein neutrales Element der Multiplikation, die sogenannte Einheitsmatrix E_n:

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

Diese Matrix hat Einsen in der Diagonale von links oben nach rechts unten und besteht ansonsten nur aus Nullen.

Vektorräume und Matrizen

Eigenschaften quadratischer Matrizen (II)

- Nicht jede quadratische Matrix A hat ein multiplikatives Inverses A^{-1}. Matrizen, die kein multiplikatives Inverses haben, heißen singulär.
- Matrizenmultiplikation ist außerdem nicht kommutativ.

Vektorräume und Matrizen

Beispiel 1: Multiplikation mit der Einheitsmatrix

$$E_3 \cdot \begin{pmatrix} -2 & 3 & 1 \\ 0,5 & 7 & -3 \\ 1 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} -2 & 3 & 1 \\ 0,5 & 7 & -3 \\ 1 & 1 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} -2+0+0 & 3+0+0 & 1+0+0 \\ 0+0,5+0 & 0+7+0 & 0+(-3)+0 \\ 0+0+1 & 0+0+1 & 0+0+0 \end{pmatrix} = \begin{pmatrix} -2 & 3 & 1 \\ 0,5 & 7 & -3 \\ 1 & 1 & 0 \end{pmatrix}$$

Für jede $n \times n$-Matrix A gilt sowohl $E_n \cdot A = A$, als auch $A \cdot E_n = A$.

Vektorräume und Matrizen

Beispiel 2: Nicht-Existenz von Inversen

Die Nullmatrix, aber auch viele andere Matrizen haben kein Inverses. Wir betrachten folgende Matrix A:

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

Es gibt keine 3×3-Matrix B, so dass $A \cdot B$ die Einheitsmatrix ist:

$$A \cdot B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} B_{1,1} & B_{1,2} & B_{1,3} \\ B_{2,1} & B_{2,3} & B_{2,3} \\ B_{3,1} & B_{3,2} & B_{3,3} \end{pmatrix}$$

$$= \begin{pmatrix} B_{1,1} & B_{1,2} & B_{1,3} \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = E_3$$

Vektorräume und Matrizen

Beispiel 3: Nicht-Kommutativität der Matrizenmultiplikation

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

$$\neq \begin{pmatrix} -2 & 1 & -2 \\ 0 & 0 & 0 \\ 6 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 0 \\ 3 & 1 & 2 \\ 0 & 3 & 1 \end{pmatrix}$$

Vektorräume und Matrizen

Die Multiplikation von zwei Matrizen entspricht der Verknüpfung der dazugehörigen linearen Abbildungen.

Matrixmultiplikation und Verknüpfung linearer Abbildungen

Sei A eine $m \times n$-Matrix über und $\psi_A \colon K^n \to K^m$ die dazugehörige lineare Abbildung mit $\psi_A(\vec{u}) = A \cdot \vec{u}$. Analog sei B eine $n \times r$-Matrix und $\psi_B \colon K^r \to K^n$ die dazugehörige lineare Abbildung.

Dann beschreibt die Matrix $C = A \cdot B$ folgende lineare Abbildung $\psi_C \colon K^r \to K^m$ mit

$$\psi_C(\vec{u}) = (A \cdot B) \cdot \vec{u} = A \cdot (B \cdot \vec{u}) = A \cdot \psi_B(\vec{u}) = \psi_A(\psi_B(\vec{u}))$$

und damit gilt $\psi_C = \psi_{A \cdot B} = \psi_A \circ \psi_B$.

Das beruht im wesentlichen auf der Assoziativität der Matrixmultiplikation.

Erzeugendensysteme und Basen

Wir betrachten nun Konzepte, mit denen man einen Vektorraum aus einigen wenigen Vektoren, sogenannten Basisvektoren erzeugen kann.

Das hat auch Beziehungen zur Berechnung von multiplikativen Inversen einer Matrix und zum Lösen von Gleichungssystemen.

Erzeugendensysteme und Basen

Erzeugendensystem

Gegeben sei ein n-dimensionaler Vektorraum über einem Körper K. Eine Menge $S = \{\vec{v}_1, \ldots, \vec{v}_m\}$ von Vektoren heißt Erzeugendensystem des Vektorraums, falls sich jeder Vektor $\vec{u} \in K^n$ als Linearkombination von Vektoren aus S darstellen läßt. D.h., für jeden Vektor $\vec{u}$ gibt es Skalare $k_1, \ldots, k_m \in K$, so dass gilt:

$$\vec{u} = k_1 \cdot \vec{v}_1 + \cdots + k_m \cdot \vec{v}_m$$

Erzeugendensysteme und Basen

Beispiel 1: die Menge

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

ist ein Erzeugendensystem für den Vektorraum $\mathbb{R}^2$. Ein Vektor $\vec{u}$ läßt sich immer folgendermaßen darstellen:

$$\vec{u} = \begin{pmatrix}u_1\\u_2\end{pmatrix} = \frac{u_1}{2} \cdot \begin{pmatrix}2\\0\end{pmatrix} + u_2 \cdot \begin{pmatrix}0\\1\end{pmatrix} + 0 \cdot \begin{pmatrix}1\\1\end{pmatrix}$$

Erzeugendensysteme und Basen

Bemerkung: Die Beziehung

$$\vec{u} = k_1 \cdot \vec{v}_1 + \cdots + k_m \cdot \vec{v}_m$$

kann auch dargestellt werden als

$$\vec{u} = \underbrace{\begin{pmatrix} \vec{v}_1 & \dots & \vec{v}_m \end{pmatrix}}_{V} \cdot \begin{pmatrix} k_1 \\ \vdots \\ k_m \end{pmatrix}$$

wobei $V = \begin{pmatrix} \vec{v}_1 & \dots & \vec{v}_m \end{pmatrix}$ eine Matrix ist, die aus den Spaltenvektoren $\vec{v}_1, \dots, \vec{v}_m$ zusammengesetzt ist.

