Universität Karlsruhe (TH)
Forschungsuniversität gegründet 1825

Lineare Algebra

17. Oktober 2008

Prof. Enrico Leuzinger
Institut für Algebra und Geometrie, Universität Karlsruhe (TH)

Inhaltsverzeichnis

Teil I
Einführung

1 Gebrauchsanweisung für dieses Skript

Die Lehrveranstaltung *Lineare Algebra* hat drei Bestandteile:

- **Vorlesung**
- **Übung**
- **Tutorium**.

Die *Vorlesung* ist eine „Führung durch die Theorie“: der Lern-Stoff wird präsentiert, die Theorie erklärt und kommentiert.

Das *Skript* erspart Ihnen das Mitschreiben in der Vorlesung und schafft so Raum für das Mitdenken. Den größten Nutzen haben Sie, wenn Sie sich mit dem Abschnitt, der jeweils gerade in der Vorlesung behandelt wird, schon vorher vertraut machen (Zeitaufwand: 30-60 Minuten). In der Vorlesung können Sie dann gezielt Notizen machen oder Fragen stellen. Übrigens: Wenn Sie einen mathematischen Text (z.B. dieses Skript) „lesen“, sollten Sie das nicht passiv, sondern aktiv mit Stift und Papier tun. Notieren Sie sich Definitionen stichwortartig. Eine neue Definition können Sie sich viel besser merken, wenn Sie ein (möglichst einfaches) Beispiel/Gegenbeispiel dazu kennen. Notieren Sie sich auch diese Beispiele. Machen Sie Sich den Inhalt von (Lehr-)Sätzen ebenfalls immer an eigenen Beispielen klar. Rechnen Sie die Beispiele im Text selber durch.

In diesem Skript sind Definitionen, Beispiele und Sätze durchnummeriert. Das soll das Verweisen in der Vorlesung erleichtern: Sie werden jederzeit genau wissen, welche Stelle gerade besprochen wird.

Die *Übungen* dienen dazu, das Verständnis zu vertiefen und die Theorie auf konkrete (mathematische) Probleme anzuwenden. Wie beim Erlernen eines Instruments oder eines Handwerks gilt auch in der Mathematik: die Beherrschung dieser Wissenschaft ist nur durch konstante Anstrengung und eigene Aktivität möglich. Genau dazu sind die Übungen da. In den *Tutorien* besteht die Möglichkeit, in kleineren Gruppen gemeinsam zu üben, zu lernen und Erfahrungen auszutauschen.

2 How to solve it?

Das Lösen von (mathematischen) Problemen ist eine Kunst, die neben Erfolgserlebnissen auch mit Frustrationen verbunden ist. Gerade für Studienanfänger stellt sich immer wieder die Frage: *Wie findet man die Lösung einer Aufgabe?* Leider gibt es dafür kein Patentrezept. Wie so oft braucht es neben Talent auch Ausdauer und Erfahrung. Der Mathematiker Georg Polya hat sich dennoch überlegt, wie eine erfolgreiche Problemlösungs-Strategie aussehen könnte. Hier seine Tipps (vgl. [14]), die Ihnen vielleicht helfen, weiter zu kommen:

1. Vorbereitung: die Aufgabe verstehen.

- Verstehen Sie die Fragestellung? Kennen Sie die vorkommenden Begriffe und Konzepte?
- Was ist gesucht? Was ist gegeben? Wie lauten die Voraussetzungen oder Bedingungen, wie die Behauptung?
- Ist es möglich, die Bedingung zu befriedigen? Ist die Bedingung ausreichend, um die Unbekannte zu bestimmen? Oder genügt sie nicht? Ist sie eventuell sogar widersprüchlich?
- Zeichen Sie Figuren und machen Sie Skizzen! Führen Sie passende Bezeichnungen ein!
- Trennen Sie die verschiedenen Teile der Voraussetzung! Können Sie sie hinschreiben?

2. Brainstorming: Einen Zusammenhang zwischen Gegebenem und Gesuchtem finden und einen Plan für die Lösung ausdenken.

- Haben Sie die Aufgabe schon früher gesehen? Oder haben Sie dasselbe Problem in einer ähnlichen Form gesehen?
- Kennen Sie eine verwandte Aufgabe? Kennen Sie einen Lehrsatz, der hilfreich sein könnte?
- Betrachten Sie die Voraussetzungen! Versuchen Sie, sich auf eine Ihnen bekannte Aufgabe zu besinnnen, die dieselben oder ähnliche Voraussetzungen hatte.
- Hier ist eine Aufgabe, die der Ihren verwandt ist und deren Lösung Sie kennen. Können Sie ihre Methode verwenden? Würden Sie irgend ein Hilfsmittel einführen, damit Sie sie verwenden können?
- Können Sie die Aufgabe anders ausdrücken? Können Sie sie auf noch verschiedenere Weise ausdrücken? Gehen Sie auf die Definition zurück!

- Wenn Sie die vorliegende Aufgabe nicht lösen können, so versuchen Sie, zuerst eine verwandte Aufgabe zu lösen. Können Sie Sich eine zugänglichere, verwandte Aufgabe denken? Eine allgemeinere Aufgabe? Eine analoge Aufgabe? Können Sie einen Teil der Aufgabe lösen? Behalten Sie nur einen Teil der Bedingungen bei und lassen Sie den andern weg; wie weit ist die Unbekannte/Behauptung dann bestimmt, wie kann man sie verändern? Können Sie etwas Nützliches aus den Daten ableiten? Können Sie sich andere Daten denken, die geeignet sind, die Unbekannte zu bestimmen? Können Sie die Unbekannte ändern oder die Daten oder, wenn nötig, beides, so dass die neue Unbekannte und die neuen Daten einander näher sind?

- Haben Sie alle Daten benutzt? Haben Sie die ganze Bedingung benutzt? Haben Sie alle wesentlichen Begriffe in Betracht gezogen, die in der Aufgabe enthalten sind?

3. Ausarbeitung und Kontrolle: Den Plan ausführen und die Lösung prüfen.

- Wenn Sie Ihren Plan der Lösung durchführen, so kontrollieren Sie jeden Schritt. Können Sie deutlich sehen, dass der Schritt richtig ist? Können Sie beweisen, dass er richtig ist?

- Können Sie das Resultat kontrollieren? Können Sie den Beweis kontrollieren?

- Können Sie das Resultat auf verschiedene Weise ableiten? Können Sie es auf den ersten Blick sehen?

- Können Sie das Resultat oder die Methode für irgend eine andere Aufgabe gebrauchen?

3 Was ist lineare Algebra?

Die Frage „Was ist Mathematik?“ ist schwierig zu beantworten und verschiedene Mathematiker haben verschiedene Antworten gegeben. Ein (etwas verstaubter) Klassiker ist Courant-Robbins [4]. Moderner und spannender sind Devlin [6] und Davis-Hersh [5]. Siehe auch Gowers [9] und Otte [13]. Gegenüber anderen Wissenschaften zeichnen sich die Begriffssysteme und Theorien, die in der Mathematik entwickelt werden, durch drei spezifische Merkmale aus:

1. **Abstraktheit**: Gegenstand der Mathematik sind Systeme von Objekten mit fixierten strukturellen Beziehungen untereinander. Diese Strukturen oder Muster stehen im Vordergrund; von allen weiteren Eigeschaften der Objekte wird abgesehen (abstrahiert).

2. **Genauigkeit**: Ist eine mathematische Struktur (axiomatisch) fixiert, so sind alle Aussagen über diese Struktur durch formales, logisches Schließen aus den einmal gemachten Annahmen ableitbar. Wie man das konkret macht, ist allerdings eine

Kunst, die neben dem Beherrschen der mathematischen Techniken vor allem Intuition und Einsicht in das Wesen der Sache erfordert (also etwas ganz anderes als Logik); siehe dazu z.B. die Bücher von Hadamard [10] und Ruelle [15].

3. **Allgemeinheit**: Ausgangspunkt für den Abstraktionsprozess und die Entwicklung einer mathematischen Struktur ist zwar oft ein konkretes (z.B. physikalisches) Problem oder Phänomen. Alle Aussagen, die über eine Struktur gewonnen werden, sind aber später in allen Situationen anwendbar, in denen Strukturen mit den gleichen Bedingungen vorliegen. Darauf beruht die universelle Anwendbarkeit und Effizienz von Mathematik in andern Wissenschaften.

Diese Besonderheiten sind natürlich auch ein Grund dafür, weshalb das Erlernen von Mathematik nicht so ganz einfach ist.

Wie die Frage „Was ist Mathematik?“ lässt sich auch die Frage „Was ist lineare Algebra?“ zu Beginn des Studiums nur sehr unvollständig und vage beantworten; etwa so: „Lineare Algebra ist die Theorie linearer Gleichungssysteme“. In diesem einleitenden Kapitel begegnen wir solchen Gleichungen, einem grundlegenden Konzept dieser Vorlesung, zum ersten Mal. Am Ende dieses Teils sollten Sie dann wissen, was lineare Gleichungssysteme sind und wie man diese systematisch lösen kann.

3.1 Lineare Gleichungen: Beispiele

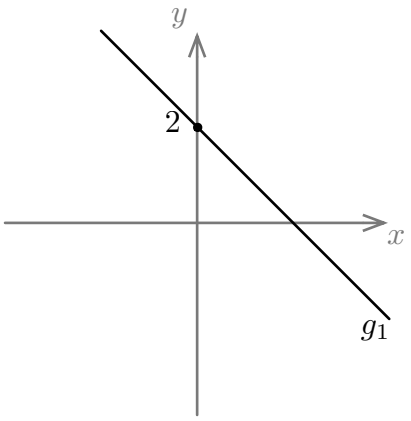
In der Mathematik treten Gleichung in verschiedender Form auf. So sind etwa **Identitäten** allgemeingültig:

- Für den Umfang U eines Kreises vom Radius R gilt immer $U = 2\pi R$.
- Für ein rechtwinkliges Dreieck mit Kathetenlängen a, b und Hypothenusenlänge c gilt immer der Satz von Pythagoras $a^2 + b^2 = c^2$.
- Für die Zahlen $0, 1, e, \pi$ und die imaginäre Einheit $\mathrm{i} = \sqrt{-1}$ gilt die Eulersche Identität $\mathrm{e}^{\pi \mathrm{i}} + 1 = 0$.

Dagegen gelten **Bestimmungsgleichungen** jeweils nur für gewisse Werte, eben die **Lösungen**, aus einer vorgegebenen Grundmenge:

- $x^2 = 2$ hat keine Lösung in der Grundmenge der natürlichen Zahlen $\mathbb{N} = \{1, 2, 3, \ldots\}$, aber die Lösungen $+\sqrt{2}$ und $-\sqrt{2}$ in der Grundmenge $\mathbb{R}$ der reellen Zahlen.
- $x^2 + y^2 = 1$ gilt für alle Punkte (x, y) auf dem Kreis mit Radius 1 und Zentrum $(0, 0)$ in der xy-Ebene.

Zentraler Gegenstand der linearen Algebra sind Bestimmungsgleichungen von relativ einfacher Bauart, sogenannte **lineare Gleichungen**, wie etwa $x + y = 2$. Geometrisch ist die Menge der Lösungen dieser Gleichung die Gerade g_1 in der xy-Ebene.



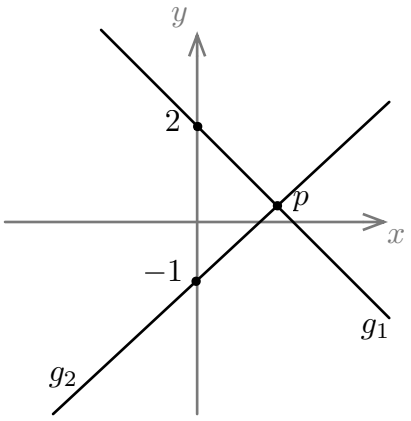
Solche Gleichungen treten in vielen alltäglichen Situationen auf. Zum Beispiel bei der Frage: In welchem Verhältnis muss man eine 20%-ige Lösung und eine 70%-ige Lösung mischen, um eine 30%-ige Lösung zu erhalten?

Ein **(lineares) Gleichungssystem** besteht aus mehreren linearen Gleichungen.

Das Gleichungssystem

$$x + y = 2 \tag{3.1}$$
$$x - y = 1 \tag{3.2}$$

beschreibt die Geraden $g_1$und g_2.



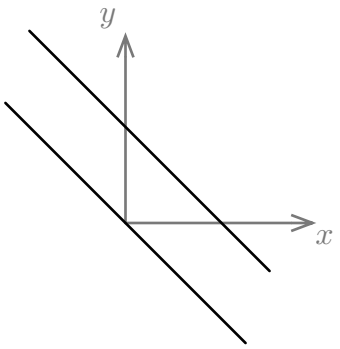
Die Lösungsmenge ist die Menge aller Punkte der xy-Ebene, die simultan beide Gleichungen erfüllen, also sowohl auf g_1 als auch auf g_2 liegen. Aus der Abbildung sieht man, dass die Lösungsmenge $\mathcal{L}$ nur aus dem Punkt p besteht: $\mathcal{L} = \{p\}$.

Um p zu bestimmen, kann man formal so vorgehen: Aus (3.2) folgt $y = x - 1$. Eingesetzt in (3.1) erhalten wir $x + (x - 1) = 2$, also $2x = 3$ oder $x = \frac{3}{2}$ und damit $y = x - 1 = \frac{3}{2} - 1 = \frac{1}{2}$, d.h. $p = (\frac{3}{2}, \frac{1}{2})$.

Zwei Gerade in der Ebene können auch parallel sein, z.B. sind

$$\begin{aligned} x + y &= 2 \\ x + y &= 0 \end{aligned}$$

parallel.



Es gibt also keine Schnittpunkte, was wiederum bedeutet, dass das Gleichungssystem *keine* Lösung hat: $\mathbb{L} = \emptyset$.

Für das System

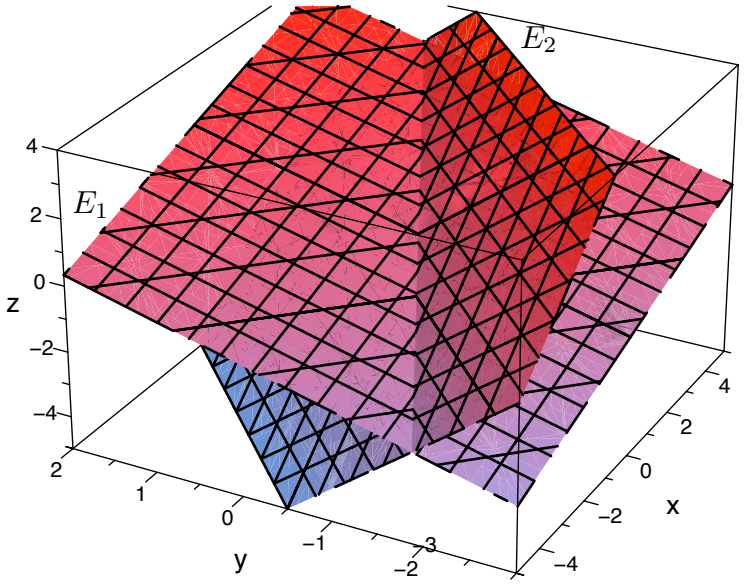
$$\begin{aligned} x + y &= 2 \\ 3x + 3y &= 6 \end{aligned}$$

fallen beide Geraden zusammen und alle Punkte der Geraden sind „Schnittpunkte“: das Gleichungssystem hat unendlich viele Lösungen.

Anstatt lineare Gleichungen mit *zwei* Unbekannten (oder Variablen) können wir natürlich auch solche mit *drei* Unbekannten x, y und z betrachten, etwa

$$x + y + z = -6 \tag{3.3}$$
$$x + 2y + 3z = -10. \tag{3.4}$$

Geometrisch sind das zwei Ebenen im xyz-Raum.



Aus der Abbildung sieht man, dass sich diese Ebenen in einer Geraden schneiden.

Wie kann man diese Schnittgerade, also die Lösungsmenge des Systems (3.3) und (3.4), formal bestimmen?

Aus (3.4) folgt $x = -2y-3z-10$, in (3.3) eingesetzt also $(-2y-3z-10)+y+z = -6$ oder vereinfacht $-y-2z = 4$, also $y = -2z-4$ und $x = -2(-2z-4)-3z-10 = z-2$. Dabei ist die Variable z beliebig wählbar. Wir erhalten eine **Parametrisierung** der Lösungsmenge (oder, geometrisch, der Schnittgeraden):

$$\mathcal{L} = \{(t-2,\ -2t-4,\ t) \mid t \text{ eine beliebige reelle Zahl}\}.$$

Zwei Ebenen können auch parallel sein. Das Gleichungssystem hat dann keine Lösung, d.h. $\mathcal{L} = \emptyset$, z.B.

$$\begin{aligned} x+y+z &= -6 \\ x+y+z &= 0. \end{aligned}$$

Oder die Ebenen können zusammenfallen und man hat unendlich viele Lösungen, z.B.

$$\begin{aligned} x+y+z &= -6 \\ -x-y-z &= 6. \end{aligned}$$

Damit man genau eine Lösung (also, geometrisch, genau einen Schnittpunkt) erhält, benötigt man drei Ebenen, z.B. hat

$$\begin{aligned} x + y + z &= -6 \\ x + 2y + 3z &= -10 \\ 2x + 3y + 6z &= -18 \end{aligned}$$

die Lösungsmenge $\mathcal{L} = \{(-3, -2, -1)\}$.

In der Praxis hat man es oft mit linearen Gleichungssystemen mit sehr vielen (z.B. 200) Unbestimmten zu tun und es stellt sich die Frage, ob, und wenn ja, wie man solche Systeme lösen kann. Ziel der linearen Algebra ist es deshalb, die allgemeinen Strukturen, die solchen linearen Gleichungssystemen zugrunde liegen, zu finden und systematisch zu analysieren. Dazu machen wir einen (in der Mathematik typischen) allgemeinen Ansatz.

3.2 Lineare Gleichungensysteme: allgemein

In den vorhergehenden Beispielen konnten wir die Lösungen der Gleichungssysteme mit zwei Unbestimmten x, y bzw. drei Unbestimmten x, y, z geometrisch als Punkte in der „Ebene“ $\mathbb{R}^2$ bzw. im „Raum“ $\mathbb{R}^3$ auffassen. Für Gleichungssysteme mit n Unbestimmten $x_1, \ldots, x_n$ definieren wir den reellen **Standardraum** $\mathbb{R}^n$ als die Menge aller reellen n-Tupel,

$$\mathbb{R}^n = \{(x_1, \ldots, x_n) \mid x_1, \ldots, x_n \in \mathbb{R}\}.$$

Die (rellen) Lösungen für Gleichungssysteme in n Unbestimmten sind dann Elemente oder Punkte im Standardraum $\mathbb{R}^n$.