D.h., eine Multiplikation einer Matrix mit einem Vektor ergibt eine Linearkombination der Spalten der Matrix.

Erzeugendensysteme und Basen

Die Menge S im vorherigen Beispiel enthält überflüssige Elemente, mindestens ein Vektor ist redundant. Beispielsweise kann der dritte Vektor durch die beiden ersten dargestellt werden.

Linear unabhängige Menge

Gegeben sei ein n-dimensionaler Vektorraum über einem Körper K. Eine Menge $S = \{\vec{v}_1, \ldots, \vec{v}_m\}$ von Vektoren heißt linear unabhängig, falls sich kein Vektor $\vec{v}$ aus S als Linearkombination der anderen Vektoren darstellen läßt.

Erzeugendensysteme und Basen

Beispiel 2: die Menge

$$S = \{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \}$$

ist linear unabhängig im $\mathbb{R}^3$, sie ist jedoch kein Erzeugendensystem.

Erzeugendensysteme und Basen

Alternative Definition für linear unabhängig:

Eine Menge $S = \{\vec{v}_1, \ldots, \vec{v}_m\}$ von Vektoren ist linear unabhängig, wenn für beliebige Skalare $k_1, \ldots, k_m \in K$ aus

$$k_1 \cdot \vec{v}_1 + \cdots + k_m \cdot \vec{v}_m = \vec{0}$$

immer $k_1 = \cdots = k_m = 0$ folgt.

Das heißt, man kann den Nullvektor nur auf eine Weise als Linearkombination von linear unabhängigen Vektoren darstellen: indem man alle Skalare mit 0 belegt.

In Kombination mit Lösungsverfahren für Gleichungssysteme ($\rightsquigarrow$ Gaußsches Eliminationsverfahren, wird im Anschluss behandelt), erhält man dadurch eine Methode, um zu überprüfen, ob eine Menge von Vektoren linear unabhängig ist.

Erzeugendensysteme und Basen

Basis

Gegeben sei ein n-dimensionaler Vektorraum über einem Körper K. Eine Menge $B = \{\vec{b}_1, \ldots, \vec{b}_m\}$ von Vektoren heißt Basis, falls sie gleichzeitig ein Erzeugendensystem und linear unabhängig ist.

Erzeugendensysteme und Basen

Beispiel 3: die Mengen

$$B_1 = \{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \}$$

und

$$B_2 = \{ \begin{pmatrix} 2 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 3 \\ 0 \end{pmatrix}, \begin{pmatrix} -2 \\ 0 \\ 1 \end{pmatrix} \}$$

sind beides Basen des $\mathbb{R}^3$.

Für B_1 ist dies relativ offensichtlich. Aus B_2 kann man einfach die Elemente von B_1 (die sogenannten Einheitsvektoren) bestimmen und außerdem sind die drei Vektoren linear unabhängig.

Erzeugendensysteme und Basen

Beispiel 3: die Menge

$$B_3 = \{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ 1 \end{pmatrix}, \begin{pmatrix} -2 \\ 2 \\ 1 \end{pmatrix} \}$$

ist keine Basis des $\mathbb{R}^3$, denn ihre Vektoren sind nicht linear unabhängig. Insbesondere kann man den dritten Vektor durch Linearkombination der anderen beiden Vektoren darstellen:

$$\begin{pmatrix} -2 \\ 2 \\ 1 \end{pmatrix} = (-2) \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} + 1 \cdot \begin{pmatrix} 0 \\ 2 \\ 1 \end{pmatrix}$$

Erzeugendensysteme und Basen

Einheitsvektoren

Gegeben sei ein n-dimensionaler Vektorraum über einem Körper K und sei $i \in \{1, \ldots, n\}$. Der i-te Einheitsvektor $\vec{e_i}$ ist der Vektor, der an der i-ten Stelle eine 1 hat und sonst nur aus Nullen besteht.

$$\vec{e_1} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \qquad \ldots \qquad \vec{e_n} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

Erzeugendensysteme und Basen

Bemerkungen:

- Wenn B eine Basis des K^n ist, dann gibt es für jeden Vektor des K^n genau eine Möglichkeit, diesen als Linearkombination von Vektoren aus B darzustellen.
- Die Einheitsvektoren bilden immer eine Basis des K^n. Für jeden Vektor $\vec{u}$ gilt:

$$\vec{u} = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} = u_1 \cdot \vec{e}_1 + \cdots + u_n \cdot \vec{e}_n$$

- Die Einheitsvektoren sind jedoch nicht die einzige Basis.

Erzeugendensysteme und Basen

Weitere Bemerkungen:

- Ein Erzeugendensystem des K^n besteht immer aus mindestens n Vektoren. Eine Menge, die weniger als n Vektoren enthält, kann also kein Erzeugendensystem sein.
- Eine linear unabhängige Menge im K^n besteht immer aus höchstens n Vektoren. Eine Menge, die mehr als n Vektoren enthält, ist also immer linear abhängig.

Erzeugendensysteme und Basen

Weitere Bemerkungen:

- Eine Basis des K^n besteht immer aus genau n Vektoren.
- Eine linear unabhängige Menge mit n Vektoren ist immer eine Basis des K^n.
- Ein Erzeugendensystem mit n Vektoren ist auch immer eine Basis des K^n.

Erzeugendensysteme und Basen

Aus den letzten beiden Bemerkungen ergeben sich zwei einfache Verfahren, um festzustellen, ob eine Menge $B \subseteq K^n$ von Vektoren eine Basis des K^n ist oder nicht:

- Man überprüft, ob B genau n Vektoren enthält und ob diese Vektoren ein Erzeugendensystem sind.
- *Oder:* Man überprüft, ob B genau n Vektoren enthält und ob diese Vektoren linear unabhängig sind.

Insbesondere kann eine Menge von Vektoren, die mehr oder weniger als n Vektoren enthält, niemals eine Basis sein.

Erzeugendensysteme und Basen

Wir können nun die Frage beantworten, wann eine quadratische Matrix A invertierbar ist.

Angenommen die Matrix A ist invertierbar, d.h., es gibt ein multiplikatives Inverses A^{-1} mit $A \cdot A^{-1} = E_n$. Wir betrachten A^{-1} als aufgebaut aus einzelnen Spaltenvektoren $\vec{a}_1, \ldots, \vec{a}_n$, d.h. $A^{-1} = \begin{pmatrix} \vec{a}_1 & \ldots & \vec{a}_n \end{pmatrix}$. Dann gilt:

$$A \cdot A^{-1} = A \cdot \begin{pmatrix} \vec{a}_1 & \ldots & \vec{a}_n \end{pmatrix} = \begin{pmatrix} A \cdot \vec{a}_1 & \ldots & A \cdot \vec{a}_n \end{pmatrix} = \begin{pmatrix} \vec{e}_1 & \ldots & \vec{e}_n \end{pmatrix}$$

Es gilt also $A \cdot \vec{a}_i = \vec{e}_i$ für $i \in \{1, \ldots, n\}$. Das bedeutet, dass man aus den Spalten von A durch Linearkombination jeden Einheitsvektor (und damit auch jeden anderen Vektor) erhalten kann.

Erzeugendensysteme und Basen

Die Menge der Spaltenvektoren von A ist damit ein Erzeugendensystem und – da sie aus genau n Vektoren besteht – eine Basis.

Umgekehrt gilt auch, dass es zu einer Matrix, deren Spaltenvektoren eine Basis bilden, Vektoren $\vec{a}_1, \ldots, \vec{a}_n$ gibt, die die obigen Eigenschaften haben und aus denen man eine inverse Matrix konstruieren kann. (Wie man diese Vektoren berechnen kann, besprechen wir später.)

Erzeugendensysteme und Basen

Zusammenfassend gilt also:

Invertierbare Matrizen und Basen

Eine $n \times n$-Matrix A über einem Körper K ist invertierbar, genau dann, wenn die Spalten von A eine Basis des K^n bilden.

Man sagt dann auch, die Matrix hat den vollen Rang.

Gaußsches Eliminationsverfahren

Wir betrachten nun ein Verfahren zum Lösen von Gleichungssystemen.

Gegeben sei eine $m \times n$-Matrix A und ein m-dimensionaler Vektor $\vec{b}$. Gesucht ist ein n-dimensionaler Vektor $\vec{x}$, der folgende Gleichung erfüllt:

$$A \cdot \vec{x} = \vec{b}$$

Wenn A quadratisch ($m = n$) und zudem noch invertierbar ist, dann kann man zeigen, dass es genau eine Lösung $\vec{x}$ gibt: man multipliziert die obige Gleichung auf beiden Seiten mit A^{-1}:

$A^{-1} \cdot A \cdot \vec{x} = A^{-1} \cdot \vec{b}$ und daraus folgt wegen $A^{-1} \cdot A \cdot \vec{x} = E_n \cdot \vec{x} = \vec{x}$, dass $\vec{x} = A^{-1} \cdot \vec{b}$.

Gaußsches Eliminationsverfahren

Trotzdem bleiben noch viele offene Fragen:

- Wie berechnet man $\vec{x}$? (Wir haben ja noch kein Verfahren, um das multiplikative Inverse einer Matrix zu bestimmen.)
- Was passiert, wenn A nicht quadratisch oder nicht invertierbar ist?
- Kann eine Gleichung evtl. mehrere Lösungen haben?
- Kann eine Gleichung evtl. keine Lösung haben?

Gaußsches Eliminationsverfahren

Wir betrachten eine Gleichung in "ausgeschriebener" Form:

$$A \cdot \vec{x} = \vec{b}$$

wird geschrieben als

$$\begin{pmatrix} A_{1,1} & \cdots & A_{1,n} \\ \vdots & \ddots & \vdots \\ A_{m,1} & \cdots & A_{m,n} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$$

und das ist gleichbedeutend damit, dass das folgende Gleichungssystem eine Lösung hat:

$$\begin{aligned} A_{1,1} \cdot x_1 + \cdots + A_{1,n} \cdot x_n &= b_1 \\ &\vdots \\ A_{m,1} \cdot x_1 + \cdots + A_{m,n} \cdot x_n &= b_m \end{aligned}$$

Gaußsches Eliminationsverfahren

In den folgenden Beispielen arbeiten wir im Körper $\mathbb{R}$.