Definition 3.1 Ein **lineares Gleichungssystem** (LGS) mit m Gleichungen und n Unbestimmten $x_1, \ldots, x_n$ ist gegeben durch

$$\begin{array}{ccccccccc} a_{11}x_1 & + & a_{12}x_2 & + & \ldots & + & a_{1n}x_n & = & b_1 \\ a_{21}x_1 & + & a_{22}x_2 & + & \ldots & + & a_{2n}x_n & = & b_2 \\ \vdots & & \vdots & & & & \vdots & & \vdots \\ a_{m1}x_1 & + & a_{m2}x_2 & + & \ldots & + & a_{mn}x_n & = & b_m \end{array} \tag{3.5}$$

Die a_{ij}, b_i für $i = 1, \ldots, m$ und $j = 1, \ldots, n$ heißen **Koeffizienten** und sind gegebene reelle Zahlen. Die x_j für $j = 1, \ldots, n$ heißen **Unbestimmte** (oder **Unbekannte** oder **Variablen**) und sind gesucht.

Sind in (3.5) alle $b_i = 0$ $(i = 1, \ldots, m)$, so heißt das LGS **homogen**, und sonst **inhomogen**.

Definition 3.2 Die **Lösungsmenge** des reellen linearen Gleichungssystems (3.5) ist die Teilmenge $\mathcal{L}$ von $\mathbb{R}^n$ bstehend aus allen n-Tupeln $(x_1, \ldots, x_n)$, die bei gegebenen Koeffizienten a_{ij}, b_i ($i = 1, \ldots, m$ und $j = 1, \ldots, n$) alle m Gleichungen in (3.5) simultan erfüllen.

Wie soll man nun vorgehen, um Lösungen des LGS (3.5) zu finden? Dazu definieren wir zunächst einfache Manipulationen des Systems:

Definition 3.3 Elementar-Operationen für das LGS (3.5) sind Umformungen der folgenden Art

(I) Vertauschen von zwei Gleichungen.

(II) Ersetzen einer Gleichung durch ihr λ-faches mit $\lambda \in \mathbb{R}$ und $\lambda \neq 0$.

(III) Ersetzen der i-ten Gleichung durch die Summe der i-ten und dem λ-fachen der j-ten Gleichung ($i \neq j$, $\lambda \in \mathbb{R}$).

Die Nützlichkeit dieser Umformungen liegt in folgender Tatsache

Satz 3.4 *Die Lösungsmenge $\mathcal{L}$ des LGS (3.5) wird bei einer Elementar-Operation nicht geändert.*

Wie immer in der Mathematik muss man eine solche Behauptung *beweisen*!

Beweis: Es reicht zu zeigen, dass eine einzige Zeilenumformung vom Typ (I), (II) oder (III) die Lösungsmenge nicht ändert, denn dann ändern auch wiederholte derartige Umformungen nichts.

Für Typ (I) ist dies klar, denn die Reihenfolge der Gleichungen ändert nichts an der Tatsachen, dass alle simultan erfüllt sein müssen.

Typ (II): Erfüllt $x = (x_1, \ldots, x_n)$ die Gleichung

$$a_{i1}x_1 + \cdots + a_{in}x_n = b_i,$$

so auch

$$\lambda a_{i1}x_1 + \cdots + \lambda a_{in}x_n = \lambda b_i.$$

Gilt umgekehrt für $x = (x_1, \ldots, x_n)$ die Gleichung

$$\lambda a_{i1}x_1 + \cdots + \lambda a_{in}x_n = \lambda b_i,$$

so kann man durch λ dividieren (hier braucht man $\lambda \neq 0$) und sieht, dass $x = (x_1, \ldots, x_n)$ auch die ursprüngliche Gleichung

$$a_{i1}x_1 + \cdots + a_{in}x_n = b_i$$

erfüllt.

Bei einer Umformung vom Typ (III) sind nur die Gleichungen i und j betroffen. Daher genügt es, zu zeigen, dass die beiden Systeme

$$\begin{array}{rcrcrcrcl} a_{i1}x_1 & + & a_{i2}x_2 & + & \dots & + & a_{in}x_n & = & b_i \\ a_{j1}x_1 & + & a_{j2}x_2 & + & \dots & + & a_{jn}x_n & = & b_j \end{array} \qquad (*)$$

und

$$\begin{array}{rcrcrcrcl} a_{i1}x_1 & + & a_{i2}x_2 & + & \dots & + & a_{in}x_n & = & b_i \\ (a_{j1}+\lambda a_{i1})x_1 & + & (a_{j2}+\lambda a_{i2})x_2 & + & \dots & + & (a_{jn}+\lambda a_{in})x_n & = & b_j+\lambda b_i \end{array} \qquad (**)$$

die gleiche Lösungsmenge haben. Erfüllt aber $x = (x_1, \dots, x_n)$ die Gleichungen $(*)$, so erfüllt x auch die erste Gleichung von $(**)$. Durch Addition des λ-fachen der ersten Gleichung von $(*)$ zur zweiten Gleichung folgt, dass x auch die zweite Gleichung von $(**)$ erfüllt. Umgekehrt folgt durch Subtraktion des λ-fachens der ersten Gleichung aus $(**)$ von der zweiten aus $(**)$ auch die zweite Gleichung von $(*)$. Damit folgt, dass ein x, das $(*)$ erfüllt auch $(**)$ erfüllt. ■

Nach Satz 3.4 kann man (mindestens im Prinzip) ein „kompliziertes“ LGS in ein „einfacheres“ umformen.

3.3 Wie man ein LGS lösen kann: Der Gaußsche Algorithmus

Ein systematisches Verfahren (Algorithmus) zur Lösung eines allgemeinen linearen Gleichungssystems geht auf Carl Friedrich Gauß (1777-1855) zurück. Das Prinzip war aber chinesischen Mathematikern schon vor mehr als 2000 Jahren bekannt.

3.3.1 Zuerst ein Beispiel

Wir führen das Gaußsche Verfahren zunächst anhand von Beispielen vor.

Beispiel 3.5 Wir betrachten folgendes reelles LGS, das einen Parameter $a \in \mathbb{R}$ enthält.

$$\begin{array}{rcrcrcrcr} x_1 & + & x_2 & - & 3x_3 & + & x_4 & = & 1 \\ 2x_1 & + & x_2 & + & x_3 & - & x_4 & = & 0 \\ & & 2x_2 & - & 13x_3 & + & x_4 & = & -1 \\ 2x_1 & - & x_2 & + & 14x_3 & - & 2x_4 & = & a \end{array}$$

1. Schritt: Wir addieren das (-2)-fache der ersten Gleichung zur zweiten und vierten

Gleichung und erhalten

$$\begin{array}{rcrcrcrl} x_1 & + & x_2 & - & 3x_3 & + & x_4 & = & 1 & \leftarrow +\\ & - & x_2 & + & 7x_3 & - & 3x_4 & = & -2 & \leftarrow 2,\ -3\\ & & 2x_2 & - & 13x_3 & + & x_4 & = & -1 & \leftarrow +\\ & - & 3x_2 & + & 20x_3 & - & 4x_4 & = & a-2 & \leftarrow +\end{array}$$

2. Schritt: Wir addieren die oben angegebenen Vielfachen der zweiten Gleichung zu den anderen Gleichungen und multiplizieren die zweite Gleichung schließlich noch mit -1:

$$\begin{array}{rcrcrcrl} x_1 & & + & 4x_3 & - & 2x_4 & = & -1 & \leftarrow +\\ & x_2 & - & 7x_3 & + & 3x_4 & = & 2 & \leftarrow +\\ & & & x_3 & - & 5x_4 & = & -5 & -4,\ 7\\ & & - & x_3 & + & 5x_4 & = & a+4 & \leftarrow +\end{array}$$

3. Schritt: Wir addieren die angegebenen Vielfachen der dritten Gleichung zu den anderen Gleichungen:

$$\begin{array}{rcrcrcl} x_1 & & & + & 18x_4 & = & 19\\ & x_2 & & - & 32x_4 & = & -33\\ & & x_3 & - & 5x_4 & = & -5\\ & & & & 0x_4 & = & a-1\,. \end{array}$$

Damit ist das Verfahren beendet. Nach Satz 3.4 hat das LGS, von dem wir ausgegangen sind, dieselbe Lösungsmenge wie das zuletzt erhaltene LGS. Aus der letzten Gleichung ergibt sich, dass das LGS für $a \neq 1$ *unlösbar* ist. Für $a = 1$ ist das LGS *lösbar*; die Lösungsmenge lässt sich aus

$$\begin{aligned} x_1 &= 19 - 18x_4\\ x_2 &= -33 + 32x_4\\ x_3 &= -5 + 5x_4 \end{aligned}$$

unmittelbar ablesen. Man sieht, dass x_4 beliebig wählbar ist, während x_1, x_2, x_3 nach Wahl von x_4 eindeutig bestimmt sind. Schreiben wir noch t anstelle von x_4, so lässt sich jedes Element x der Lösungsmenge $\mathcal{L}$ folgendermaßen darstellen:

$$(x_1, x_2, x_3, x_4) = (19, -33, -5, 0) + t(-18, 32, 5, 1)$$

oder

$$x = u + t\,v, \qquad t \in \mathbb{R}.$$

Beobachtung: $u = (19, -33, -5, 0)$ ist eine Lösung des LGS und $v = (-18, 32, 5, 1)$ eine Lösung des zugehörigen homogenen LGS.

3.3.2 Die wesentlichen Daten: Matrizen

Die durchgeführten Elementaroperationen verändern lediglich die Koeffizienten des LGS. Wenn also die Zugehörigkeit der Koeffizienten zu den Variablen klar ist, kann man sich das Schreiben der Variablen $x_1, \ldots, x_n$ ersparen. Zu diesem Zweck führen wir die ökonomische Matrixschreibweise ein.

Definition 3.6 Eine **Matrix** mit m **Zeilen** und n **Spalten** ist ein rechteckiges Schema von m mal n Zahlen a_{ij} mit $i = 1, \ldots, m$ und $j = 1, \ldots, n$ der Form

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

Merkregel für die Reihenfolge der Indizes: **Z**eile **z**uerst, **Sp**alte **sp**äter.

Einem linearen Gleichungssystem kann man wie folgt eine Matrix zuordnen: Im „Schnittpunkt“ der i-ten Zeile mit der j-ten Spalte hat die **Matrix des LGS** (3.5) den Eintrag a_{ij}.

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}. \tag{3.6}$$

Die **erweiterte Matrix des LGS** (3.5) enthält als letzte Spalte zusätzlich $b_1, \ldots, b_m$:

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_m \end{pmatrix}. \tag{3.7}$$

Beispiel 3.7 Wir betrachten das reelle LGS

$$\begin{array}{rcrcrcrcrcr} & & 2x_2 & + & 4x_3 & - & 2x_4 & + & x_5 & + & 7x_6 & = & -1 \\ x_1 & & & + & x_3 & + & 3x_4 & & & - & x_6 & = & 1 \\ x_1 & + & x_2 & + & 3x_3 & + & 2x_4 & & & + & x_6 & = & 1 \\ & & x_2 & + & 2x_3 & - & x_4 & - & x_5 & - & x_6 & = & 1 \\ 3x_1 & + & 2x_2 & + & 7x_3 & + & 7x_4 & - & x_5 & - & 2x_6 & = & a \end{array}$$

mit der erweiterten Matrix

$$\begin{pmatrix} 0 & 2 & 4 & -2 & 1 & 7 & -1 \\ 1 & 0 & 1 & 3 & 0 & -1 & 1 \\ 1 & 1 & 3 & 2 & 0 & 1 & 1 \\ 0 & 1 & 2 & -1 & -1 & -1 & 1 \\ 3 & 2 & 7 & 7 & -1 & -2 & a \end{pmatrix}$$

1. Schritt: Wir addieren das (-1)-fache der zweiten Gleichung (bzw. Matrix-Zeile) zur dritten und das (-3)-fache der zweiten Gleichung (bzw. Matrix-Zeile) zur letzten. Schließlich vertauschen wir noch die ersten beiden Gleichungen, damit die Eins links oben steht, und erhalten folgende Matrix:

$$\begin{pmatrix} 1 & 0 & 1 & 3 & 0 & -1 & 1 \\ 0 & 2 & 4 & -2 & 1 & 7 & -1 \\ 0 & 1 & 2 & -1 & 0 & 2 & 0 \\ 0 & 1 & 2 & -1 & -1 & -1 & 1 \\ 0 & 2 & 4 & -2 & -1 & 1 & a-3 \end{pmatrix}$$

2. Schritt: Wir addieren die angegebenen Vielfachen der dritten Gleichung zur zweiten, vierten und fünften Gleichung. Dann vertauschen wir noch die zweite und dritte Gleichung, damit die Eins links oben im „Kästchen“ steht, und erhalten

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

3. Schritt: Wegen den Nullen in der dritten und vierten Spalte können wir die dritte und vierte Variable überspringen. Wir addieren die dritte Gleichung zur vierten und fünften Gleichung und bekommen

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

Das Verfahren ist damit beendet. Das zugehörige LGS

$$\begin{array}{rcrcrcrcl} x_1 & & + & x_3 & + & 3x_4 & & - & x_6 & = & 1 \\ & x_2 & + & 2x_3 & - & x_4 & & + & 2x_6 & = & 0 \\ & & & & & & x_5 & + & 3x_6 & = & -1 \\ & & & & & & & & 0x_6 & = & 0 \\ & & & & & & & & 0x_6 & = & a-4 \end{array}$$

hat dieselbe Lösungsmenge wie das Ausgangssystem und ist für $a \neq 4$ *unlösbar*, für $a = 4$ *lösbar*. Die Lösungsmenge lässt sich (für $a = 4$) aus

$$\begin{array}{rcrcrcrcr} x_1 & = & 1 & - & x_3 & - & 3x_4 & + & x_6 \\ x_2 & = & & - & 2x_3 & + & x_4 & - & 2x_6 \\ x_5 & = & -1 & & & & & - & 3x_6 \end{array}$$

ablesen: Setzen wir $x_3 = t_1$, $x_4 = t_2$, $x_6 = t_3$, so bekommt man

$$\begin{array}{rcrcrcrcr} x_1 & = & 1 & - & t_1 & - & 3t_2 & + & t_3 \\ x_2 & = & & - & 2t_1 & + & t_2 & - & 2t_3 \\ x_3 & = & & & t_1 & & & & \\ x_4 & = & & & & & t_2 & & \\ x_5 & = & -1 & & & & & - & 3t_3 \\ x_6 & = & & & & & & & t_3 \end{array} ,$$

und die Lösungsmenge besteht aus allen Elementen $x = (x_1, \ldots, x_6) \in \mathbb{R}^6$, die sich darstellen lassen als

$$x = u + t_1\, v_1 + t_2\, v_2 + t_3\, v_3 \quad \text{mit} \quad t_1, t_2, t_3 \in \mathbb{R}$$

mit

$$u = (1, 0, 0, 0, -1, 0), \quad v_1 = (-1, -2, 1, 0, 0, 0),$$

$$v_2 = (-3, 1, 0, 1, 0, 0), \quad v_3 = (1, -2, 0, 0, -3, 1).$$

3.3.3 Das allgemeine Vorgehen

Gegeben sei das relle LGS (3.5) mit $m, n \in \mathbb{N}$ und reellen Koeffizienten a_{ik}, b_i und der erweiterten Matrix (3.7).

Ziel ist es, die erweiterte Matrix $(A \mid b)$ durch elementare Zeilenoperationen möglichst zu vereinfachen, d.h. möglichst viele Einträge zu Null (oder Eins) zu machen.

Der Fall, dass alle a_{ik} Null sind, ist uninteressant: Dann ist nämlich entweder (3.5) unlösbar (falls es ein $b_i \neq 0$ gibt), oder die Lösungsmenge ist $\mathbb{R}^n$ (falls alle $b_i = 0$ sind). Wir werden also im Folgenden annehmen, dass es mindestens ein $a_{ik} \neq 0$ gibt.

1. Schritt: Ist ein Element a_{i1} in der ersten Spalte von (3.5) von Null verschieden, so lässt sich (nötigenfalls durch eine Vertauschung (I)) erreichen, dass $a_{11} \neq 0$. Weiter kann man durch Elementaroperationen (II) und (III) erreichen, dass $a_{11} = 1$ und $a_{i1} = 0$: Man multipliziert dazu die 1. Zeile mit $\frac{1}{a_{11}}$ und addiert zur i-ten Zeile das $-a_{i1}$-fache der ersten Zeile ($i = 2, \ldots, m$). Sind dagegen alle Elemente der ersten Spalte Null und kommt in der k-ten Spalte zum ersten Mal ein von Null verschiedenes

Element vor, so kann man entsprechend $a_{1k} = 1$, $a_{ik} = 0 \quad (i = 2, \ldots, m)$ erreichen. (3.5) geht somit im ersten Schritt über in

$$\begin{pmatrix} 0 & \cdots & 0 & 1 & a'_{1,k+1} & \cdots & a'_{1n} & b'_1 \\ \vdots & & \vdots & 0 & a'_{2,k+1} & \cdots & a'_{2n} & b'_2 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & \cdots & 0 & 0 & a'_{m,k+1} & \cdots & a'_{mn} & b'_m \end{pmatrix}. \tag{3.8}$$

2. Schritt: Ist mindestens eins der a'_{ij} mit $i \geq 2$ und $j \geq k+1$ von Null verschieden, so verfährt man wie beim ersten Schritt und erhält eine erweiterte Matrix der Form

$$\begin{pmatrix} 0 & \cdots & 0 & 1 & * & \cdots & * & * & * & \cdots & * & * \\ \vdots & & \vdots & 0 & 0 & \cdots & 0 & 1 & * & \cdots & * & * \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & 0 & * & \cdots & * & * \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & * & \cdots & * & * \end{pmatrix}. \tag{3.9}$$

Gibt es noch von Null verschiedene Koeffizienten in den Zeilen $3, 4, \ldots$ (mit Ausnahme der Elemente in der letzten Spalte), so folgt in entsprechender Weise ein **3. Schritt** usw.

Das Verfahren ist beendet, wenn entweder in den letzten Zeilen nur noch Nullen stehen (bis auf die Elemente in der letzten Spalte) oder wenn man mit der zuletzt erhaltenen Eins die letzte Spalte oder Zeile der einfachen (d.h. nicht erweiterten) Matrix erreicht hat. Die Endgestalt der Matrix hat schließlich folgende **Zeilen-Stufen-Form**:

$$\left(\begin{array}{ccc|cccccccccc|c} 0 & \cdots & 0 & 1 & * & \cdots & * & * & * \cdots * & * & * & \cdots & * & c_1 \\ \vdots & & \vdots & 0 & 0 & \cdots & 0 & 1 & * \cdots * & \vdots & \vdots & & \vdots & \vdots \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & 0 & \ddots & * & \vdots & & \vdots & \vdots \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & \ddots & 1 & * & \cdots & * & c_r \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & & 0 & 0 & \cdots & 0 & c_{r+1} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & c_m \end{array}\right). \tag{3.10}$$

Aus (3.10) liest man ab:

Folgerung 3.8 *Das zu (3.10) gehörige LGS und damit nach Satz 3.4 auch das LGS (3.5) ist genau dann lösbar, wenn gilt* $c_{r+1} = c_{r+2} = \ldots = c_m = 0$.