Beispiel 1: Gleichungssystem mit einer Lösung

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

Man kann dieses Gleichungssystem durch "geschicktes" Einsetzen lösen: zweite Gleichung wird umgeformt in $x_1 = 5 + 3 \cdot x_2$, eingesetzt in die erste Gleichung ergibt

$$3 \cdot (5 + 3 \cdot x_2) + 4 \cdot x_2 = 15 + 13 \cdot x_2 = 2$$

und daraus folgt $x_2 = -1$. Daher: $x_1 = 5 + 3 \cdot x_2 = 5 + 3 \cdot (-1) = 2$.

Die (einzige) Lösung ist damit $x_1 = 2$, $x_2 = -1$.

Gaußsches Eliminationsverfahren

Für dieses Beispiel gilt:

$$A = \begin{pmatrix} 3 & 4 \\ 1 & -3 \end{pmatrix} \qquad \vec{b} = \begin{pmatrix} 2 \\ 5 \end{pmatrix}$$

und A hat das multiplikative Inverse

$$A^{-1} = \begin{pmatrix} \frac{3}{13} & \frac{4}{13} \\ \frac{1}{13} & -\frac{3}{13} \end{pmatrix}$$

(Wir werden noch sehen, wie man solche Inverse tatsächlich berechnen kann.)

Test:

$$\vec{x} = A^{-1} \cdot \vec{b} = \begin{pmatrix} \frac{3}{13} & \frac{4}{13} \\ \frac{1}{13} & -\frac{3}{13} \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 5 \end{pmatrix} = \begin{pmatrix} \frac{26}{13} \\ -\frac{13}{13} \end{pmatrix} = \begin{pmatrix} 2 \\ -1 \end{pmatrix}$$

Gaußsches Eliminationsverfahren

Beispiel 2: Gleichungssystem ohne Lösung

$$\begin{aligned} x_1 + 2 \cdot x_2 &= 3 \\ -2 \cdot x_1 - 4 \cdot x_2 &= 1 \end{aligned}$$

Man sieht, dass man $-2 \cdot x_1 - 4 \cdot x_2$ erhält, indem man $x_1 + 2 \cdot x_2$ mit -2 multipliziert. Also müsste auch das Ergebnis rechts unten ($= 1$) ein entsprechendes Vielfaches des Ergebnisses rechts oben ($= 3$) sein. Das ist aber nicht der Fall.
Daher hat das Gleichungssystem keine Lösung.

Hier sieht man, dass die Matrix

$$A = \begin{pmatrix} 1 & 2 \\ -2 & -4 \end{pmatrix}$$

aus linear abhängigen Spaltenvektoren besteht und nicht den vollen Rang hat. Sie ist also nicht invertierbar.

Gaußsches Eliminationsverfahren

Beispiel 3: Gleichungssystem mit mehreren Lösungen

$$\begin{aligned} x_1 + 2 \cdot x_2 &= 3 \\ -2 \cdot x_1 - 4 \cdot x_2 &= -6 \end{aligned}$$

Die untere Gleichung ist ein Vielfaches der oberen Gleichung (Faktor -2). Also ist die untere Gleichung redundant und wir müssen alle Lösungen der oberen Gleichung bestimmen. Es gilt $x_1 = 3 - 2 \cdot x_2$, also hat die Lösung $\vec{x}$ die Form:

$$\vec{x} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 3 - 2 \cdot x_2 \\ x_2 \end{pmatrix} = \begin{pmatrix} 3 \\ 0 \end{pmatrix} + x_2 \cdot \begin{pmatrix} -2 \\ 1 \end{pmatrix}$$

Dabei kann $x_2 \in \mathbb{R}$ beliebig gewählt werden und wir haben unendlich viele Lösungen.

Wie in Beispiel 2 ist die Matrix nicht invertierbar.

Gaußsches Eliminationsverfahren

Wir betrachten nun ein allgemeines Verfahren, um solche Gleichungssystem zu lösen: das Gaußsche Eliminationsverfahren. Der Einfachheit halber stellen wir ein Gleichungssystem folgendermaßen dar:

$$\begin{aligned} A_{1,1} \cdot x_1 + \cdots + A_{1,n} \cdot x_n &= b_1 \\ &\vdots \\ A_{m,1} \cdot x_1 + \cdots + A_{m,n} \cdot x_n &= b_m \end{aligned}$$

entspricht

$$\left(\begin{array}{ccc|c} A_{1,1} & \cdots & A_{1,n} & b_1 \\ \vdots & \ddots & \vdots & \vdots \\ A_{m,1} & \cdots & A_{m,n} & b_m \end{array}\right)$$

Gaußsches Eliminationsverfahren

Das Gaußsche Eliminationsverfahren basiert auf folgenden Beobachtungen:

- Wenn man zwei Zeilen vertauscht, so ändern sich dadurch die Lösungen nicht.
- Wenn man eine Zeile mit einem Wert ungleich 0 multipliziert, so ändern sich dadurch die Lösungen nicht.
- Wenn man das Vielfache einer Zeile zu einer anderen Zeile addiert (von einer anderen Zeile subtrahiert), so ändern sich dadurch die Lösungen nicht.
- Wenn man zwei Spalten i, j vertauscht, so ändert sich dadurch die Reihenfolge der Variablen (Wert von x_i wird mit Wert von x_j vertauscht). Das kann man sich merken und am Ende wieder in Ordnung bringen.