Durch weitere Zeilenumformungen kann man erreichen, dass oberhalb der Einsen überall Nullen stehen. So erhält man schließlich die **Gaußsche Normalform** des LGS (3.5):

$$\left(\begin{array}{ccc|ccccc|cccc|c} 0 & \cdots & 0 & 1 & * & \cdots & * & 0 & * \cdots * & 0 & * & \cdots & * & d_1 \\ \vdots & & \vdots & 0 & 0 & \cdots & 0 & 1 & * \cdots * & \vdots & \vdots & & \vdots & \vdots \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & 0 & \ddots & 0 & \vdots & & \vdots & \vdots \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & \ddots & 1 & * & \cdots & * & d_r \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & & 0 & 0 & \cdots & 0 & d_{r+1} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & d_m \end{array}\right). \tag{3.11}$$

Parametrisierung der Lösungsmenge: Falls das zu (3.11) bzw. (3.5) gehörige LGS lösbar ist (also $d_{r+1} = \ldots = d_m = 0$), so lassen sich alle Lösungen von (3.5) an (3.11) ablesen.

Um die Darstellung zu vereinfachen, nehmen wir an, dass die Gaußsche Normalform folgende Gestalt hat

$$\left(\begin{array}{ccccc|ccc|c} 1 & 0 & 0 & \cdots & 0 & a''_{1,r+1} & \cdots & a''_{1,n-r} & d_1 \\ 0 & 1 & 0 & & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 1 & & \vdots & \vdots & & \vdots & \vdots \\ \vdots & & & \ddots & & \vdots & & \vdots & \vdots \\ 0 & & & 0 & 1 & a''_{r,r+1} & & a''_{r,n-r} & d_r \\ \vdots & & & \vdots & 0 & 0 & \cdots & 0 & 0 \\ \vdots & & & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & \cdots & \cdots & 0 & 0 & 0 & \cdots & 0 & 0 \end{array}\right). \tag{3.12}$$

Durch eine Umordnung der Spalten von A, d.h. eine andere Numerierung der Unbekannten des LGS, kann man das stets erreichen.

Man wählt dann (wie im Beispiel) $t_1, \ldots, t_{n-r} \in \mathbb{R}$ als **Parameter** und setzt

$$x_{r+1} := t_1,\ x_{r+2} := t_2,\ \ldots,\ x_n := t_{n-r}.$$

Aus (3.12) erhält man dann für die restlichen r Unbekannten:

$$\begin{array}{rcl} x_1 &=& d_1 - t_1\, a''_{1,r+1} - \cdots - t_{n-r}\, a''_{1,n-r} \\ &\vdots& \\ x_r &=& d_r - t_1\, a''_{r,r+1} - \cdots - t_{n-r}\, a''_{r,n-r} \\ x_{r+1} &=& t_1 \\ &\vdots& \qquad\qquad \ddots \\ x_n &=& t_{n-r} \end{array} \tag{3.13}$$

Durchlaufen $t_1, \ldots, t_{n-r}$ jeweils alle reellen Zahlen, so erhält man mit (3.13) alle Lösungen von (3.5). Für $t_1 = \ldots = t_{n-r} = 0$ ergibt sich speziell die Lösung $x = (d_1, \ldots, d_r, 0, \ldots, 0)$.

Folgerung 3.9 *Ein homogenes LGS mit mehr Unbekannten als Gleichungen ($n > m$) ist immer nichttrivial lösbar (d.h. hat nicht nur die Null-Lösung).*

3.4 Einige weiterführende Fragen

- Wir haben in diesem Abschnitt bereits die Begriffe Menge, Teilmenge, Lösungsmenge verwendet und sind „intuitiv“ damit umgegangen. Wie lassen sich diese Begriffe präzisieren, welche Schreibweisen gibt es dafür und welche Operationen kann man mit Mengen ausführen?

- Wie kann man das logische Schließen (etwa im Beweis von Satz 3.4) systematisieren und übersichtlich darstellen? Was für logische Operationen gibt es? Was für Beweis-Methoden gibt es?

- Gibt es noch weitere „Zahlbereiche“, mit denen man formal wie mit den reellen oder den rationalen Zahlen rechnen kann?

- Kann man herausfinden, ob ein gegebenes lineares Gleichungssystem eine Lösung hat, ohne den Gaußschen Algorithmus durchzuführen? Kann man a priori etwas über die mögliche Anzahl der Lösungen sagen? (Gibt es z.B. ein LGS, dessen Lösungsmenge genau zwei Elemente enthält?)

- Was sind die algemeinen Eigenschaften (Struktur) der Lösungsmenge eines LGS?

Teil II
Grundlegende Begriffe

In diesem Kapitel führen wir einige Begiffe und Bezeichnungen ein, die nicht nur für die Lineare Algebra, sondern für die gesamte Mathematik grundlegend sind: *Logische Begriffe* sind unentbehrlich, um mathematische Aussagen präzise zu fassen und neue deduktiv herzuleiten. Die Objekte der Mathematik lassen sich zweckmäßig als *Mengen* beschreiben. Mittels *Abbildungen* kann man Beziehungen zwischen einzelnen Mengen beschreiben.

Unser Ziel ist eine kurze Vorstellung der Konzepte und die Festlegung von Sprechweise und Notation anhand von Beispielen. Wir verzichten auf eine systematische Einführung in die Gebiete „Logik“ und „Mengenlehre“ und verweisen z.B. auf die Bücher von Tarski [16] und Halmos [11].

4 Logik und Mengenlehre: ein Steilkurs

4.1 Logik

In der **Aussagenlogik** werden aus „elementaren“ Aussagen und logischen Verknüpfungen neue Aussagen zusammengesetzt.

Beispiel 4.1 Zwei Beispiele für Aussagen sind: Es ist Nacht und 3 ist eine natürliche Zahl.

Logische Verknüpfungen sind

Symbol	Name	Sprechweise
$\wedge$	Konjunktion	„und“
$\vee$	Disjunktion	„oder“
$\neg$	Negation	„nicht“
$\Rightarrow$	Implikation	„daraus folgt“
$\Leftrightarrow$	Äquivalenz	„ist äquivalent zu“

Durch Negation einer „wahren“ Aussage erhält man eine „falsche“ und durch Negation einer falschen Aussage erhält man eine wahre.

Beispiel 4.2 Bezeichnet A die Aussage -1 ist eine natürliche Zahl, so ist A falsch, ihre Negation $\neg A$ (gesprochen „nicht A“) ist eine wahre Aussage. $\neg A$ lässt sich umgangssprachlich formulieren als -1 ist keine natürliche Zahl.

Beispiel 4.3 Im Satz In der Nacht sind alle Katzen grau lassen sich zwei Teil-Aussagen erkennen, nämlich $N :=$ Es ist Nacht und $K :=$ Alle Katzen sind grau. (Das Zeichen $:=$ bedeutet, dass der links stehende Ausdruck durch den rechts stehenden Ausdruck definiert wird.)

Diese beiden Aussagen sind durch eine Implikation verknüpft, was man deutlicher sieht, wenn man den Satz umformuliert in Wenn es Nacht ist, dann sind alle Katzen grau. Mit Hilfe der logischen Verknüpfung $\Rightarrow$ (gesprochen „daraus folgt“ oder „impliziert“) lässt sich der Satz also folgendermaßen schreiben:

$$N \Rightarrow K.$$

Wir haben hier aus den beiden elementaren Aussagen N und K mit Hilfe der logischen Verknüpfung $\Rightarrow$ eine neue, zusammengesetzte Aussage erzeugt.

Weitaus weniger gebräuchlich als die fünf oben genannten Verknüpfungen ist das Zeichen $\veebar$ für „entweder-oder“.

Wenn man mehr als zwei elementare Aussagen zu zusammengesetzten Aussagen verknüpft, muss man auf korrekte Klammerung der einzelnen Aussagen achten, wie man an folgendem Beispiel beobachten kann.

Beispiel 4.4 Zu den oben eingeführten elementaren Aussagen N und K nehmen wir noch eine weitere Aussage hinzu: $R :=$ Es regnet. Mit diesen Aussagen bilden wir die beiden Aussagen

$$N \wedge (R \Rightarrow K) \quad \text{und} \quad (N \wedge R) \Rightarrow K. \tag{4.1}$$

Die beiden Aussagen sind sehr verschieden: die erste kann man lesen als Es ist Nacht und wenn es regnet, sind alle Katzen grau. Die zweite Aussage lautet etwa In regnerischen Nächten sind alle Katzen grau. Dass die beiden Aussagen wirklich verschieden sind, werden wir in Beispiel 4.6 noch genauer verstehen.

Der Wahrheitswert von zusammengesetzten Aussagen wird aus den Wahrheitswerten der einzelnen elementaren Aussagen abgeleitet. Das geschieht mittels **Wahrheitstafeln**, die angeben, in welchen Fällen eine zusammengesetzte Aussage den Wahrheitswert „wahr“ (w) oder „falsch“ (f) annimmt. Die Wahrheitstafeln für die einzelnen Verknüpfungen lauten wie folgt:

D	E	$D \wedge E$
w	w	w
w	f	f
f	w	f
f	f	f

D	E	$D \vee E$
w	w	w
w	f	w
f	w	w
f	f	f

E	$\neg E$
w	f
f	w

D	E	$D \Rightarrow E$
w	w	w
w	f	f
f	w	w
f	f	w

D	E	$D \Leftrightarrow E$
w	w	w
w	f	f
f	w	f
f	f	w

D	E	$D \underline{\vee} E$
w	w	f
w	f	w
f	w	w
f	f	f

Die erste Wahrheitstafel gibt beispielsweise an, dass die Aussage $D \wedge E$ nur dann wahr ist, wenn sowohl D als auch E wahr sind. Die Disjunktion von D und E ist hingegen nur dann falsch, wenn sowohl D als auch E falsch sind. Damit $D \vee E$ wahr ist, muss mindestens eine der beiden Aussagen wahr sein. Im Gegensatz dazu ist die Aussage $D \underline{\vee} E$ nur wahr, wenn genau eine von beiden wahr ist, da sich die Aussagen gegenseitig ausschließen.

Bemerkung 4.5 Beachten Sie, dass die Aussage $D \Rightarrow E$ wahr ist, auch wenn D falsch ist und zwar unabhängig vom Wahrheitswert von E. Umgangssprachlich formuliert: „Aus einer falschen Aussage kann man alles folgern“.

Beispiel 4.6

1. Ist A die Aussage -1 ist eine natürliche Zahl und B die Aussage 3 ist eine natürliche Zahl, dann ist die Aussage $A \Rightarrow B$ (Wenn -1 eine natürliche Zahl ist, dann ist 3 eine natürliche Zahl) wahr, denn eine Implikation $D \Rightarrow E$ hat den Wahrheitswert w, falls D den Wahrheitswert f hat. Die Aussage $A \wedge B$ (also: -1 und 3 sind beides natürliche Zahlen) ist falsch (da mindestens eine der beiden Aussagen falsch ist, in diesem Fall A) und die Aussage $A \vee B$ ist wahr (da mindestens eine der beiden Aussagen wahr ist, in diesem Fall B.)

2. Wenn die Aussagen N und R im obigen Beispiel falsch sind (Es ist nicht Nacht bzw. Es regnet nicht), dann ist die Aussage $N \wedge (R \Rightarrow K)$ falsch (da eine Konjunktion $D \wedge E$ den Wahrheitswert f hat, wenn eine der beiden Aussagen den Wahrheitswert f hat). Die Aussage $(N \wedge R) \Rightarrow K$ ist in diesem Fall jedoch wahr (da eine Implikation $D \Rightarrow E$ den Wahrheitswert w hat, falls D den Wahrheitswert f hat). Die Aussagen in (4.1) sind also tatsächlich verschieden.

Eine Verallgemeinerung der Aussagenlogik ist die **Prädikatenlogik**.

Hier betrachtet man allgemeine **Aussageformen**, die nach dem Einsetzen eines Elementes aus einer gegebenen Menge zu Aussagen im Sinne der Aussagenlogik werden.

Beispiel 4.7

1. $A_1(x) := x$ ist eine natürliche Zahl ist eine Aussageform auf der Menge $\mathbb{Z}$ der ganzen Zahlen. Die Größe x bezeichnet man hier als **Variable** der Aussageform A_1. Setzt man eine ganze Zahl für x ein, so erhält man eine Aussage, z.B. ist $A_1(3)$ die Aussage 3 ist eine natürliche Zahl und $A_1(-1)$ die Aussage -1 ist eine natürliche Zahl.

2. $A_2(x) := (x + x = 2x)$ ist eine Aussageform auf der Menge der ganzen Zahlen $\mathbb{Z}$, die beim Einsetzen eines beliebigen Elementes von $\mathbb{Z}$ für x immer eine wahre Aussage ergibt. Eine solche Aussageform nennt man **allgemeingültig**.

3. $A_3(x) := (3 \leq x) \wedge (x \leq 5)$ ist eine Aussageform auf $\mathbb{Z}$, die zwar nicht allgemeingültig, aber immerhin **erfüllbar** ist, d.h. es gibt mindestens ein Element der Grundmenge, für das die Aussage wahr ist. In diesem Beispiel etwa ist $A_3(4)$ eine wahre und $A_3(1)$ eine falsche Aussage.

4. $G(n, k) :=$ In der Nacht n ist Katze k grau ist eine (zweistellige) Aussageform auf der Grundmenge, die aus allen Paaren (n, k) aus Nächten n und Katzen k besteht.

5. $T(x, y) := x$ ist ein Teiler von y ist eine Aussageform auf der Menge aller Paare von natürlichen Zahlen. Z.B. ist $T(4, 12)$ eine wahre Aussage und $T(1, y)$ eine allgemeingültige Aussageform auf der Menge der natürlichen Zahlen.

6. Sind die Koeffizienten a_{ij} und b_i mit $i = 1, \ldots, m$ und $j = 1, \ldots, n$ fest vorgegeben, so ist $A(x) := x$ ist Lösung des LGS (3.5) eine Aussageform auf der Menge $\mathbb{R}^n$ aller reellen n-Tupel $x = (x_1, \ldots, x_n)$. In dieser Sprechweise ist das LGS genau dann lösbar, wenn $A(x)$ eine erfüllbare Aussageform ist.

Die Variablen in einer Aussageform werden oft **quantifiziert** mit Hilfe des **Existenzquantors** $\exists$ (gesprochen „Es gibt ein...“) und des **Allquantors** $\forall$ (gesprochen „Für alle...“).

Beispiel 4.8

1. $\exists\, x \in \mathbb{Z} :\ A_3(x)$ liest sich als Es gibt eine ganze Zahl x, so dass gilt: $3 \leq x$ und $x \leq 5$ und ist eine wahre Aussage, da beispielsweise $A_3(4)$ wahr ist. Die Aussage $\forall\, x \in \mathbb{Z} :\ A_3(x)$ liest sich als Für alle ganzen Zahlen x gilt: $3 \leq x$ und $x \leq 5$ und ist eine falsche Aussage.

2. $\forall\, x \in \mathbb{N}\ \exists\, y \in \mathbb{N} :\ T(x, y)$ ist eine wahre Aussage, da es zu jeder natürlichen Zahl x mindestens eine Zahl y gibt, deren Teiler sie ist; man setze z.B.

$y := 2x$. Die Aussage $\exists\, y \in \mathbb{N}\ \forall\, x \in \mathbb{N} : T(x, y)$ ist eine falsche Aussage; in Umgangssprache formuliert lautet sie Es gibt eine natürliche Zahl y, die von allen natürlichen Zahlen geteilt wird.

Bemerkung 4.9 Anhand des letzten Beispiel kann man sehen, dass die Reihenfolge der einzelnen Quantifizierungen der Variablen entscheidend ist: $\forall\, x \in \mathbb{N}\ \exists\, y \in \mathbb{N} : T(x, y)$ ist eine ganz andere Aussage als $\exists\, y \in \mathbb{N}\ \forall\, x \in \mathbb{N} : T(x, y)$.

Ein weiterer Quantor ist $\exists_1$, der „Es gibt genau ein ...“ bedeutet. Für eine Aussageform $E(x)$ auf der Grundmenge M ist $\exists_1 x \in M : E(x)$ genau dann eine wahre Aussage, wenn es genau ein Element x in M gibt, für das die Aussage $E(x)$ wahr ist.

4.2 Mengen

Bei der Untersuchung von mathematischen Strukturen werden aus gegebenen Konzepten neue aufgebaut. Verfolgt man diesen Prozess zurück, so stößt man zwangsläufig auf Grundbegriffe, die mathematisch nicht weiter erklärt werden können. Man kann solche Begriffe nur dadurch festlegen, dass man den Umgang mit ihnen durch Gesetze (sogenannte **Axiome**) regelt.

Grundlegend für die gesamte Mathematik ist der Begriff der **Menge**. Der Begründer der Mengenlehre, Georg Cantor (1845–1918), hatte noch definiert:

Unter einer „Menge“ verstehen wir jede Zusammenfassung M von bestimmten wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens (welche die „Elemente“ von M genannt werden) zu einem Ganzen.

In der modernen Mathematik verzichtet man auf eine Definition des Begriffs „Menge“ und verwendet ihn als Grundbegriff. Um Widersprüche zu vermeiden wird gefordert, dass eine Menge sich nicht selbst als Element enthalten darf. Mehr über den axiomatischen Aufbau der Mengenlehre und dabei mögliche Widersprüche findet man in dem Buch von Halmos [11].

Ist ein „Objekt“ a in einer Menge M enthalten, schreiben wir $a \in M$ (lies „a Element M“), andernfalls $a \notin M$ (lies „a nicht Element M“).

Mengen kann man beschreiben durch Auflisten ihrer Elemente, z.B. $M = \{1, 2, 3, 4, 5\}$ oder durch Auswahl bestimmter Elemente einer Grundmenge G mit Hilfe einer Aussageform $A(x)$ auf G, z.B. $G = \mathbb{N}$ und $M = \{n \in \mathbb{N} \mid 1 \leq n \leq 5\}$. Die allgemeine Schreibweise ist $M = \{x \in G \mid A(x)\}$ mit einer Grundmenge G und einer Aussageform $A(x)$ auf G.