Gaußsches Eliminationsverfahren

Ziel: wir bringen das Gleichungssystem durch die oben beschriebenen Umformungen auf folgende Form (obere Dreiecksform):

$$\left(\begin{array}{ccccccc|c}
A_{1,1} & A_{1,2} & \dots & A_{1,k} & \dots & A_{1,n} & b_1 \\
0 & A_{2,2} & \dots & A_{2,k} & \dots & A_{2,n} & b_2 \\
\vdots & \ddots & \ddots & \vdots & \ddots & \vdots & \vdots \\
0 & \dots & 0 & A_{k,k} & \dots & A_{k,n} & b_k \\
0 & & & \dots & & 0 & b_{k+1} \\
\vdots & & & \ddots & & \vdots & \vdots \\
0 & & & \dots & & 0 & b_m
\end{array}\right)$$

wobei $A_{1,1} = 1, A_{2,2} = 1, \dots, A_{k,k} = 1$

Gaußsches Eliminationsverfahren

Bemerkung:

Es handelt sich dabei um eine Matrix mit Einsen auf der (nicht notwendigerweise durchgehenden) Diagonale, bei der unterhalb der Diagonale nur Nullen stehen.

Außerdem kommen ab der $k+1$-sten Zeile nur noch Nullen vor. Dieser Block von Nullen kann auch vollkommen fehlen.

Aus obiger Form kann man dann relativ einfach alle Lösungen ablesen.

Gaußsches Eliminationsverfahren

Bei einer $m \times n$-Matrix A läuft das Gaußsche Eliminationsverfahren in n Schritten ab. In jedem Schritt wird eine weitere Spalte in die gewünschte Form gebracht.

Gaußsches Eliminationsverfahren (i-ter Schritt)

Angenommen die Spalten $1, \ldots, i-1$ sind schon in der gewünschten Form. Dann sieht die Matrix folgendermaßen aus:

$$\left(\begin{array}{ccccccc|c}
1 & A_{1,2} & \ldots & & A_{1,i} & \ldots & A_{1,n} & b_1 \\
0 & 1 & \ldots & & A_{2,i} & \ldots & A_{2,n} & b_2 \\
\vdots & \ddots & \ddots & & \vdots & \ddots & \vdots & \vdots \\
0 & \ldots & 0 & & A_{i,i} & \ldots & A_{i,n} & b_i \\
0 & \ldots & 0 & & A_{i+1,i} & \ldots & A_{i+1,n} & b_{i+1} \\
\vdots & \ddots & \vdots & & \vdots & \ddots & \vdots & \vdots \\
0 & \ldots & 0 & & A_{m,i} & \ldots & A_{m,n} & b_m
\end{array}\right)$$

Gaußsches Eliminationsverfahren

Wir betrachten nun $A_{i,i}$, das sogenannte Pivotelement.

Pivotelement $A_{i,i} \neq 0$

In diesem Fall hat $A_{i,i}$ ein multiplikatives Inverses $A_{i,i}^{-1}$ (wir arbeiten in einem Körper!).

Wir multiplizieren die i-te Zeile mit $A_{i,i}^{-1}$, wodurch das Pivotelement nun den Wert 1 hat. Wir haben folgende Situation:

$$\left(\begin{array}{ccccccc|c}
1 & A_{1,2} & \dots & A_{1,i} & \dots & A_{1,n} & b_1 \\
0 & 1 & \dots & A_{2,i} & \dots & A_{2,n} & b_2 \\
\vdots & \ddots & \ddots & \vdots & \ddots & \vdots & \vdots \\
0 & \dots & 0 & 1 & \dots & A_{i,n} & b_i \\
0 & \dots & 0 & A_{i+1,i} & \dots & A_{i+1,n} & b_{i+1} \\
\vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & \dots & 0 & A_{m,i} & \dots & A_{m,n} & b_m
\end{array}\right)$$

Gaußsches Eliminationsverfahren

Pivotelement $A_{i,i} \neq 0$ (Fortsetzung)

Wir behandeln nun jede Zeile j (mit $j > i$): wir multiplizieren die i-te Zeile mit $A_{j,i}$ und ziehen sie von der j-ten Zeile ab.

Dadurch ergibt sich folgende Zeile:

$$0 \quad \ldots \quad 0 \quad (A_{j,i} - A_{j,i} \cdot 1) \quad \ldots \quad (A_{j,n} - A_{j,i} \cdot A_{i,n}) \mid (b_j - A_{j,i} \cdot b_i)$$

und es gilt $A_{j,i} - A_{j,i} \cdot 1 = 0$.

Damit ist die i-te Spalte jetzt in der richtigen Form.

Gaußsches Eliminationsverfahren

Falls das Pivotelement $A_{i,i}$ den Wert 0 hat, so hat es kein multiplikatives Inverses und wir können das vorherige Verfahren nicht anwenden. Wir unterscheiden zwei Fälle:

Pivotelement $A_{i,i} = 0$ (Fall 1)

Angenommen es gibt ein Element $A_{j,i}$ (mit $j > i$) unterhalb von $A_{i,i}$ mit $A_{j,i} \neq 0$.

Dann vertausche die i-te und die j-te Zeile und fange mit dem i-ten Schritt wieder von vorne an.
(Achtung: die Elemente b_i, b_j in der rechten Spalte müssen auch getauscht werden.)