Beispiel 4.10

1. die **leere Menge** $\emptyset = \{\}$, die keine Elemente enthält.
2. die **natürlichen Zahlen** $\mathbb{N} = \{1, 2, 3, \ldots\}$. Nehmen wir die Null hinzu, so schreiben wir $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$.
3. die **ganzen Zahlen** $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$.
4. die **rationalen Zahlen**Aus Zeitgründen $\mathbb{Q} = \{\frac{p}{q} \mid p, q \in \mathbb{Z}, q \neq 0\}$.
5. die **reellen Zahlen** $\mathbb{R}$, deren Konstruktion in der Vorlesung „Analysis I“ detailiert behandelt wird.
6. die **komplexen Zahlen** $\mathbb{C} = \{x + \mathrm{i}y \mid x, y \in \mathbb{R}, \mathrm{i} = \sqrt{-1}\}$. Sie werden später in Abschnitt 5.3.1 näher vorgestellt.
7. Die Lösungsmenge $\mathcal{L}$ des LGS (3.5) bei vorgegebenen (reellen) Koeffizienten a_{ij} und b_i lässt sich mit Hilfe der Aussageform $A(x) = x$ ist Lösung des LGS (3.5) ausdrücken als $\mathcal{L} = \{x \in \mathbb{R}^n \mid A(x)\}$.

A heißt **Teilmenge** von B, wenn jedes Element von A auch in B liegt, wenn also aus $x \in A$ folgt $x \in B$. Die Menge B heißt dann **Obermenge** von A. Wir schreiben $A \subset B$ oder $B \supset A$. Dabei kann A echte oder unechte Teilmenge von B sein, je nachdem, ob $A \neq B$ oder $A = B$ ist. Man nennt $\subset$ das **Inklusionszeichen**.

Zwei Mengen M_1 und M_2 sind **gleich**, wenn sie die gleichen Elemente besitzen, d.h. wenn für jedes x gilt:

$$\text{Aus } x \in M_1 \text{ folgt } x \in M_2 \text{ und aus } x \in M_2 \text{ folgt } x \in M_1\,.$$

Es gilt also $M_1 = M_2$ genau dann, wenn $M_1 \subset M_2$ und $M_2 \subset M_1$.

Die Menge aller Teilmengen einer Menge M heißt **Potenzmenge**

$$\mathcal{P}(M) := \{A \mid A \subset M\}.$$

Der Name erklärt sich aus folgendem Beispiel:

Ist M eine endliche Menge mit k Elementen, so ist $\mathcal{P}(M)$ eine Menge mit 2^k Elemente. Z.B. ist die Potenzmenge der Menge $M = \{1, 2, 3\}$ die Menge

$$\mathcal{P}(M) = \{\ \emptyset,\ \{1\},\ \{2\},\ \{3\},\ \{1, 2\},\ \{1, 3\},\ \{2, 3\},\ \{1, 2, 3\}\ \}$$

mit $2^3 = 8$ Elementen.

Der **Durchschnitt** der Mengen A, B ist die Menge

$$A \cap B := \{x \mid x \in A \wedge x \in B\}.$$

Ein Element liegt also genau dann im Durchschnitt von A und B, wenn es sowohl in A als auch in B liegt. Ist der Durchschnitt $A \cap B$ leer, so heißen A und B **disjunkt**.

Der **Vereinigung** der Mengen A, B ist die Menge

$$A \cup B := \{x \mid x \in A \vee x \in B\}.$$

Ein Element liegt also in der Vereinigungsmenge $A \cup B$, wenn es wenigstens in einer der beiden Mengen liegt.

Bemerkung 4.11 Eigenschaften von $\cup$, $\cap$:

- $A \cap B = B \cap A$ und $A \cup B = B \cup A$ (Kommutativgesetze)
- $(A \cap B) \cap C = A \cap (B \cap C)$ und $(A \cup B) \cup C = A \cup (B \cup C)$ (Assoziativgesetze)
- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ und $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (Distributivgesetze)

Unter dem (cartesischen) **Produkt** der Mengen A, B versteht man die Menge

$$A \times B := \{(x, y) \mid x \in A \wedge y \in B\}.$$

Dabei ist (x, y) ein geordnetes Paar, und $(x, y) = (x', y')$ gilt genau dann, wenn $x = x'$ und $y = y'$. Ein Beispiel ist $\mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R}$.

Die **Differenz** der Mengen A, B ist die Menge

$$A \backslash B := \{x \mid x \in A \wedge x \notin B\}.$$

Ist insbesondere A die Grundmenge G, so nennt man $B^c := G \backslash B$ das **Komplement**:

$$B^c = \{x \mid x \notin B\}.$$

Bemerkung 4.12 Es gelten die Formeln

$$A \backslash A = \emptyset, \quad A \cap A^c = \emptyset, \quad A \cup A^c = G, \quad (A^c)^c = A,$$

sowie die **Regeln von de Morgan**

$$(A \cup B)^c = A^c \cap B^c, \qquad (A \cap B)^c = A^c \cup B^c.$$

Durchschnitt und Vereinigung lassen sich auch von mehr als zwei Mengen bilden, indem man die obigen Definitionen sinngemäß überträgt. Sei $\mathcal{M}$ eine Menge von Mengen, z.B. $\mathcal{M} \subset \mathcal{P}(A)$ für eine Menge A.

Der **Durchschnitt** aller Mengen B des Mengensystems $\mathcal{M}$ ($\mathcal{M} \neq \emptyset$) ist die Menge

$$\bigcap_{B \in \mathcal{M}} B := \{x \mid \text{für alle } B \in \mathcal{M} \text{ gilt } x \in B\} = \{x \mid \forall B \in \mathcal{M} : x \in B\}.$$

Sie besteht aus denjenigen Elementen x, die zu *allen* Mengen $B \in \mathcal{M}$ gehören.

Die **Vereinigung** aller Mengen $M \in \mathcal{M}$ ist die Menge

$$\bigcup_{B \in \mathcal{M}} B := \{x \mid \text{es gibt ein } B \in \mathcal{M} \text{ mit } x \in B\} = \{x \mid \exists B \in \mathcal{M} : x \in B\}.$$

Sie besteht aus denjenigen Elementen x, die zu *mindestens einer* Menge $B \in \mathcal{M}$ gehören.

4.3 Beweisprinzipien

Mathematische (Lehr-)Sätze sind wenn-dann-Aussagen. Aus einer gegebenen Aussage V (der **Voraussetzung**) wird mittels logischer Gesetze eine andere Aussage B (die **Behauptung**) abgeleitet; die Darstellung dieser Ableitung ist der Beweis. Formal hat also jede mathematische Aussage die Gestalt $V \Rightarrow B$ und der Zweck des Beweises ist, diese Implikation mit den Mitteln der Logik nachzuweisen. Dafür gibt es verschiedene Methoden; die gebräuchlichsten sind

- **direkter Beweis**: Aus der Voraussetzung wird die Behauptung „direkt“ bewiesen. Ein Beispiel ist Satz 3.4.

- **indirekter Beweis**: Hier benutzt man die Tatsache, dass die Implikation $V \Rightarrow B$ gleichwertig ist mit der Implikation $\neg B \Rightarrow \neg V$. Anstatt die Aussage „Aus V folgt B“ nachzuweisen, kann man genauso gut die Aussage „Aus nicht B folgt nicht V“ zeigen (und ist dann fertig!). Praktisch formuliert man einen indirekten Beweis meistens als **Widerspruchsbeweis**: „Angenommen, die Behauptung B ist falsch, dann (so muss man zeigen) ist auch die Voraussetzung V falsch“.

- **Ringschlüsse**: Mathematische Sätze sind oft Äquivalenzaussagen: verschiedene Behauptungen sind gleichwertig; wenn eine gilt, so gelten auch alle anderen. Hier kann man so vorgehen: Wenn etwa $A \Leftrightarrow B \Leftrightarrow C$ zu zeigen ist, genügt es, $A \Rightarrow B$, $B \Rightarrow C$ und $C \Rightarrow A$ nachzuweisen.

- **vollständige Induktion**: Hier muss man Aussagen A_n für *für alle natürlichen Zahlen* $n \in \mathbb{N}$ beweisen. Dazu geht man so vor:

  INDUKTIONS-VERANKERUNG: Man zeigt, dass etwa A_1 gilt.

  INDUKTIONS-SCHRITT: Sei dann $k \geq 1$ beliebig. Man nimmt an, dass $A_1, A_2, \ldots, A_k$ gelten. Unter dieser Voraussetzung zeigt man dann, dass auch A_{k+1} gilt.

4.4 Abbildungen

Definition 4.13 Gegeben seien zwei Mengen A und B. Eine **Abbildung** von A in B ordnet jedem Element von A genau ein Element von B zu. Wir schreiben

$$f : A \to B, \quad a \mapsto f(a)$$

A heißt **Definitionsmenge** und B **Zielmenge** von f. Die Menge $f(A) := \{f(a) \mid a \in A\} \subset B$ heißt **Bildmenge** von f. Die Menge $\{(a, f(a)) \mid a \in A\} \subset A \times B$ heißt **Graph** der Abbildung f.

Ist die Zielmenge $\mathbb{R}$ oder $\mathbb{C}$, so sagt man statt Abbildung auch **Funktion** .

Eine Abbildung $f : A \to A$ einer Menge A in sich heißt **Selbstabbildung** der Menge A. Insbesondere ist die **identische Abbildung** von A

$$\mathrm{id}_A : A \to A, \quad x \mapsto x$$

eine Selbstabbildung.

Beispiel 4.14

1. $f : \mathbb{N} \to \mathbb{N}, x \mapsto x^2$.
2. $f : \mathbb{R}_{>0} \to \mathbb{R}_{>0}, x \mapsto x^2$, wobei $\mathbb{R}_{>0}$ die Menge der positiven reellen Zahlen bezeichnet.
3. $f : \mathbb{R} \to \mathbb{R}, x \mapsto \sin(x)$.
4. $f : \mathbb{N} \to \{0, 1\}, x \mapsto f(x) = \begin{cases} 0 & \text{für} \quad x \text{ gerade} \\ 1 & \text{für} \quad x \text{ ungerade} \end{cases}$
5. Ist B die Menge der Bücher der Universitätsbibliothek Karlsruhe und U die Menge der Bibliotheksbenutzer, so ist die Zuordnung $L : B \rightsquigarrow U$, die jedem Buch seine Leser zuordnet, keine Abbildung (wieso nicht?).

An den Beispielen zeigen sich einige typische Eigenschaften von Abbildungen, die wir in den folgenden Definitionen präzisieren. Für die Abbildung $f : A \to B$ sagen wir:

Definition 4.15 (a) f heißt **surjektiv**, wenn $f(A) = B$.

Jedes $b \in B$ kommt hier als Bildelement $f(a)$ vor. Man sagt auch: f ist eine Abbildung von A auf B.

(b) f heißt **injektiv**, wenn gilt:

$$\forall x_1, x_2 \in A \ : \ x_1 \neq x_2 \quad \Longrightarrow \quad f(x_1) \neq f(x_2)\,.$$

Bei injektiven Abbildungen haben also verschiedene Elemente auch verschiedene Bilder. Dazu äquivalent ist

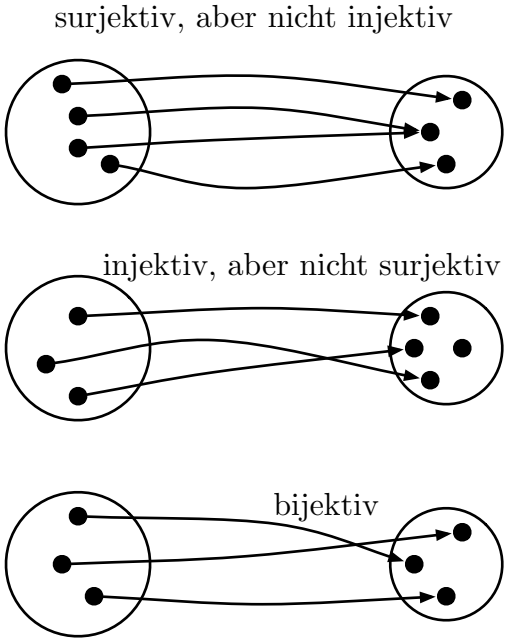
$$\forall x_1, x_2 \in A \ : \ f(x_1) = f(x_2) \quad \Longrightarrow \quad x_1 = x_2.$$

Eine solche injektive Abbildung besitzt eine **Umkehrabbildung**, nämlich

$$f^{-1} : f(A) \to A, \quad y \mapsto f^{-1}(y) \quad \text{mit} \quad f^{-1}(y) = x, \ \text{wenn } f(x) = y.$$

Es ist $f^{-1}(f(x)) = x$ für alle $x \in A$ und $f(f^{-1}(y)) = y$ für alle $y \in f(A)$.

(c) f heißt **bijektiv**, wenn f injektiv und surjektiv ist.



Eine bijektive Selbstabbildung einer endlichen Menge heißt **Permutation** von A.

In Beispiel 4.14 ist 3. weder surjektiv noch injektiv, 4. ist surjektiv, aber nicht injektiv, 1. ist injektiv, aber nicht surjektiv, 2. ist eine bijektive Selbstabbildung der Menge $\mathbb{R}_{>0}$.

Definition 4.16 **(a)** Zwei Abbildungen $f : A \to B$ und $f' : A' \to B'$ sind **gleich**, wenn $A = A', B = B'$ und $f(x) = f'(x)$ für alle $x \in A = A'$.

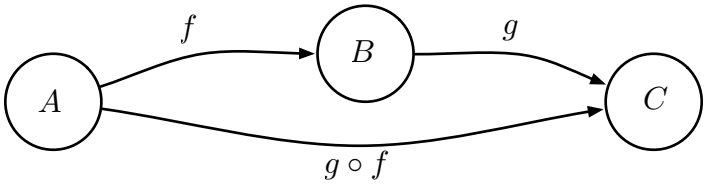
(b) Es seien $f : A \to B$ und $g : A' \to B$ zwei Abbildungen mit $A' \subset A$, und für jedes $x \in A'$ sei $f(x) = g(x)$. Dann heißt g die **Einschränkung** von f auf A' (Schreibweise: $g = f|_{A'}$). Umgekehrt heißt f eine **Fortsetzung** von g auf A.

Unter geeigneten Bedingungen kann man Abbildungen „nacheinander“ ausführen oder „verketten“:

(c) Es seien $f : A \to B$ und $g : B \to C$ zwei Abbildungen. Dann heißt die Abbildung

$$h : A \to C, \quad x \mapsto h(x) := g(f(x))$$

die **Verkettung** von f und g. Schreibweise: $h = g \circ f$ (gelesen: g nach f).



Im Allgemeinen ist $g \circ f \neq f \circ g$. Jedoch gilt das Assoziativgesetz für Verkettungen:

Hilfssatz 4.17 *Für die Abbildungen $f : A \to B$, $g : B \to C$, $h : C \to D$ ist $h \circ (g \circ f) = (h \circ g) \circ f$.*

Beweis: Die Verkettungen sind alle ausführbar, Definitionsmenge ist jeweils A, Zielmenge jeweils D, und es gilt für alle $x \in A$

$$\begin{aligned} (h \circ (g \circ f))(x) &= h((g \circ f)(x)) = h(g(f(x))) \\ ((h \circ g) \circ f)(x) &= (h \circ g)(f(x)) = h(g(f(x))). \end{aligned}$$

■

4.5 Relationen

Definition 4.18 A und B seien zwei Mengen. Eine **Relation** ist eine Teilmenge $R \subset A \times B$ des cartesischen Produkts $A \times B$. Für $(x, y) \in R$ schreibt man auch xRy und sagt: „x steht in der Relation R zu y“.

Beispiel 4.19

1. A = Menge der Männer, B = Menge der Frauen, $R := \{(x, y) \in A \times B \mid x \text{ ist verheiratet mit } y\}$.
2. A = Menge der Punkte, B = Menge der Geraden in der Ebene, $R := \{(x, y) \in A \times B \mid \text{Der Punkt } x \text{ liegt auf der Geraden } y\}$.

4.5.1 Ordnungsrelationen

Es sei $A = B$ und $R \subset A \times A$. Wir verwenden hier anstatt R das Zeichen $\leq$.

Definition 4.20 Eine Relation $\leq$ heißt **Ordnungsrelation** in A und $(A, \leq)$ heißt (partiell) **geordnete Menge**, wenn für alle $a, b, c \in A$ gilt:

O1 $a \leq a$ (reflexiv)

O2 $a \leq b \wedge b \leq a \implies a = b$ (antisymmetrisch)

O3 $a \leq b \wedge b \leq c \implies a \leq c$ (transitiv).

Eine Menge A mit Ordnungsrelation $\leq$ heißt **total geordnet**, wenn für alle $a, b \in A$ gilt:

$$a \leq b \ \vee \ b \leq a.$$

Beispiel 4.21

1. Für eine beliebige Menge M ist die Inklusion $\subset$ eine Ordnungsrelation in der Potenzmenge $\mathcal{P}(M)$ und $(\mathcal{P}(M), \subset)$ ist partiell geordnet.
2. $(\mathbb{N}, \leq)$ ist eine total geordnete Menge.

In Beispiel 2 sind je zwei Elemente **vergleichbar**: Für beliebige $x, y \in \mathbb{N}$ ist $x \leq y$ oder $y \leq x$. In Beispiel 1 gilt das nicht: Man kann bei einer Menge mit mindestens zwei Elementen stets Teilmengen X, Y finden, für die weder $X \subset Y$ noch $Y \subset X$ gilt.

4.5.2 Äquivalenzrelationen

Es sei wieder $A = B$ und $R \subset A \times A$. Für R verwenden wir jetzt das Zeichen $\sim$.

Definition 4.22 $\sim$ heißt **Äquivalenzrelation**, wenn für alle $a, b, c \in A$ gilt:

Ä1 $a \sim a$ (reflexiv)

Ä2 $a \sim b \implies b \sim a$ (symmetrisch)

Ä3 $a \sim b \ \wedge \ b \sim c \implies a \sim c$ (transitiv).

Äquivalenzrelationen sind die vielleicht wichtigsten Relationen. Sie kommen in allen Bereichen der Mathematik vor.

Beispiel 4.23

1. A sei die Menge der Geraden in einer Ebene. $g \sim h$ gelte genau dann, wenn die Geraden g, h parallel sind (d.h. keinen Schnittpunkt haben oder zusammenfallen). Man sieht leicht ein, dass **Ä1**, **Ä2** und **Ä3** erfüllt sind.

2. A sei die Potenzmenge $\mathcal{P}(M)$ einer Menge M. Für zwei Teilmengen X, Y von M gelte $X \sim Y$ genau dann, wenn es eine bijektive Abbildung von X auf Y gibt. X und Y heißen dann **gleichmächtig**. Gleichmächtigkeit ist eine Äquivalenzrelation.

Es sei $\sim$ eine Äquivalenzrelation in A. Zu jedem $a \in A$ bilden wir die Menge

$$K_a := \{x \in A \mid x \sim a\},$$

der Elemente aus A, die zu a äquivalent sind. K_a heißt (Äquivalenz-)**Klasse** von a; und a ist ein **Repräsentant** der Klasse K_a.

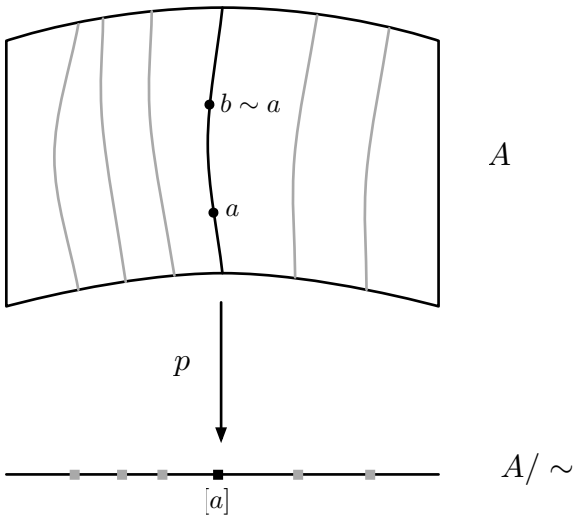
Satz 4.24 (Äquivalenzklassen-Zerlegung) *Ist $\sim$ eine Äquivalenzrelation in der Menge A, so ist A die disjunkte Vereinigung der Äquivalenzklassen von $\sim$.*

Beweis: Wegen der Reflexivität **Ä1** ist $a \in K_a$, also liegt jedes a in *wenigstens* einer Klasse. Damit haben wir $A \subset \bigcup_{a \in A} K_a \subset A$. Bleibt zu zeigen, dass zwei beliebige Klassen K_b und K_c entweder gleich oder disjunkt sind. Nehmen wir also an, dass $K_b \cap K_c \neq \emptyset$. Sei dann etwa $a \in K_b \cap K_c$. Nach Definition einer Äquivalenzklasse gilt $a \sim b$ und $a \sim c$. Mit **Ä2** und **Ä3** folgt dann aber $b \sim c$. Ist jetzt $x \in K_b$, also $x \sim b$, so folgt mit $b \sim c$ wegen **Ä3** $x \sim c$, d.h. $x \in K_c$, also $K_b \subset K_c$. Entsprechend folgt $K_c \subset K_b$, und damit schließlich $K_b = K_c$. ■

Die Menge der Klassen einer Äquivalenzrelation in A nennen wir **Faktormenge** $\tilde{A}$ von A bezüglich $\sim$. Die Abbildung

$$p : A \to \tilde{A} = A/\sim, \quad a \mapsto p(a) = K_a =: \tilde{a},$$

die jedem $a \in A$ seine Klasse $K_a = \tilde{a} \in \tilde{A}$ zuordnet, heißt zugehörige **natürliche** (oder **kanonische**) **Projektion**. Eine andere übliche Schreibweise für die Äquivalenzklassen ist $[a] = K_a$.



4.5.3 Beispiel: Die Menge $\mathbb{Z}/n\mathbb{Z}$ der Restklassen modulo n

Wir betrachten die Menge $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ der ganzen Zahlen und wählen eine natürliche Zahl n. Mit diesem n definieren wir auf $\mathbb{Z}$ die Relation $\sim$ durch

$$a \sim b \iff n \text{ teilt } b - a. \tag{4.2}$$

Dabei bedeutet „n teilt $b - a$“ wie üblich $\exists z \in \mathbb{Z} : b - a = zn$, bzw.

$$\exists z \in \mathbb{Z} : b = a + zn\,. \tag{4.3}$$

Also sind a und b äquivalent, wenn beide bei Division durch n den gleichen Rest ergeben. Für (4.2) bzw. (4.3) schreibt man kürzer $b \equiv a \pmod{n}$. Sprechweise: „b kongruent a modulo n“.

Beispielsweise ist $19 \equiv 9 \pmod{5}, 19 \equiv 4 \pmod{5}, 19 \equiv -1 \pmod{5}$. Die Relation $\sim$ in (4.2) ist eine Äquivalenzrelation in $\mathbb{Z}$: Für alle $a, b, c \in \mathbb{Z}$ gilt nämlich

Ä1: $a \equiv a \pmod{n}$, denn n teilt $a - a = 0$.

Ä2: Gilt $b \equiv a \pmod{n}$, so gibt es ein $z \in \mathbb{Z}$ mit $b = a + zn$. Also ist $a = b + (-z)n$ mit $-z \in \mathbb{Z}$ und somit $a \equiv b \pmod{n}$.

Ä3: Gilt $b \equiv a \pmod{n}$ und $c \equiv b \pmod{n}$, so gibt es $z_1, z_2 \in \mathbb{Z}$ mit $b = a + z_1 n, c = b + z_2 n$ und damit $c = a + (z_1 + z_2)n$. Wegen $z_1 + z_2 \in \mathbb{Z}$ ist also $c \equiv a \pmod{n}$.

Die von $a \in \mathbb{Z}$ erzeugte Klasse ist

$$\tilde{a} = \{x \in \mathbb{Z} \mid x \sim a\} = \{x \in \mathbb{Z} \mid \exists z \in \mathbb{Z} : x = a + zn\} = a + n\mathbb{Z}.$$

Um die Faktormenge für dieses Beispiel explizit zu beschreiben, benutzen wir die sogenannte **Division mit Rest** in $\mathbb{Z}$: Zu je zwei ganzen Zahlen a, b mit $b \neq 0$ gibt es genau zwei weitere ganze Zahlen q, r mit $a = qb + r$ und $0 \leq r < |b|$. Wir können also genau einen **Repräsentanten** r von $\tilde{a}$ wählen mit $0 \leq r < n$. Die Klasse $\tilde{a} = r + n\mathbb{Z}$ besteht dann aus allen $x \in \mathbb{Z}$, die bei Division durch n den Rest r haben. $\tilde{a}$ heißt daher auch **Restklasse mod** n. Die Faktormenge $\mathbb{Z}/\sim$, die wir auch mit $\mathbb{Z}/n\mathbb{Z}$ bezeichnen, können wir dann schreiben als

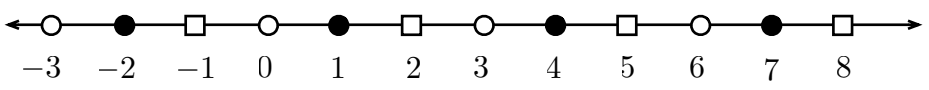
$$\mathbb{Z}/n\mathbb{Z} = \{\tilde{0}, \tilde{1}, \ldots, \widetilde{n-1}\}.$$

Für $n = 3$ sind die Klassen von $\mathbb{Z}/3\mathbb{Z}$ in der folgenden Abbildung skizziert:

○ $\equiv 0 \mod 3$

● $\equiv 1 \mod 3$

□ $\equiv 2 \mod 3$



5 Algebraische Grundbegriffe

5.1 Worum es geht: das Beispiel der ganzen Zahlen

Was macht man eigentlich, wenn man „rechnet“? Mit welchen Objekten kann man rechnen? Welche Gesetze müssen gelten, damit man Gleichungen formulieren und lösen kann?

Wir betrachten dazu zunächst einmal das Modell-Beispiel der Menge der ganzen Zahlen $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$. Ganze Zahlen kann man addieren, subtrahieren und multiplizieren. Wenn man hingegen eine ganze Zahl durch eine andere dividiert, erhält man im Allgemeinen eine rationale Zahl; die Division „führt aus der Menge der ganzen Zahlen heraus“.

Diese Tatsachen kann man mit Hilfe des Abbildungsbegriffes präzisieren. Wir fassen die Addition zweier ganzer Zahlen als eine Abbildung mit zwei Argumenten auf, und ordnen diesem Paar eine weitere ganze Zahl zu:

$$+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (x, y) \mapsto x + y,$$

wobei wir wie üblich $x+y$ statt $+(x, y)$ schreiben. Eine Abbildung, die zwei Elementen einer Menge ein Element aus derselben Menge zuordnet, heißt *Verknüpfung*.

In $\mathbb{Z}$ gibt es ein Element, das bezüglich der Addition vor allen anderen ausgezeichnet ist: die Null. Denn diese hat als einziges Element die Eigenschaft, dass man sie zu allen Elementen $a \in \mathbb{Z}$ hinzuaddieren kann, ohne dass sich die Zahl a dadurch ändert: $a + 0 = a$ für alle $a \in \mathbb{Z}$. Man sagt „0 ist das neutrale Element bezüglich der Addition“.

Das Addieren einer Zahl $a \in \mathbb{Z}$ zu einer weiteren Zahl lässt sich rückgängig machen durch das Subtrahieren von a, was das Gleiche ist wie das Addieren von $-a \in \mathbb{Z}$. Man sagt: $-a$ ist das *inverse Element* von a bezüglich der Addition. Das inverse Element $-a$ von a zeichnet sich dadurch aus, dass gilt

$$a + (-a) = 0,$$

d.h. addiert man zu einer Zahl $a \in \mathbb{Z}$ ihr inverses Element $-a$, so erhält man das neutrale Element 0.

Durch diese Struktur sind wir in der Lage, Gleichungen der Form $a + x = b$ nach x aufzulösen: wir addieren auf beiden Seiten der Gleichung das inverse Element $-a$ von a und erhalten $x = b + (-a) := b - a$ als eindeutige Lösung.

Betrachten wir nun die Multiplikation auf $\mathbb{Z}$. Auch diese schreiben wir als Abbildung

$$\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \quad (x, y) \mapsto x \cdot y.$$

Bei dieser Verknüpfung gibt es ebenfalls ein neutrales Element: die Eins. Es gilt nämlich $a \cdot 1 = 1 \cdot a = a$ für alle $a \in \mathbb{Z}$. Jedoch lässt sich die Multiplikation nicht umkehren (jedenfalls nicht, ohne die Menge $\mathbb{Z}$ zu verlassen). Z.B. lässt sich die Multiplikation einer Zahl $a \in \mathbb{Z}$ mit 2 nicht rückgängig machen, denn dafür müsste man mit der *rationalen* Zahl $\frac{1}{2}$ multiplizieren. Da $\frac{1}{2}$ aber nicht in $\mathbb{Z}$ liegt, gibt es in $\mathbb{Z}$ kein inverses Element von 2 bezüglich der Multiplikation:

$$2 \cdot x = 1 \quad \text{gilt für keine Zahl } x \in \mathbb{Z}.$$

Zwei weitere Eigenschaften der Addition und der Multiplikation haben wir stillschweigend verwendet. Bei der Durchführung mehrerer Additionen bzw. mehrerer Multiplikationen kommt es nicht auf die Reihenfolge an: für beliebige $a, b, c \in \mathbb{Z}$ gilt $(a+b)+c = a+(b+c)$ und $a+b = b+a$ (entsprechend für die Multiplikation). Diese Eigenschaften sind natürlich für das „Rechnen“ mit ganzen Zahlen entscheidend. Im Folgenden definieren wir die in diesem Beispiel aufgetretenen Konzepte allgemein und untersuchen ihre Beziehungen.

5.2 Gruppen: die wichtigsten algebraischen Objekte

Definition 5.1 Gegeben sei eine Menge A. Eine (innere) **Verknüpfung** $*$ auf A ist eine Abbildung

$$* : A \times A \to A, \quad (x,\, y) \mapsto x * y$$

Bemerkung 5.2 Bei Verknüpfungen schreibt man $x * y$ für das Bild $*(x, y)$ von (x, y) unter der Abbildung $*$. Statt $*$ verwendet man auch häufig die Verknüpfungszeichen $+, -, \cdot$ usw.

Beispiel 5.3

1. Die Addition $+$ und die Multiplikation $\cdot$ sind Verknüpfungen auf $\mathbb{Z}$, aber nicht die Division :.

2. Die Subtraktion $-$ ist keine Verknüpfung auf $\mathbb{N}$ (da $2-4 \notin \mathbb{N}$) und die Division : keine Verknüpfung auf $\mathbb{R}$ (da die Division durch 0 in $\mathbb{R}$ nicht erklärt ist). Die Division : ist aber eine Verknüpfung auf $\mathbb{R}\backslash\{0\}$.

3. Auf der Menge $\mathrm{Abb}(M, M) = \{f : M \to M\}$ aller Selbstabbildungen einer nichtleeren Menge M ist die Verkettung eine Verknüpfung.

Definition 5.4 Wir nennen eine Verknüpfung $*$ auf einer Menge A **assoziativ**, wenn

$$\forall a, b, c \in A \ : \ (a * b) * c = a * (b * c)$$

gilt, und **kommutativ**, wenn

$$\forall a, b \in A \ : \ a * b = b * a$$

gilt.

Beispiel 5.5

1. Auf $\mathbb{Z}$ ist $+$ assoziativ und kommutativ.
2. Auf $\mathbb{Z}$ ist $-$ weder assoziativ noch kommutativ.
3. Auf $\mathbb{Z}$ ist die Verknüpfung $\diamond : (a, b) \mapsto |a - b|$ nicht assoziativ, aber kommutativ.
4. Die Verkettung von Abbildungen auf der Menge $\mathrm{Abb}(M, M)$ aller Selbstabbildungen von A ist stets assoziativ, aber i.Allg. nicht kommutativ.
5. In $\mathbb{Z}/n\mathbb{Z}$ (vgl. Abschnitt 4.5.3) definieren wir eine Verknüpfung $+$ durch

   $$+ : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}; \quad (\tilde{a}, \tilde{b}) \mapsto \tilde{a} + \tilde{b} := \widetilde{a + b}\,.$$

   (Beachten Sie, dass das Zeichen $+$ hier in zwei verschiedenen Bedeutungen benutzt wird: einmal ist $+$ die „gewöhnliche“ Addition in $\mathbb{Z}$ und einmal die neu definierte Addition in $\mathbb{Z}/n\mathbb{Z}$.) Damit obige Definition sinnvoll ist, hat man die Unabhängigkeit der Summenklasse $\widetilde{a + b}$ von der Repräsentantenauswahl zu prüfen, damit wirklich jedem Paar $(\tilde{a}, \tilde{b})$ genau eine Klasse $\widetilde{a + b}$ als Bild zugeordnet wird (Wohldefiniertheit):

   Haben wir $\tilde{a}_0 = \tilde{a}$, $\tilde{b}_0 = \tilde{b}$, also $a_0 \sim a$, $b_0 \sim b$, so gilt $a_0 \equiv a \pmod{n}$, $b_0 \equiv b \pmod{n}$. Es gibt also $z_1, z_2 \in \mathbb{Z}$ mit $a_0 = a + z_1 n$, $b_0 = b + z_2 n$, woraus $a_0 + b_0 = (a + b) + (z_1 + z_2)n$, also

   $$a_0 + b_0 \equiv a + b \pmod{n}$$

   folgt. Es gilt also tatsächlich $\widetilde{a_0 + b_0} = \widetilde{a + b}$. Damit haben wir gezeigt, dass die auf $\mathbb{Z}/n\mathbb{Z}$ definierte Addition tatsächlich eine Verknüpfung auf $\mathbb{Z}/n\mathbb{Z}$ ist. Sie ist assoziativ und kommutativ. Die **Verknüpfungstafel** für die Addition $+$ etwa auf $\mathbb{Z}/3\mathbb{Z}$ sieht folgendermaßen aus

$+$	$\tilde{0}$	$\tilde{1}$	$\tilde{2}$
$\tilde{0}$	$\tilde{0}$	$\tilde{1}$	$\tilde{2}$
$\tilde{1}$	$\tilde{1}$	$\tilde{2}$	$\tilde{0}$
$\tilde{2}$	$\tilde{2}$	$\tilde{0}$	$\tilde{1}$

Definition 5.6 **(a)** Ist $*$ eine Verknüpfung auf A und gibt es ein Element $e \in A$ mit

$$\forall a \in A \ : \ e * a = a = a * e,$$

so heißt e **neutrales Element** bezüglich $*$.

(b) Ist $*$ eine Verknüpfung auf A mit neutralem Element e und gibt es zu einem Element $a \in A$ ein $a^{-1} \in A$ mit

$$a^{-1} * a = e = a * a^{-1},$$

so heißt a^{-1} **inverses Element von** a.

Bemerkung 5.7 **(a)** Es gibt *höchstens ein* neutrales Element für eine Verknüpfung $*$ auf A. Denn sind e_1 und e_2 neutrale Elemente bezüglich $*$, so ist nach Definition $e_1 * e_2 = e_1$, aber auch $e_1 * e_2 = e_2$, also $e_1 = e_2$.

(b) Unter der zusätzlichen Voraussetzung, dass $*$ assoziativ ist, lässt sich zeigen, dass es zu einem $a \in A$ *höchstens ein* Inverses a^{-1} gibt! Denn sind a_1^{-1} und a_2^{-1} inverse Elemente von a, so gilt

$$a_1^{-1} = a_1^{-1} * e = a_1^{-1} * (a * a_2^{-1}) = (a_1^{-1} * a) * a_2^{-1} = e * a_2^{-1} = a_2^{-1}.$$

Beispiel 5.8 Die Addition $+$ auf $\mathbb{Z}$ hat das neutrale Element 0. Das inverse Element von $z \in \mathbb{Z}$ ist $-z$.

Besonders wichtig und reichhaltig sind assoziative Verknüpfungen mit neutralem Element, bei der *jedes* Element ein Inverses besitzt:

Definition 5.9 Eine **Gruppe** ist ein Paar $(G, *)$ bestehend aus einer (nichtleeren) Menge G und einer Verknüpfung $*$ auf G mit folgenden Eigenschaften:

G1 (**assoziativ**): $\forall a, b, c \in G : (a * b) * c = a * (b * c)$

G2 (**neutrales Element**): $\exists e \in G \ \forall a \in G : e * a = a = a * e$

G3 (**inverses Element**): $\forall a \in G \ \exists a^{-1} \in G : a^{-1} * a = e = a * a^{-1}$.

Gilt zusätzlich

G4 $\forall a, b \in G : a * b = b * a$,

so heißt die Gruppe G **abelsch**.

Bemerkung 5.10 Nach der Bemerkungen 5.7 ist das neutrale Element einer Gruppe *eindeutig* bestimmt und zu jedem Gruppenelement a gibt es *genau ein* Inverses a^{-1}.

Beispiel 5.11

1. $(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+),(\mathbb{R}\backslash\{0\},\cdot)$ sind abelsche Gruppen. $(\mathbb{Z},\cdot)$ und $(\mathbb{Q},\cdot)$ sind keine Gruppen.