Gaußsches Eliminationsverfahren

Pivotelement $A_{i,i} = 0$ (Fall 2)

Angenommen es gibt kein Element $A_{j,i}$ (mit $j > i$) unterhalb von $A_{i,i}$ mit $A_{j,i} \neq 0$. D.h., alle Elemente in dieser Spalte, angefangen mit $A_{i,i}$, sind gleich Null.

Dann betrachten wir das Rechteck rechts unten in der Matrix:

$$\left(\begin{array}{ccc|c} A_{i,i} & \dots & A_{i,n} & b_i \\ A_{i+1,i} & \dots & A_{i+1,n} & b_{i+1} \\ \vdots & \ddots & \vdots & \vdots \\ A_{m,i} & \dots & A_{m,n} & b_m \end{array}\right)$$

Falls alle Elemente $A_{j,\ell}$ (mit $j \geq i$ und $\ell \geq i$) gleich Null sind, dann hält das Verfahren an.

Gaußsches Eliminationsverfahren

Pivotelement $A_{i,i} = 0$ (Fall 2) (Fortsetzung)

Ansonsten finde eine Spalte ℓ, in der es einen Wert $A_{j,\ell} \neq 0$ gibt (mit $j \geq i$, $\ell \geq i$) und vertausche die Spalte i und die Spalte ℓ.

Diese Vertauschung muss gemerkt und später wieder rückgängig gemacht werden!

Beginne mit dem i-ten Schritt wieder von vorne.

Gaußsches Eliminationsverfahren

Ablesen der Lösung: ▸ Umgeformtes Gleichungssystem

Keine Lösung

Wir betrachten zunächst den unteren Block, in dem nur Nullen stehen. Falls eines der Elemente $b_{k+1}, \ldots, b_m$ ungleich Null ist, so hat das Gleichungssystem keine Lösung.

Gaußsches Eliminationsverfahren

▸ Umgeformtes Gleichungssystem

Lösung bestimmen

Ansonsten betrachte den oberen Block mit
$A_{1,1} = 1, A_{2,2} = 1, \ldots, A_{k,k} = 1$

$$\left(\begin{array}{ccccccc|c} A_{1,1} & A_{1,2} & \ldots & A_{1,k} & \ldots & A_{1,n} & b_1 \\ 0 & A_{2,2} & \ldots & A_{2,k} & \ldots & A_{2,n} & b_2 \\ \vdots & \ddots & \ddots & \vdots & \ddots & \vdots & \vdots \\ 0 & \ldots & 0 & A_{k,k} & \ldots & A_{k,n} & b_k \end{array}\right)$$

und behandle die Zeilen von unten nach oben wie im Folgenden beschrieben.

Gaußsches Eliminationsverfahren

▸ Umgeformtes Gleichungssystem

Lösung bestimmen (Fortsetzung)

Die j-te Zeile entspricht folgender Gleichung:

$$x_j + A_{j,j+1} \cdot x_{j+1} + \cdots + A_{j,n} \cdot x_n = b_j$$

Es gilt

$$x_j = b_j - A_{j,j+1} \cdot x_{j+1} - \cdots - A_{j,n} \cdot x_n$$

Setze dabei für $x_{j+1}, \ldots, x_n$ möglicherweise bereits berechneten Werte ein.

Gaußsches Eliminationsverfahren

Nachbehandlung

Zuletzt mache noch die gemerkten Vertauschungen rückgängig.

Dadurch erhält man die Werte von $x_1, \ldots, x_n$, wobei gegebenenfalls Variablen x_j in der Darstellung übrigbleiben. Diese bleiben stehen und repräsentieren beliebige Körperelemente.
Dies passiert immer dann, wenn der obere Block nicht quadratisch ist und die Diagonale daher nicht ganz durchgeht.

Insgesamt erhält man eine Menge von Lösungsvektoren $\vec{x}$, die wie folgt dargestellt werden können:

$$\vec{x} \in \{\vec{u} + x_{j_1} \cdot \vec{v}_1 + \cdots + x_{j_r} \cdot \vec{v}_r \mid x_{j_k} \in \mathbb{R}\}$$

Falls $\vec{u} = \vec{0}$ (das passiert, falls $\vec{b} = \vec{0}$), dann ist die Lösungsmenge ein Vektorraum und $\vec{v}_1, \ldots, \vec{v}_r$ eine Basis dieses Vektorraums.

Gaußsches Eliminationsverfahren

Bemerkungen:

Beim Zeilen- bzw. Spaltentausch hat man meist mehrere Möglichkeiten. In diesem Fall tauscht man mit der Zeile, die das günstigste Pivotelement liefert.

Ein Pivotelement ist günstig, wenn es ein einfach zu handhabendes multiplikatives Inverses hat. Am besten ist natürlich die Eins als Pivotelement.