2. $(\mathbb{Z}/n\mathbb{Z},\ +)$ ist eine abelsche Gruppe. $\tilde{0}$ ist das neutrale Element und $\widetilde{n-r}$ ist das zu $\tilde{r}$ inverse Element $(0 \leq r < n)$.

3. Für die Menge $\mathrm{Abb}(M,M)$ der Selbstabbildungen $f : M \to M$ ist die Verkettung assoziativ mit der Identität id_M als neutralem Element; $\mathrm{Abb}(M,M)$ ist aber im Allgemeinen keine Gruppe, weil die Gruppeneigenschaft G3 nicht erfüllt ist. Beschränkt man sich jedoch auf die Teilmenge S_M der bijektiven Selbstabbildungen von M, so ist $(S_M,\circ)$ eine Gruppe. Für den Fall einer endlichen Menge M werden uns mit solchen Gruppen im nächsten Abschnitt noch genauer beschäftigen.

Hilfssatz 5.12 (Multiplikation mit Inversen) *In einer Gruppe $(G,*)$ sind die Gleichungen $a*x=b$ und $x*c=d$ eindeutig nach x lösbar.*

Beweis: $x = a^{-1}*b$ ist Lösung von $a*x=b$, denn

$$a*(a^{-1}*b) = (a*a^{-1})*b = e*b = b.$$

Diese Lösung ist die einzige, denn sind x_1, x_2 zwei Lösungen von $a*x=b$, so gilt

$$\begin{aligned} a*x_1 = a*x_2 &\implies a^{-1}*(a*x_1) = a^{-1}*(a*x_2) \\ &\implies (a^{-1}*a)*x_1 = (a^{-1}*a)*x_2 \\ &\implies e*x_1 = e*x_2 \\ &\implies x_1 = x_2. \end{aligned}$$

Entsprechend hat $x*c=d$ die eindeutige Lösung $x = d*c^{-1}$. ■

Bemerkung 5.13 Man kann zeigen, dass eine Menge G mit einer assoziativen Verknüpfung $*$ bereits dann eine Gruppe ist, wenn gilt:

$$\exists e \in G\ \forall a \in G : a*e = a \quad (e \text{ ist rechtsneutral})$$

und

$$\forall a \in G\ \exists a^{-1} \in G : a*a^{-1} = e \quad (a^{-1} \text{ ist rechtsinvers}).$$

5.2.1 Beispiel: Die symmetrische Gruppe

Definition 5.14 Es sei M eine endliche Menge. Die Menge S_M der Permutationen (also Selbstabbildungen) von M ist eine Gruppe bezglich der Verkettung $\circ$ von Abbildungen und heißt **symmetrische Gruppe** von M.

Jede endliche Menge mit m Elementen ist bijektiv zur Menge $M = \{1, 2, \ldots, m\}$. Es genügt also, dieses spezielle M zu betrachten. Statt S_M schreiben wir dann S_m.

Bemerkung 5.15 Mittels vollständiger Induktion beweist man: Es gibt $1 \cdot 2 \cdot 3 \cdot \cdots \cdot m = m!$ Permutationen der Menge $\{1, 2, \ldots, m\}$; die Gruppe S_m hat also $m!$ Elemente.

Eine Permutation $\pi \in S_m$ schreiben wir schematisch folgendermaßen:

$$\pi = \begin{pmatrix} 1 & 2 & \cdots & m \\ \pi(1) & \pi(2) & \cdots & \pi(m) \end{pmatrix}.$$

Wir setzen also unter jedes $i \in \{1, 2, \ldots, m\}$ das entsprechende Bild $\pi(i)$. Zum Beispiel hat die symmetrische Gruppe S_3 von $M = \{1, 2, 3\}$ die $3! = 1 \cdot 2 \cdot 3 = 6$ Elemente

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \pi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \pi_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

$$\pi_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \pi_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \pi_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

und die Gruppentafel

$(S_3, \circ)$	π_1	π_2	π_3	π_4	π_5	π_6
π_1	π_1	π_2	π_3	π_4	π_5	π_6
π_2	π_2	π_3	π_1	π_6	π_4	π_5
π_3	π_3	π_1	π_2	π_5	π_6	π_4
π_4	π_4	π_5	π_6	π_1	π_2	π_3
π_5	π_5	π_6	π_4	π_3	π_1	π_2
π_6	π_6	π_4	π_5	π_2	π_3	π_1

Dabei steht beispielsweise in der 2. Zeile und 5. Spalte der Tafel die Verkettung $\pi_2 \circ \pi_5 = \pi_4$, in der 5. Zeile und 2. Spalte dagegen $\pi_5 \circ \pi_2 = \pi_6$. Die Gruppe S_3 ist also *nicht abelsch*.

Für $m = 1$ besteht die symmetrische Gruppe S_1 nur aus der identischen Abbildung von $M = \{1\}$. Wir wollen im Folgenden stets $m \geq 2$ voraussetzen und zeigen, dass

sich jedes $\pi \in S_m$ als Verkettung von gewissen „einfachen“ Permutationen darstellen lässt. Eine **Transposition** ist eine Permutation aus S_m, bei der zwei verschiedene, fest gewählte Zahlen $i, k \in \{1, 2, \ldots, m\}$ vertauscht werden, während alle übrigen Zahlen fest bleiben, also

$$\begin{aligned} \pi(i) &= k \qquad (i \neq k), \\ \pi(k) &= i \qquad (i \neq k), \\ \pi(l) &= l \qquad \text{für alle } l \neq i, k. \end{aligned}$$

Man schreibt für diese Transposition auch kurz $(i\ k)$. Zum Beispiel ist für $m = 3$

$$\pi_4 = (2\ 3), \quad \pi_5 = (3\ 1), \quad \pi_6 = (1\ 2).$$

Für π_1, π_2, π_3 gilt

$$\pi_1 = (1\ 2) \circ (1\ 2), \quad \pi_2 = (1\ 3) \circ (1\ 2), \quad \pi_3 = (2\ 3) \circ (1\ 2),$$

oder auch

$$\pi_3 = (2\ 3) \circ (1\ 3) \circ (2\ 3) \circ (1\ 3).$$

Bemerkung 5.16 Ist $\tau = (i\ k)$ eine Transposition, so gilt $\tau \circ \tau = \mathrm{id}$; insbesondere also $\tau^{-1} = \tau$.

Allgemein gilt der

Satz 5.17 (S_m wird von Transpositionen erzeugt) *Jede Permutation $\pi \in S_m$ (für $m \geq 2$) lässt sich als Verkettung von Transpositionen darstellen.*

Beweis: Wir beweisen die Aussage durch vollständige Induktion: Die Aussage des Satzes ist für $m = 2$ richtig, denn für die S_2 gilt

$$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = (1\ 2) \circ (1\ 2), \qquad \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = (1\ 2).$$

Unter der Annahme, dass der Satz für $m = k \geq 1$ gilt, zeigen wir jetzt, dass er auch für $m = k + 1$ richtig ist.

1. FALL: Wenn $\pi(1) = 1$, so lässt sich

$$\pi = \begin{pmatrix} 1 & 2 & \cdots & k+1 \\ 1 & \pi(2) & \cdots & \pi(k+1) \end{pmatrix}$$

als Permutation der k Zahlen $2, 3, \ldots, k+1$ nach Induktionsannahme als Verkettung von Transpositionen darstellen.

2. FALL: Wenn $\pi(1) = i \neq 1$, so gilt

$$\pi = \begin{pmatrix} 1 & 2 & \cdots & i-1 & i & i+1 & \cdots & k+1 \\ i & \pi(2) & \cdots & \pi(i-1) & \pi(i) & \pi(i+1) & \cdots & \pi(k+1) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & \cdots & i-1 & i & i+1 & \cdots & k+1 \\ \pi(i) & \pi(2) & \cdots & \pi(i-1) & i & \pi(i+1) & \cdots & \pi(k+1) \end{pmatrix} \circ (1\ i)$$

und π ist wieder als Verkettung von Transpositionen darstellbar, weil in der vorletzten Permutation i fest ist. ■

Definition 5.18 Es sei $\pi \in S_m$ eine Permutation. Die **Fehlstandszahl** $F(\pi)$ von π ist die (eindeutige) Anzahl der Fälle, in denen für $i < k$ gilt $\pi(i) > \pi(k)$. Die Permutationen mit gerader Fehlstandszahl $F(\pi)$ heißen **gerade**, die Permutationen mit ungerader Fehlstandszahl heißen **ungerade**.

Beispielsweise ist die Fehlstandszahl für

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}$$

gleich 5, weil 2 vor 1, 4 vor 1, 4 vor 3, 5 vor 1 und 5 vor 3 steht.

Die Anzahl der Transpositionen in der Darstellung einer Permutation ist *nicht eindeutig* bestimmt. Zum Beispiel gilt

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix} = (1\ 4) \circ (1\ 2) \circ (3\ 5) = (2\ 3) \circ (2\ 5) \circ (1\ 3) \circ (2\ 3) \circ (2\ 4).$$

Hingegen gilt der

Hilfssatz 5.19 (Anzahl Transpositionen) *Sei $\pi \in S_m$ ($m \geq 2$) eine Permutation. Die Anzahl der Transpositionen in allen Darstellungen von π ist für π gerade stets gerade und für π ungerade stets ungerade.*

Beweis: Wir überlegen zuerst wie sich die Fehlstandszahl ändert, wenn man eine Permutation π mit einer Transposition verkettet.

1. FALL: (Transposition vertauscht zwei benachbarte Ziffern): Bei

$$(\pi(i)\ \ \pi(i+1)) \circ \begin{pmatrix} 1 & \cdots & i & i+1 & \cdots & m \\ \pi(1) & \cdots & \pi(i) & \pi(i+1) & \cdots & \pi(m) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & \cdots & i & i+1 & \cdots & m \\ \pi(1) & \cdots & \pi(i+1) & \pi(i) & \cdots & \pi(m) \end{pmatrix}$$

ändert sich die Fehlstandszahl gegenüber $F(\pi)$ um $+1$, falls $\pi(i) < \pi(i+1)$ bzw. um -1, falls $\pi(i) > \pi(i+1)$.

2. FALL: (Transposition vertauscht zwei nicht benachbarte Ziffern): Bei

$$(\pi(i)\ \ \pi(k)) \circ \begin{pmatrix} 1 & \cdots & i & \cdots & k & \cdots & m \\ \pi(1) & \cdots & \pi(i) & \cdots & \pi(k) & \cdots & \pi(m) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & \cdots & i & \cdots & k & \cdots & m \\ \pi(1) & \cdots & \pi(k) & \cdots & \pi(i) & \cdots & \pi(m) \end{pmatrix}$$

können wir die Vertauschung durch schrittweises Vertauschen benachbarter Ziffern erreichen, denn es ist (wir schreiben π_j für $\pi(j)$)

$$\begin{aligned}(\pi_i\ \ \pi_k) \circ \pi \ &= \ (\pi_{i+1}\ \pi_k) \circ \cdots \circ (\pi_{k-2}\ \pi_k) \circ (\pi_{k-1}\ \pi_k) \circ \cdots \\ &\quad \cdots \circ (\pi_i\ \pi_k) \circ (\pi_i\ \pi_{k-1}) \circ \cdots \circ (\pi_i\ \pi_{i+2}) \circ (\pi_i\ \pi_{i+1}) \circ \pi.\end{aligned}$$

Bei jedem der $k-i+k-1-i = 2(k-i)-1$ Schritte ändert sich F um ± 1, insgesamt also um eine ungerade Zahl.

FAZIT: Bei Verkettung von π mit einer Transposition τ gilt für die Fehlstandszahl

$$F(\tau \circ \pi) = F(\pi) + n \qquad \text{mit ungeradem } n.$$

Nach Satz 5.17 ist die Permutation π als (nicht eindeutige) Verkettung von, sagen wir r, Transpositionen $\tau_1, \tau_2, \ldots, \tau_r$ darstellbar. Wir können also schreiben

$$\pi = \tau_r \circ \cdots \circ \tau_1 \circ \text{ id}.$$

Ausgehend von der identischen Abbildung id, die die Fehlstandszahl 0 hat, ändert sich auf der rechten Seite obiger Gleichung bei jedem Schritt die Fehlstandszahl um eine ungerade Zahl, so dass

$$\begin{aligned} F(\pi) &= 0 + n_1 + n_2 + \cdots + n_r \\ &= (2z_1 + 1) + (2z_2 + 1) + \cdots + (2z_r + 1) \\ &= 2z + r. \end{aligned}$$

Ist nun π eine gerade Permutation, also die durch π eindeutig bestimmte Fehlstandszahl $F(\pi)$ gerade, so muss nach obiger Formel auch die Anzahl r der Transpositionen gerade sein. Ist π (und damit auch $F(\pi)$) ungerade, dann auch r. ■

Folgerung 5.20 *Die geraden Permutationen von S_m ($m \geq 2$) bilden bezüglich $\circ$ eine Gruppe $(A_m, \circ)$, die sogenannte* **alternierende Gruppe**.

Bemerkung 5.21 Die Teilmenge B_m der ungeraden Permutationen von S_m ($m \geq 2$) ist bezüglich $\circ$ *keine Gruppe*, denn $\circ$ ist keine Verknüpfung in B_m (wieso nicht?).

Die Anzahl der geraden Permutationen von S_m ($m \geq 2$) ist ebenso groß wie die Anzahl der ungeraden Permutationen, nämlich $\frac{1}{2}m!$. Begründung: Die Abbildung

$$f : A_m \to B_m, \quad \pi_g \mapsto \pi_u = (1\ 2) \circ \pi_g$$

ist bijektiv; A_m und B_m sind also gleichmächtig.

5.2.2 Untergruppen

Die eben angetroffene Situation, dass die Teilmenge A_m von S_m selbst wieder eine Gruppe bezüglich der von S_m übernommenen Verknüpfung ist, motiviert folgende Definition:

Definition 5.22 Gegeben sei eine Gruppe $(G, *)$ und eine Teilmenge $U \subset G$, die bezüglich der von G induzierten Verknüpfung $*$ ebenfalls eine Gruppe ist. Dann heißt $(U, *)$ **Untergruppe** von $(G, *)$.

Beispiel 5.23

1. Jede Gruppe $(G, *)$ hat mindestens zwei Untergruppen: $(\{e\}, *)$ und $(G, *)$.
2. Die alternierende Gruppe $(A_m, \circ)$ ist eine Untergruppe von $(S_m, \circ)$.
3. $(\mathbb{Z}, +)$ ist eine Untergruppe von $(\mathbb{Q}, +)$.

Bemerkung 5.24 Das neutrale Element e' einer Untergruppe $(U, *)$ von $(G, *)$ stimmt mit dem neutralen Element e von $(G, *)$ überein. Denn nach Hilfssatz 5.12 ist die Gleichung $e' * x = e'$ in G eindeutig lösbar; die Lösungen e und e' sind also gleich. Ebenso sieht man, dass für ein Element $a \in U \subset G$ das inverse Element in $(G, *)$ und in $(U, *)$ dasselbe ist.

Der folgende Satz zeigt, dass man nicht alle Gruppeneigenschaften nachprüfen muss, um festzustellen, ob eine Untergruppe vorliegt.

Satz 5.25 (Untergruppen-Kriterium) *Sei $(G, *)$ eine Gruppe. Eine Teilmenge $U \subset G$ ist Untergruppe von G, wenn gilt:*

UG1 $U \neq \emptyset$

UG2 $\forall a, b \in U : a * b^{-1} \in U$.

BEWEIS: Wegen **UG1** gibt es mindestens ein $a \in U$. Wegen **UG2** liegt mit jedem $a \in U$ auch $a * a^{-1} = e$ in U, also gilt für U die Eigenschaft **G2**. Mit e und a liegt nach **UG2** auch $e * a^{-1} = a^{-1}$ in U, also gilt **G3**. Wenn a, $b \in U$, so auch $b^{-1} \in U$ und damit nach **UG2** auch $a * b = a * (b^{-1})^{-1} \in U$, so dass $*$ eine Verknüpfung in U ist. $(U, *)$ ist assoziativ, d.h. es gilt **G1**, da $*$ auf $G \supset U$ assoziativ ist. ■

Definition 5.26 Sei $(G, *)$ eine Gruppe und $M \subset G$ eine beliebige Teilmenge. Dann heißt die kleinste Untergruppe von G, die M enthält, die **von** M **erzeugte Untergruppe** $\langle M \rangle$. Eine von einem einzigen Element $a \in G$ erzeugte Untergruppe heißt **zyklisch** (Schreibweise: $U = \langle a \rangle$).

Beispiel 5.27 In $(\mathbb{Z}, +)$ ist $n\mathbb{Z} = \{\ldots, -3n, -2n, -n, 0, n, 2n, 3n, \ldots\}$ die von $n \in \mathbb{Z}$ erzeugte zyklische Untergruppe: $\langle n \rangle = n\mathbb{Z}$.

5.2.3 Homomorphismen

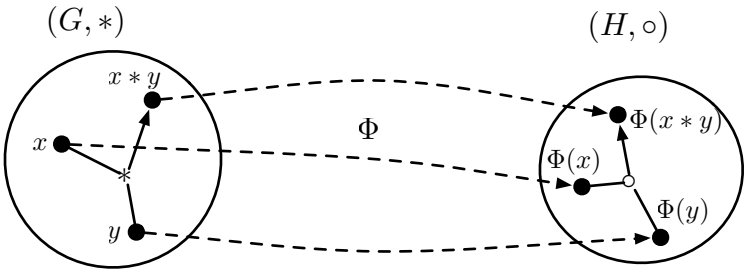
Wenn man zwei Mengen vergleichen will, auf denen Verknüpfungen definiert sind, interessiert man sich besonders für Abbildungen zwischen diesen Mengen, die mit der Verknüpfungsstruktur der Mengen „verträglich“ sind. Man nennt solche **strukturerhaltende Abbildungen** auch **Homomorphismen**. Einen bijektiven Homomorphismus nennt man **Isomorphismus**.

Welche speziellen Eigenschaften eine solche Abbildung haben muss, hängt jeweils von den gegebenen Verknüpfungen ab.

Definition 5.28 Seien $(G, *)$ und $(H, \circ)$ zwei Gruppen und $\Phi : G \to H$ eine Abbildung. Dann heißt Φ ein **(Gruppen-)Homomorphismus**, wenn gilt

$$\forall x, y \in G : \Phi(x * y) = \Phi(x) \circ \Phi(y).$$

Stimmen die beiden Gruppen $(G, *)$ und $(H, \circ)$ überein (ist Φ also eine Selbstabbildung), so spricht man von **Endomorphismen** statt von Homomorphismen. Einen bijektiven Endomorphismus nennt man auch **Automorphismus**.



Beispiel 5.29

1. Die Abbildung $\Phi_1 : \mathbb{Z} \to \mathbb{Q}$, $x \mapsto 3x$ ist ein Homomorphismus der Gruppe $(\mathbb{Z}, +)$ in die Gruppe $(\mathbb{Q}, +)$.