Gaußsches Eliminationsverfahren

Beispiel 4:

Wir lösen folgendes Gleichungssystem in $\mathbb{R}$:

$$\begin{array}{llll} & & +3 \cdot x_3 & +x_4 & = 3 \\ 3 \cdot x_1 & +4 \cdot x_2 & -2 \cdot x_3 & +3 \cdot x_4 & = 4 \\ 6 \cdot x_1 & +8 \cdot x_2 & +x_3 & -x_4 & = -13 \end{array}$$

In Matrixschreibweise:

$$\begin{pmatrix} 0 & 0 & 3 & 1 \\ 3 & 4 & -2 & 3 \\ 6 & 8 & 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 3 \\ 4 \\ -13 \end{pmatrix}$$

Gaußsches Eliminationsverfahren

Anfangssituation:

$$\left(\begin{array}{cccc|c} 0 & 0 & 3 & 1 & 3 \\ 3 & 4 & -2 & 3 & 4 \\ 6 & 8 & 1 & -1 & -13 \end{array}\right)$$

Schritt 1(a): Zeile 1 und Zeile 2 vertauschen, um Pivotelement ungleich 0 zu erhalten

$$\left(\begin{array}{cccc|c} 3 & 4 & -2 & 3 & 4 \\ 0 & 0 & 3 & 1 & 3 \\ 6 & 8 & 1 & -1 & -13 \end{array}\right)$$

Gaußsches Eliminationsverfahren

Schritt 1(b): Zeile 1 mit $\frac{1}{3}$ multiplizieren, um Pivotelement zu eins zu machen

$$\left(\begin{array}{cccc|c} 1 & \frac{4}{3} & -\frac{2}{3} & 1 & \frac{4}{3} \\ 0 & 0 & 3 & 1 & 3 \\ 6 & 8 & 1 & -1 & -13 \end{array}\right)$$

Schritt 1(c): Rechne "(Zeile 2) $-$ 0$\cdot$ (Zeile 1)" und "(Zeile 3) $-$ 6$\cdot$ (Zeile 1)"

$$\left(\begin{array}{cccc|c} 1 & \frac{4}{3} & -\frac{2}{3} & 1 & \frac{4}{3} \\ 0 & 0 & 3 & 1 & 3 \\ 0 & 0 & 5 & -7 & -21 \end{array}\right)$$

Gaußsches Eliminationsverfahren

Schritt 2(a): Spalte 2 und Spalte 4 vertauschen, um Pivotelement ungleich 0 zu erhalten. (Spaltenvertauschung merken!)

$$\left(\begin{array}{cccc|c} 1 & 1 & -\frac{2}{3} & \frac{4}{3} & \frac{4}{3} \\ 0 & 1 & 3 & 0 & 3 \\ 0 & -7 & 5 & 0 & -21 \end{array}\right)$$

Das Pivotelement ist bereits 1.

Schritt 2(b): Rechne "(Zeile 3) − (−7)· (Zeile 2)"

$$\left(\begin{array}{cccc|c} 1 & 1 & -\frac{2}{3} & \frac{4}{3} & \frac{4}{3} \\ 0 & 1 & 3 & 0 & 3 \\ 0 & 0 & 26 & 0 & 0 \end{array}\right)$$

Gaußsches Eliminationsverfahren

Schritt 2(c): Zeile 3 mit $\frac{1}{26}$ multiplizieren, um Pivotelement zu eins zu machen

$$\left(\begin{array}{cccc|c} 1 & 1 & -\frac{2}{3} & \frac{4}{3} & \frac{4}{3} \\ 0 & 1 & 3 & 0 & 3 \\ 0 & 0 & 1 & 0 & 0 \end{array}\right)$$

Damit ist das Gleichungssystem in der gewünschten Form.

Existenz der Lösung: es gibt keinen Block von Nullen, daher existiert eine Lösung.

Gaußsches Eliminationsverfahren

Bestimmung der Lösung:

Zeile 3: $x_3 = 0$
Zeile 2: $x_2 + 3 \cdot x_3 = 3$, also $x_2 = 3 - 3 \cdot x_3 = 3 - 0 = 3$
Zeile 1: $x_1 + x_2 - \frac{2}{3} \cdot x_3 + \frac{4}{3} \cdot x_4 = \frac{4}{3}$,
also $x_1 = \frac{4}{3} - x_2 + \frac{2}{3} \cdot x_3 - \frac{4}{3} \cdot x_4 = \frac{4}{3} - 3 + 0 - \frac{4}{3} \cdot x_4 = -\frac{5}{3} - \frac{4}{3} \cdot x_4$.

Vertauschungen rückgängig machen: wir müssen noch x_2 und x_4 zurücktauschen, es ergibt sich damit

$$x_1 = -\frac{5}{3} - \frac{4}{3} \cdot x_2 \qquad x_2 \text{ beliebig} \qquad x_3 = 0 \qquad x_4 = 3$$

Gaußsches Eliminationsverfahren

Vektorschreibweise:

$$\vec{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} -\frac{5}{3} - \frac{4}{3} \cdot x_2 \\ x_2 \\ 0 \\ 3 \end{pmatrix} = \begin{pmatrix} -\frac{5}{3} \\ 0 \\ 0 \\ 3 \end{pmatrix} + x_2 \cdot \begin{pmatrix} -\frac{4}{3} \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

Dieses Gleichungssystem hat unendlich viele Lösungen, eine für jede Belegung von x_2 mit einer reellen Zahl.

Gaußsches Eliminationsverfahren

Beispiel 2 (noch einmal):

$$\begin{aligned} x_1 + 2 \cdot x_2 &= 3 \\ -2 \cdot x_1 - 4 \cdot x_2 &= 1 \end{aligned}$$

Anfangssituation:

$$\left.\begin{array}{rr|l} 1 & 2 & 3 \\ -2 & -4 & 1 \end{array}\right.$$

Gaußsches Eliminationsverfahren

Schritt 1: Rechne "(Zeile 2) − (−2)·(Zeile 1)"

$$\begin{array}{cc|c} 1 & 2 & 3 \\ 0 & 0 & 7 \end{array}$$

Existenz der Lösung: Im unteren Block der Nullen ist das Element in der rechten Spalte ungleich Null (7). Daher existiert keine Lösung.