   Die Abbildung $\Phi_2 : \mathbb{Z} \to \mathbb{Q}$, $x \mapsto x^2$ ist kein Homomorphismus (wieso nicht?).

2. Die Abbildung $\Phi_3 : \mathbb{R} \to \mathbb{R}$, $x \mapsto 3x$ ist ein Endomorphismus der Gruppe $(\mathbb{R}, +)$, da für alle $x, y \in \mathbb{R}$ gilt $3(x + y) = 3x + 3y$. Da Φ bijektiv ist, ist Φ_3 sogar ein Automorphismus von $(\mathbb{R}, +)$.

3. Die Abbildung $\Phi_4 : \mathbb{Z} \to \mathbb{Z}$, $x \mapsto 2x$ ist ein Endomorphismus der Gruppe $(\mathbb{Z}, +)$, aber kein Automorphismus.

4. Die Exponential-Abbildung $\exp : \mathbb{R} \to \mathbb{R}_{>0}$, $x \mapsto \mathrm{e}^x$ ist ein Isomorphismus der additiven Gruppe der reellen Zahlen $(\mathbb{R}, +)$ in die multiplikative Gruppe der positiven reellen Zahlen $(\mathbb{R}_{>0}, \cdot)$, denn exp ist bijektiv und für alle $x, y \in \mathbb{R}$ gilt $\mathrm{e}^{x+y} = \mathrm{e}^x \cdot \mathrm{e}^y$.

Bemerkung 5.30 Gegeben sei eine Gruppe $(G, *)$ und eine Menge B, auf der eine Verknüpfung $\circ$ erklärt ist. Weiter sei $\Phi : G \to B$ eine Abbildung, die die Homomorphieeigenschaft $\forall x, y \in G : \Phi(x * y) = \Phi(x) \circ \Phi(y)$ erfüllt. Dann ist $(\Phi(G), \circ)$ eine Gruppe. Kurz: „Das homomorphe Bild einer Gruppe ist wieder eine Gruppe“.

5.3 Ringe und Körper: Verallgemeinerungen von $\mathbb{Z}$ und $\mathbb{R}$

Die Menge $\mathbb{Z}$ der ganzen Zahlen ist bezüglich der Addition $+$ eine (abelsche) Gruppe. Auf $\mathbb{Z}$ ist durch die Multiplikation $\cdot$ noch eine zweite Verknüpfung erklärt. Wie wir in 3.1 gesehen haben, ist $(\mathbb{Z}, \cdot)$ jedoch *keine* Gruppe. Die Multiplikation ist aber assoziativ und zudem sind Addition und Multiplikation durch Distributivgesetze verbunden. Diese Struktur verallgemeinern wir in folgender Definition.

Definition 5.31 Ein **Ring** ist eine Menge R zusammen mit zwei Verknüpfungen $+$ und $\cdot$ mit folgenden Eigenschaften:

R1 $(R, +)$ ist eine abelsche Gruppe,

R2 $\cdot$ ist assoziativ,

R3 Distributivgesetze: für alle $a, b, c \in R$ gilt:

$$a \cdot (b + c) = a \cdot b + a \cdot c \text{ und } (b + c) \cdot a = b \cdot a + c \cdot a.$$

Wenn die Verknüpfung $\cdot$ kommutativ ist, nennt man den Ring **kommutativ**. Das neutrale Element in $(R, +)$ bezeichnet man mit 0 (**Nullelement**), das zu a inverse Element mit $-a$. Die Differenz $b - a$ ist durch $b - a := b + (-a)$ erklärt. Hat der Ring auch ein neutrales Element ($\neq 0$) bezüglich der Multiplikation $\cdot$, so schreibt man dafür 1 und nennt es **Einselement**; R heißt dann **Ring mit Eins**.

Beispiel 5.32

1. $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring mit Eins.
2. $(\mathbb{R}, +, \cdot)$ ist ebenfalls ein kommutativer Ring mit Eins (aber noch viel mehr, siehe später).

Bemerkung 5.33 Einige allgemeine Eigenschaften von Ringen:

1. Für alle $a \in R$ gilt $a \cdot 0 = 0 = 0 \cdot a$.
2. Für alle $a, b \in R$ gilt $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$ und $(-a) \cdot (-b) = a \cdot b$.
3. Für alle $a, b, c \in R$ gilt $a \cdot (b - c) = a \cdot b - a \cdot c$.

Beweis:

1. Es ist $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$. Da in $(R, +)$ die Gleichung $c + x = c$ die eindeutig bestimmte Lösung $x = 0$ hat, folgt $a \cdot 0 = 0$. Entsprechend gilt $0 \cdot a = 0$.
2. Es ist $a \cdot b + (-a) \cdot b = (a + (-a)) \cdot b = 0 \cdot b = 0$. Da $c + x = 0$ die eindeutig bestimmte Lösung $x = -c$ hat, ist $(-a) \cdot b = -(a \cdot b)$. Entsprechend folgt $a \cdot (-b) = -(a \cdot b)$. Weiter ist $(-a) \cdot (-b) = -(a \cdot (-b)) = -(-(a \cdot b))$. Da in $(R, +)$ stets $-(-c) = c$ gilt, folgt schließlich $(-a) \cdot (-b) = a \cdot b$.
3. $a \cdot (b - c) = a \cdot (b + (-c)) = a \cdot b + a \cdot (-c) = a \cdot b + (-a \cdot c) = a \cdot b - a \cdot c$. ■

Beispiel 5.34 In 5.2 haben wir auf der Menge der Restklassen modulo n eine Addition definiert durch

$$+ : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \quad (\tilde{a}, \tilde{b}) \mapsto \tilde{a} + \tilde{b} := \widetilde{a + b} \quad \text{für } a \in \tilde{a},\ b \in \tilde{b}.$$

$(\mathbb{Z}/n\mathbb{Z}, +)$ ist dann eine abelsche Gruppe. Wir definieren eine weitere Verknüpfung auf $\mathbb{Z}/n\mathbb{Z}$ durch

$$\cdot : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \quad (\tilde{a}, \tilde{b}) \mapsto \tilde{a} \cdot \tilde{b} := \widetilde{ab} \quad \text{für } a \in \tilde{a},\ b \in \tilde{b}.$$

Auch hier müssen wir die Wohldefiniertheit überprüfen. Dazu seien $\tilde{a}_0 = \tilde{a}, \tilde{b}_0 = \tilde{b}$, also $a_0 \equiv a \pmod{n}, b_0 \equiv b \pmod{n}$. Dann gibt es $z_1, z_2 \in \mathbb{Z}$ mit $a_0 = a + z_1 n, b_0 = b + z_2 n$ und es gilt $a_0 b_0 = ab + (az_2 + bz_1 + z_1 z_2 n)n$. Wegen $az_2 + bz_1 + z_1 z_2 n \in \mathbb{Z}$ gilt $a_0 b_0 \equiv ab \pmod{n}$, also tatsächlich $\widetilde{a_0 b_0} = \widetilde{ab}$.

Eine Multiplikationstafel für das Beispiel $(\mathbb{Z}/3\mathbb{Z}, \cdot)$ sieht so aus:

$(\mathbb{Z}/3\mathbb{Z}, \cdot)$	$\tilde{0}$	$\tilde{1}$	$\tilde{2}$
$\tilde{0}$	$\tilde{0}$	$\tilde{0}$	$\tilde{0}$
$\tilde{1}$	$\tilde{0}$	$\tilde{1}$	$\tilde{2}$
$\tilde{2}$	$\tilde{0}$	$\tilde{2}$	$\tilde{1}$

Die Multiplikation $\cdot$ ist also eine Verknüpfung auf $\mathbb{Z}/n\mathbb{Z}$. Man prüft leicht nach, dass $\cdot$ assoziativ und kommutativ ist und das Einselement $\tilde{1}$ besitzt. Wegen der Kommutativität von $\cdot$ braucht man nur ein Distributivgesetz zu prüfen: Für alle $\tilde{a}, \tilde{b}, \tilde{c} \in \mathbb{Z}/n\mathbb{Z}$ gilt

$$\begin{aligned} \tilde{a} \cdot (\tilde{b} + \tilde{c}) &= \tilde{a} \cdot \widetilde{(b+c)} = \widetilde{a(b+c)} \\ &= \widetilde{ab + ac} = \widetilde{ab} + \widetilde{ac} \\ &= \tilde{a} \cdot \tilde{b} + \tilde{a} \cdot \tilde{c}. \end{aligned}$$

Also ist $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ ein kommutativer Ring mit Eins.

Definition 5.35 Ein Element $a \neq 0$ eines Rings R heißt (linker) **Nullteiler**, wenn es ein $b \in R$, $b \neq 0$ gibt mit $ab = 0$.

Beispiel 5.36 Im Ring $\mathbb{Z}/3\mathbb{Z}$ gibt es keine Nullteiler (vgl. obige Multiplikationstafel). Im Ring $\mathbb{Z}/6\mathbb{Z}$ hingegen ist z.B. $\tilde{2}$ ein linker Nullteiler, denn es ist $\tilde{2} \cdot \tilde{3} = \tilde{6} = \tilde{0}$ mit $\tilde{2} \neq \tilde{0}$ und $\tilde{3} \neq \tilde{0}$.

Definition 5.37 Sind $(R_1, +, \cdot)$ und $(R_2, +, \cdot)$ zwei Ringe mit Eins, dann nennt man eine Abbildung $\Phi : R_1 \to R_2$ **(Ring-)Homomorphismus**, wenn für alle $x, y \in R_1$ gilt

$$\Phi(x + y) = \Phi(x) + \Phi(y), \quad \Phi(x \cdot y) = \Phi(x) \cdot \Phi(y) \quad \text{und} \quad \Phi(1) = 1.$$

Beispiel 5.38 Die kanonische Projektion $k : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $x \mapsto \tilde{x}$, die jedem Element von $\mathbb{Z}$ seine Äquivalenzklasse im Restklassenring $\mathbb{Z}/n\mathbb{Z}$ zuordnet, ist ein Ring-Homomorphismus. Das folgt unmittelbar aus der Wohldefiniertheit (also Repräsentanten-Unabhängigkeit) der Addition und Multiplikation auf $\mathbb{Z}/n\mathbb{Z}$.

Im Gegensatz zu $(\mathbb{Z}\backslash\{0\}, \cdot)$ ist $(\mathbb{R}\backslash\{0\}, \cdot)$ eine (abelsche) Gruppe. Solche Ringe sind von besonderer Bedeutung in der linearen Algebra.

Definition 5.39 Ein Ring $(\mathbb{K}, +, \cdot)$, für den $(\mathbb{K}\backslash\{0\}, \cdot)$ eine abelsche Gruppe ist, heißt **Körper**.

Ein Körper ist also ein kommutativer Ring mit Eins, in dem jedes von Null verschiedene Element ein multiplikativ Inverses hat.

Ein Körper hat insbesondere stets ein Einselement $1 \neq 0$ und zu jedem $a \neq 0$ ein eindeutig bestimmtes Inverses a^{-1} bezüglich der Multiplikation. Jede Gleichung $a \cdot x = b$ ist für $a \neq 0$ durch $x = a^{-1} \cdot b = b \cdot a^{-1}$ eindeutig lösbar. Aus $u \cdot v = 0$ folgt also $u = 0$ oder $v = 0$; die Gleichung $u \cdot v = 0$ kann für $u \neq 0$ und $v \neq 0$ nicht gelten. Ein Körper ist also notwendigerweise „nullteilerfrei“.

Beispiel 5.40 $(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot)$ sind Körper, ebenso $(\mathbb{Z}/3\mathbb{Z}, +, \cdot)$. Hingegen ist der Ring $(\mathbb{Z}/6\mathbb{Z}, +, \cdot)$ kein Körper, denn er hat Nullteiler.

Bemerkung 5.41 Sie können nachprüfen, dass in den Abschnitten 3.2 und 3.3 nur die Körpereigenschaften der reellen Zahlen $(\mathbb{R}, +, \cdot)$ benutzt wurden. Die Begriffe und Ergebnisse aus diesen Abschnitten übertragen sich deshalb wörtlich auf lineare Gleichungssysteme *über beliebigen* Körpern $\mathbb{K}$. Deshalb gilt auch in diesem allgemeinen Kontext die Invarianz der Lösungsmenge unter Elementaroperationen und der Gaußsche Algorithmus.

Definition 5.42 Sind $(\mathbb{K}_1, +, \cdot)$ und $(\mathbb{K}_2, +, \cdot)$ zwei Körper, dann heißt eine Abbildung $\Phi : \mathbb{K}_1 \to \mathbb{K}_2$ ein **(Körper-)Homomorphismus**, wenn für alle $x, y \in \mathbb{K}_1$ gilt

$$\Phi(x + y) = \Phi(x) + \Phi(y), \quad \Phi(x \cdot y) = \Phi(x) \cdot \Phi(y) \quad \text{und} \quad \Phi(1) = 1.$$

Beispiel 5.43 Die Einbettung von $\mathbb{Q}$ in $\mathbb{R}$, $\Phi : \mathbb{Q} \to \mathbb{R}$, $x \mapsto x$ ist ein injektiver Körperhomomorphismus.

Definition 5.44 Ist $(\mathbb{K}, +, \cdot)$ ein Körper und gibt es eine natürliche Zahl m, sodass

$$\underbrace{1 + 1 + \cdots + 1}_{m \text{ mal}} = 0$$

gilt, so heißt die kleinste solche Zahl p die **Charakteristik** (char $\mathbb{K}$) von $\mathbb{K}$. Gibt es kein solches m, so hat $\mathbb{K}$ per Definition die Charakteristik 0.

Beispiel 5.45 In $(\mathbb{Z}/3\mathbb{Z}, +, \cdot)$ ist $\tilde{1}$ das Einselement, und es gilt $\tilde{1} + \tilde{1} + \tilde{1} = \tilde{0}$. $\mathbb{Z}/3\mathbb{Z}$ hat also die Charakteristik char $\mathbb{K} = 3$. Dagegen ist in $(\mathbb{Q}, +, \cdot)$ niemals $1 + 1 + \cdots + 1 = 0$. Es gilt also char $\mathbb{Q} = 0$.

Bemerkung 5.46 Ist die Charakteristik $p \neq 0$, so ist die p-fache Summe $a + a + \cdots + a = 0$ für *alle* $a \in \mathbb{K}$ und p ist eine Primzahl.

BEWEIS: Es ist $\underbrace{a+\cdots+a}_{p \text{ mal}} = a\cdot 1+\cdots a\cdot 1 = a\cdot(\underbrace{1+\cdots+1}_{p \text{ mal}}) = a\cdot 0 = 0$. Wegen $1\neq 0$ kann p nicht 1 sein in $\mathbb{K}$. Wenn $p>1$ keine Primzahl wäre, so gäbe es eine Darstellung $p=p_1p_2$ mit natürlichen Zahlen p_1,p_2, die beide $<p$ sind. Wegen des in $\mathbb{K}$ geltenden Distributivgesetzes haben wir dann

$$\underbrace{1+1+\cdots+1}_{p_1p_2 \text{ mal}} = \underbrace{(1+\cdots+1)}_{p_1 \text{ mal}}\cdot\underbrace{(1+\cdots+1)}_{p_2 \text{ mal}} = 0.$$

Da $\mathbb{K}$ als Körper nullteilerfrei ist, folgt also $\underbrace{1+\cdots+1}_{p_1 \text{ mal}} = 0$ oder $\underbrace{1+\cdots+1}_{p_2 \text{ mal}} = 0$, im Widerspruch zur Definition der Charakteristik als kleinste derartige Zahl. ■

Bemerkung 5.47 Der Ring $(\mathbb{Z}/p\mathbb{Z},+,\cdot)$ ist genau dann ein Körper, wenn p eine Primzahl ist. In diesem Fall ist $\operatorname{char}\mathbb{Z}/p\mathbb{Z}=p$. Zu jeder Primzahl p gibt es also einen Körper

$$\mathbb{Z}/p\mathbb{Z} = \{\tilde{0},\tilde{1},\ldots,\widetilde{p-1}\}$$

mit p Elementen. $\mathbb{Z}/p\mathbb{Z}$ heißt daher ein **endlicher Körper**. $\mathbb{Z}/2\mathbb{Z}=\{\tilde{0},\tilde{1}\}$ ist der kleinste (endliche) Körper.

Man kann weiter zeigen, dass es zu jeder Primzahl p und jeder natürlichen Zahl k einen Körper $\mathbb{F}_{p^k}$ gibt mit p^k Elementen und $\operatorname{char}\mathbb{K}=p$.

Beispiel 5.48 (Ein Körper mit 4 Elementen) Auf dem cartesischen Produkt $\mathbb{F}_4 := \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ erklären wir zwei Verknüpfungen

$$\begin{aligned} x+y &= (\tilde{x}_1,\tilde{x}_2)+(\tilde{y}_1,\ \tilde{y}_2) = (\tilde{x}_1+\tilde{y}_1,\ \tilde{x}_2+\tilde{y}_2)\\ x\cdot y &= (\tilde{x}_1,\tilde{x}_2)\cdot(\tilde{y}_1,\tilde{y}_2) = (\tilde{x}_1\cdot\tilde{y}_1+\tilde{x}_2\cdot\tilde{y}_2,\tilde{x}_1\cdot\tilde{y}_2+\tilde{x}_2\cdot\tilde{y}_1+\tilde{x}_2\cdot\tilde{y}_2)\end{aligned}$$

mit $\tilde{x}_1,\tilde{x}_2,\tilde{y}_1,\tilde{y}_2\in\mathbb{Z}/2\mathbb{Z}$.
Setzen wir noch $0:=(\tilde{0},\tilde{0}), u:=(\tilde{1},\tilde{0}), v:=(\tilde{0},\tilde{1}), w:=(\tilde{1},\tilde{1})$, so erhalten wir die Verknüpfungstafeln

$+$	0	u	v	w
0	0	u	v	w
u	u	0	w	v
v	v	w	0	u
w	w	v	u	0

und

$\cdot$	0	u	v	w
0	0	0	0	0
u	0	u	v	w
v	0	v	w	u
w	0	w	u	v

.

Hieraus ergibt sich, dass $(\mathbb{F}_4,+,\cdot)$ ein Körper ist mit 4 Elementen und $\operatorname{char}\mathbb{F}_4=2$. Das Nullelement in $\mathbb{F}_4$ ist 0 und das Einselement ist a. Die additive Gruppe ist die sogenannte Kleinsche Vierergruppe $\mathcal{V}_4$ und die multiplikative Gruppe $(\mathbb{F}_4\backslash\{0\},\cdot) = \{u,v,w\} = \{v,v^2,v^3\}$ ist die von v erzeugte zyklische Gruppe.