Gaußsches Eliminationsverfahren

Bemerkung:

Das Gaußsche Eliminationsverfahren kann *nicht* dazu benutzt werden, um diophantische Gleichungen zu lösen.

Dort sucht man nach Lösungen in den ganzen Zahlen $\mathbb{Z}$. Die ganzen Zahlen mit der Addition und Multiplikation bilden jedoch keinen Körper (fehlende multiplikative Inverse!).

Das Gaußsche Eliminationsverfahren ist jedoch für jeden beliebigen Körper (z.B. $(\mathbb{Z}_p, +_p, \cdot_p)$, p Primzahl) anwendbar.

Multiplikatives Inverses einer Matrix

Mit Hilfe des Gaußschen Eliminationsverfahrens kann man nun das multiplikative Inverse einer Matrix bestimmen.

Gegeben sei eine quadratische Matrix

$$A = \begin{pmatrix} A_{1,1} & \dots & A_{1,n} \\ \vdots & \ddots & \vdots \\ A_{n,1} & \dots & A_{n,n} \end{pmatrix}$$

Man stellt sich vor, dass das multiplikative Inverse A^{-1} aus Spaltenvektoren $\vec{a}_1, \dots, \vec{a}_n$ zusammengesetzt ist und schreibt $A^{-1} = \begin{pmatrix} \vec{a}_1 & \dots & \vec{a}_n \end{pmatrix}$.

(Siehe auch den Abschnitt über Erzeugendensysteme und Basen ▸ Invertierbare Matrizen und Basen.)

Multiplikatives Inverses einer Matrix

Damit A^{-1} das Inverse von A ist, muss gelten:

$$A \cdot A^{-1} = A \cdot \begin{pmatrix} \vec{a}_1 & \dots & \vec{a}_n \end{pmatrix} = \begin{pmatrix} A \cdot \vec{a}_1 & \dots & A \cdot \vec{a}_n \end{pmatrix}$$

$$= E_n = \begin{pmatrix} 1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & 1 \end{pmatrix} = \begin{pmatrix} \vec{e}_1 & \dots & \vec{e}_n \end{pmatrix}$$

Also gilt für jedes $i \in \{1, \dots, n\}$: $A \cdot \vec{a}_i = \vec{e}_i$

Dabei ist $\vec{e}_i$ der i-te Einheitsvektor.

Man muss also n Gleichungssysteme mit jeweils n Gleichungen lösen. Existieren für alle Gleichungssysteme Lösungen, so erhält man die Inverse A^{-1}. Anderenfalls gibt es keine Inverse.

Multiplikatives Inverses einer Matrix

Beispiel: wir bestimmen das multiplikative Inverse folgender Matrix

$$A = \begin{pmatrix} 3 & 4 \\ 1 & -3 \end{pmatrix}$$

Wir setzen zunächst $\vec{a}_1 = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ und lösen das Gleichungssystem $A \cdot \vec{a}_1 = \vec{e}_1$:

$$\begin{aligned} 3 \cdot x_1 + 4 \cdot x_2 &= 1 \\ x_1 - 3 \cdot x_2 &= 0 \end{aligned}$$

Das ergibt die Lösungen $x_1 = \frac{3}{13}$ und $x_2 = \frac{1}{13}$.

Multiplikatives Inverses einer Matrix

Wir setzen nun $\vec{a}_2 = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$ und lösen das Gleichungssystem $A \cdot \vec{a}_2 = \vec{e}_2$:

$$\begin{aligned} 3 \cdot y_1 + 4 \cdot y_2 &= 0 \\ y_1 - 3 \cdot y_2 &= 1 \end{aligned}$$

Das ergibt die Lösungen $y_1 = \frac{4}{13}$ und $y_2 = -\frac{3}{13}$.

Insgesamt erhält man folgende Matrix A^{-1}:

$$A^{-1} = \begin{pmatrix} \vec{a}_1 & \vec{a}_2 \end{pmatrix} = \begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \end{pmatrix} = \begin{pmatrix} \frac{3}{13} & \frac{4}{13} \\ \frac{1}{13} & -\frac{3}{13} \end{pmatrix}$$

Multiplikatives Inverses einer Matrix

Bemerkung (Gauß-Jordan-Verfahren):

Es gibt eine effizientere Methode um das Inverse einer Matrix zu bestimmen. Man kann insbesondere alle n Gleichungssysteme "gleichzeitig" lösen.

Dabei schreibt man die zu invertierende Matrix und die Einheitsmatrix wie folgt nebeneinander:

$$\left(\begin{array}{cc|cc} 3 & 4 & 1 & 0 \\ 1 & -3 & 0 & 1 \end{array}\right)$$

Dann formt man die linke Matrix durch Zeilentausch (nicht Spaltentausch!), indem man Zeilen mit einem Wert (ungleich 0) multipliziert und indem man Vielfache von Zeilen zu anderen Zeilen addiert, zur Einheitsmatrix um.
Die Matrix, die dabei rechts entsteht, ist dann die Inverse.

Schlussbemerkungen

Es gibt noch viele andere wichtige Gebiete im Zusammenhang mit algebraischen Strukturen, Vektorräumen und Matrizen:

- Ringe (Strukturen, die ähnlich zu Körpern sind, in denen aber weniger Gesetze gelten)
- Eigenvektoren und Eigenwerte
- Determinanten
- ...