5.3.1 Beispiel: Der Körper $\mathbb{C}$ der komplexen Zahlen

Ausgehend vom Körper $\mathbb{R}$ betrachten wir das cartesische Produkt $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ aller geordneten Paare (a, b) reeller Zahlen und definieren für diese Menge zwei Verknüpfungen

$$\begin{array}{lrcl} \text{Addition:} & (a,b)+(a',b') & = & (a+a', b+b'), \\ \text{Multiplikation:} & (a,b)\cdot(a',b') & = & (aa'-bb', ab'+a'b). \end{array}$$

Mit diesen Verknüpfungen wird $\mathbb{C}$ zu einem Körper; seine Elemente heißen **komplexe Zahlen**.

Bemerkung 5.49 $(1, 0)$ ist das Einselement in $\mathbb{C}$ und $(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2})$ ist das multiplikative Inverse von $(a, b) \neq (0, 0)$.

Wir wollen jetzt die üblichen Schreibweise für komplexe Zahlen einführen und betrachten dazu die Abbildung

$$h : \mathbb{R} \to \mathbb{C}, \quad a \mapsto (a, 0).$$

Dann ist h ein injektiver Körperhomomorphismus, sodass wir $\mathbb{R}$ mit dem Teilkörper $h(\mathbb{R}) \subset \mathbb{C}$ identifizieren können. Das Element $a \in \mathbb{R}$ wird also mit $(a, 0) \in \mathbb{C}$ identifiziert. In diesem Sinne ist dann $\mathbb{R}$ in den Körper $\mathbb{C}$ „eingebettet“: $\mathbb{R} \subset \mathbb{C}$.

Schreiben wir i für die komplexe Zahl $(0, 1)$, so lässt sich jetzt die komplexe Zahl $z = (a, b)$ eindeutig in der Form $z = (a, b) = (a, 0) + (0, b) = (a, 0) + (0, 1) \cdot (b, 0)$, also

$$z = a + \mathrm{i}b \quad \text{mit } a, b \in \mathbb{R} \tag{5.1}$$

schreiben. Man nennt a den **Realteil** ($a = \mathrm{Re}\ z$) und b den **Imaginärteil** ($b = \mathrm{Im}\ z$) der komplexen Zahl z. Weiter nennt man

$$\overline{z} = (a, -b) = a - \mathrm{i}b$$

die zu $z = a + \mathrm{i}b$ **konjugiert komplexe Zahl** und

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

den (Absolut-)**Betrag** von z.

Die Addition bzw. Multiplikation in der neuen Schreibweise (5.1) lauten jetzt

$$\begin{aligned} z_1 + z_2 &= a_1 + \mathrm{i}b_1 + a_2 + \mathrm{i}b_2 = a_1 + a_2 + \mathrm{i}(b_1 + b_2) \\ z_1 z_2 &= (a_1 + \mathrm{i}b_1)(a_2 + \mathrm{i}b_2) = a_1a_2 - b_1b_2 + \mathrm{i}(a_1b_2 + b_1a_2), \end{aligned}$$

Man rechnet also „wie gewohnt“ unter Berücksichtigung der Vorschrift $\mathrm{i}^2 = -1$.

5.4 Matrizen

Definition 5.50 Es seien $m, n \in \mathbb{N}$ und $\mathbb{K}$ ein Körper. Eine **Matrix** über $\mathbb{K}$ mit m Zeilen und n Spalten, kurz eine $m \times n$-Matrix, ist ein rechteckiges Schema der Form

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1k} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2k} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{j1} & a_{j2} & \cdots & a_{jk} & \cdots & a_{jn} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mk} & \cdots & a_{mn} \end{pmatrix}, \tag{5.2}$$

mit Einträgen $a_{jk} \in \mathbb{K}$ für $j = 1, \ldots, m$ und $k = 1, \ldots, n$. Man schreibt auch kurz

$$A = (a_{jk})$$

und nennt die a_{jk} die **Komponenten** der $m \times n$-Matrix A. Die Menge aller $m \times n$-Matrizen über $\mathbb{K}$ bezeichnen wir mit $\mathbb{K}^{m \times n}$.

5.4.1 Matrizen-Addition

Zwei $m \times n$ Matrizen $A = (a_{ij})$ und $B = (b_{ij})$ kann man **komponentenweise addieren**:

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} + \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{m1} & \cdots & b_{mn} \end{pmatrix} = \begin{pmatrix} a_{11} + b_{11} & \cdots & a_{1n} + b_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} + b_{m1} & \cdots & a_{mn} + b_{mn} \end{pmatrix},$$

d.h. $(a_{jk}) + (b_{jk}) := (a_{jk} + b_{jk})$. Mit dieser Addition wird $\mathbb{K}^{m \times n}$ zu einer abelschen Gruppe. Das neutrale Element bezüglich der Addition ist die **Nullmatrix**

$$O = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix},$$

deren Komponenten alle Null sind. Das additive Inverse $-A$ von A ist

$$-A = \begin{pmatrix} -a_{11} & \cdots & -a_{1n} \\ \vdots & \ddots & \vdots \\ -a_{m1} & \cdots & -a_{mn} \end{pmatrix}.$$

5.4.2 Matrizen-Multiplikation

Wir wollen nun zwei geeignete Matrizen A, B auch multiplizieren. Dabei müssen wir *voraussetzen*, dass

1. die Anzahl q der Spalten von A mit der Anzahl q der Zeilen von B übereinstimmt und

2. dass $A \in \mathbb{K}^{p\times q}$ und $B \in \mathbb{K}^{q\times r}$ ist, dass also A, B beides Matrizen über dem selben Körper $\mathbb{K}$ sind.

Definition 5.51 Es seien A eine $p \times q$-Matrix und B eine $q \times r$-Matrix über $\mathbb{K}$. Unter dem **(Matrizen-)Produkt** $C = AB$ verstehen wir dann die $p \times r$-Matrix $C = (c_{jk}) \in \mathbb{K}^{p\times r}$ mit

$$c_{jk} := a_{j1}b_{1k} + a_{j2}b_{2k} + \cdots + a_{jq}b_{qk} = \sum_{s=1}^{q} a_{js}b_{sk}\,; \quad j = 1,\ldots,p;\ k = 1,\ldots,r. \tag{5.3}$$

Die Komponente c_{jk} der Produktmatrix AB wird also gemäß (5.3) gebildet, indem man in A die j-te Zeile, in B die k-te Spalte auswählt, nacheinander die Produkte der an gleicher Stelle stehenden Zeilen- bzw. Spaltenelemente bildet und addiert:

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{j1} & a_{j2} & \cdots & a_{jn} \\ \cdots & \cdots & \cdots & \cdots \\ a_{p1} & a_{p2} & \cdots & a_{pn} \end{pmatrix} \begin{pmatrix} b_{11} & \vdots & b_{1k} & \vdots & b_{1q} \\ b_{21} & \vdots & b_{2k} & \vdots & b_{2q} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ b_{n1} & \vdots & b_{nk} & \vdots & b_{nq} \end{pmatrix} = \begin{pmatrix} & \vdots & \\ \cdots & c_{jk} & \cdots \\ & \vdots & \end{pmatrix}.$$

Beispiel 5.52

1. $\begin{pmatrix} 1 & -1 & 3 \\ 2 & 0 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 0 \\ 0 & -1 & -2 & 1 \\ 5 & 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 16 & 9 & 8 & 8 \\ 22 & 12 & 10 & 12 \end{pmatrix}.$

2. $\begin{pmatrix} 1 & -1 & 3 \\ 2 & 0 & 4 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 5 \end{pmatrix} = \begin{pmatrix} 16 \\ 22 \end{pmatrix}.$

3. $\begin{pmatrix} 1 & -1 & 3 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 5 \end{pmatrix} = \begin{pmatrix} 16 \end{pmatrix}.$

4. $\begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix} \begin{pmatrix} 2 & 0 & -1 \end{pmatrix} = \begin{pmatrix} 2 & 0 & -1 \\ 4 & 0 & -2 \\ 6 & 0 & -3 \\ 8 & 0 & -4 \end{pmatrix}$.

Insbesondere lassen sich **quadratische Matrizen**, d.h. Matrizen, bei denen die Zeilen- und Spaltenzahl übereinstimmt, stets miteinander multiplizieren. Die Matrizen-Multiplikation ist also eine Verknüpfung auf der Menge $\mathbb{K}^{n\times n}$ der quadratischen $n \times n$-Matrizen. Das neutrale Element ist die **Einheitsmatrix**

$$E = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix}.$$

Die Matrizen-Multiplikation ist aber keine Verknüpfung auf der Menge $\mathbb{K}^{m\times n}$ mit $m \neq n$.

Satz 5.53 *Es sei $n \in \mathbb{N}$ und $\mathbb{K}$ ein Körper. Bezeichnet $+$ die komponentenweise Addition und $\cdot$ die Matrizen-Multiplikation, dann ist $(\mathbb{K}^{n\times n}, +, \cdot)$ ein Ring mit Eins.*

Beweis: Neben dem Beweis, dass $(\mathbb{K}^{n\times n}, +)$ eine abelsche Gruppe ist, bleibt zu zeigen, dass das Assoziativgesetz

$$\forall\, A, B, C \in \mathbb{K}^{n\times n} : (AB)C = A(BC)$$

und die beiden Distributivgesetze

$$\forall A, B, C \in \mathbb{K}^{n\times n} : A(B + C) = AB + AC \quad \text{und} \quad (A + B)C = AC + BC$$

gelten. Mit $A = (a_{jk})$, $B = (b_{jk})$, $C = (c_{jk})$ gilt für die Matrix $M = A(B + C) = (m_{il})$ nach Definition der Addition und Matrizen-Multiplikation

$$m_{il} = \sum_{s=1}^{n} a_{is}(b_{sl} + c_{sl}) = \sum_{s=1}^{n} a_{is}b_{sl} + \sum_{s=1}^{n} a_{is}c_{sl}\ ; \quad i,\, l = 1, \ldots, n,$$

also $M = AB + AC$. Damit ist das 1. Distributivgesetz bewiesen, das 2. beweist man analog. ■

Bemerkung 5.54 Die Matrizen-Multiplikation ist im Allgemeinen *nicht kommutativ*! Zum Beispiel gilt:

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

An diesem Beispiel sieht man auch, dass $\mathbb{K}^{n\times n}$ Nullteiler hat. Der Matrizenring $(\mathbb{K}^{n\times n}, +, \cdot)$ ist also im Allgemeinen weder kommutativ noch nullteilerfrei.

Bemerkung 5.55 Ein LGS (3.5) über dem Körper $\mathbb{K}$ lässt sich als Matrixgleichung schreiben: Sei dazu

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \in \mathbb{K}^{m\times n}$$

die Matrix des LGS, vgl. (3.6), und weiter

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{K}^{n\times 1} \qquad \text{und} \qquad b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \in \mathbb{K}^{m\times 1}.$$

Dann lässt sich das LGS (3.5) nach Definition der Matrizen-Multiplikation schreiben als

$$A \cdot x = b.$$

Es gilt nämlich $\sum_{k=1}^{n} a_{ik}x_k = b_i$ für $i = 1, \ldots, m$.

5.4.3 Inverse Matrizen

Definition 5.56 Gibt es zu einer quadratischen Matrix $A \in \mathbb{K}^{n\times n}$ über dem Körper $\mathbb{K}$ ein inverses Element bezüglich der Matrizen-Multiplikation, d.h. eine Matrix $A^{-1} \in \mathbb{K}^{n\times n}$ mit $AA^{-1} = A^{-1}A = E$, so heißt A **invertierbar** und A^{-1} ihre **Inverse** oder **inverse Matrix**.

Satz 5.57 *Die Menge* $\mathbf{GL}(n, \mathbb{K})$ *aller invertierbaren* $n\times n$*-Matrizen über dem Körper* $\mathbb{K}$ *ist bezüglich der Matrizen-Multiplikation eine Gruppe.*[1]

Beweis: Nach Satz 5.53 ist die Matrizen-Multiplikation assoziativ und hat als neutrales Element die Einheitsmatrix E. Nach Voraussetzung hat jede Matrix ein inverses Element. Es bleibt also nur noch zu zeigen, dass $\mathbf{GL}(n, \mathbb{K})$ bezüglich der Matrizen-Multiplikation abgeschlossen ist. Seien dazu $A, B \in \mathbf{GL}(n, \mathbb{K})$. Dann ist auch AB invertierbar, die Inverse von AB ist nämlich gerade $B^{-1}A^{-1}$ wegen

$$B^{-1}A^{-1}A\,B = B^{-1}EB = E \quad \text{und} \quad A\,B\,B^{-1}A^{-1} = A\,E\,A^{-1} = E.$$

■

[1] $\mathbf{GL}(n, \mathbb{K})$ steht für *general linear group*.

5.4.4 Wie berechnet man die inverse Matrix?

Die inverse Matrix einer gegebenen Matrix $A \in \mathbb{K}^{n\times n}$ lässt sich - falls sie existiert - mit dem Gaußschen Algorithmus berechnen. Die Inverse $A^{-1} = (x_{jk}) \in \mathbb{K}^{n\times n}$ existiert genau dann, wenn die Matrizengleichung $AA^{-1} = E$ lösbar ist. Da das inverse Element in einer Gruppe eindeutig bestimmt ist, ist A^{-1} dann auch eindeutig. Wir bezeichnen die k-te Spalte der gesuchten Matrix A^{-1} mit x_k, also

$$x_k = \begin{pmatrix} x_{1k} \\ \vdots \\ x_{nk} \end{pmatrix} \in \mathbb{K}^{n\times 1}.$$

Die Matrizengleichung $A \cdot A^{-1} = E$ ist (nach Definition der Matrizen-Multiplikation) genau dann lösbar, wenn die n Gleichungssysteme

$$A \cdot x_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad A \cdot x_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots, A \cdot x_n = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

mit den zugehörigen erweiterten Matrizen

$$\left(\begin{array}{cccc|c} a_{11} & a_{12} & \cdots & a_{1n} & 1 \\ a_{21} & a_{22} & \cdots & a_{2n} & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} & 0 \end{array}\right), \left(\begin{array}{cccc|c} a_{11} & a_{12} & \cdots & a_{1n} & 0 \\ a_{21} & a_{22} & \cdots & a_{2n} & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} & 0 \end{array}\right), \ldots, \left(\begin{array}{cccc|c} a_{11} & a_{12} & \cdots & a_{1n} & 0 \\ a_{21} & a_{22} & \cdots & a_{2n} & \vdots \\ \vdots & \vdots & \ddots & \vdots & 0 \\ a_{n1} & a_{n2} & \cdots & a_{nn} & 1 \end{array}\right)$$

lösbar sind. Wenn wir auf diese n linearen Gleichungssysteme den Gaußschen Algorithmus anwenden, ergibt sich aus dem k-ten Gleichungssystem

mit Matrix $\left(\begin{array}{ccc|c} a_{11} & \cdots & a_{1n} & 0 \\ \vdots & & \vdots & \vdots \\ \vdots & \ddots & \vdots & 1 \\ \vdots & & \vdots & \vdots \\ a_{n1} & \cdots & a_{nn} & 0 \end{array}\right)$ die Endgestalt $\left(\begin{array}{ccc|c} 1 & \cdots & 0 & x_{1k} \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & x_{nk} \end{array}\right)$,

aus deren letzter Spalte sich die Lösung x_k ablesen lässt. Da jedesmal die Matrix A vorkommt, wird das Verfahren zweckmäßigerweise so durchgeführt, dass man die Elementaroperationen für alle n Gleichungssysteme simultan vornimmt:

$$\left(\begin{array}{ccc|ccc} a_{11} & \cdots & a_{1n} & 1 & & 0 \\ \vdots & & \vdots & 0 & \ddots & \vdots \\ \vdots & & \vdots & \vdots & & 0 \\ a_{n1} & \cdots & a_{nn} & 0 & & 1 \end{array}\right) \rightsquigarrow \left(\begin{array}{ccc|ccc} 1 & \cdots & 0 & x_{11} & \cdots & x_{1n} \\ \vdots & \ddots & \vdots & x_{21} & \ddots & x_{2n} \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 1 & x_{n1} & \cdots & x_{nn} \end{array}\right).$$

Beispiel 5.58 Es sei $A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & -1 & 4 \\ 1 & 0 & 2 \end{pmatrix}$. Der Gaußsche Algorithmus liefert

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 2 & -1 & 4 & 0 & 1 & 0 \\ 1 & 0 & 2 & 0 & 0 & 1 \end{array}\right) \begin{matrix} \\ \leftarrow -2 \cdot + \\ \leftarrow -1 \cdot + \end{matrix} \rightsquigarrow \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & -5 & -2 & -2 & 1 & 0 \\ 0 & -2 & -1 & -1 & 0 & 1 \end{array}\right) \begin{matrix} \leftarrow -1 \cdot + \\ \\ \leftarrow 3 \cdot + \end{matrix}$$

$$\rightsquigarrow \left(\begin{array}{ccc|ccc} 1 & -4 & 0 & -2 & 0 & 3 \\ 0 & -1 & 0 & 0 & 1 & -2 \\ 0 & 2 & 1 & 1 & 0 & -1 \end{array}\right) \begin{matrix} \leftarrow -4 \cdot + \\ \leftarrow 2 \cdot + \\ \\ \end{matrix} \rightsquigarrow \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & -2 & -4 & 11 \\ 0 & 1 & 0 & 0 & -1 & 2 \\ 0 & 0 & 1 & 1 & 2 & -5 \end{array}\right).$$

Also ist

$$A^{-1} = \begin{pmatrix} -2 & -4 & 11 \\ 0 & -1 & 2 \\ 1 & 2 & -5 \end{pmatrix}.$$

Bestätigen Sie durch direktes Nachrechnen, dass $A\,A^{-1} = A^{-1}A = E$ ist!

Bemerkung 5.59 Ist $A \in \mathbb{K}^{n\times n}$ eine invertierbare Matrix, so lässt sich das lineare Gleichungssystem $A \cdot x = b$ mit $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ und $b = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$ eindeutig lösen. Die Lösung ist $x = A^{-1} \cdot b$.

5.4.5 Transponierte Matrizen

Aus einer gegebenen $m \times n$-Matrix

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \in \mathbb{K}^{m\times n}$$

über $\mathbb{K}$ kann man eine $n \times m$-Matrix dadurch bilden, dass man die Zeilen (unter Beibehaltung der Reihenfolge) in die Spalten (und umgekehrt) schreibt. Man erhält so die **transponierte Matrix**

$$A^\top := \begin{pmatrix} a_{11} & \cdots & a_{m1} \\ a_{12} & \cdots & a_{m2} \\ \vdots & & \vdots \\ a_{1n} & \cdots & a_{mn} \end{pmatrix} \in \mathbb{K}^{n\times m}.$$

Satz 5.60

1. *Für alle* $A, B \in \mathbb{K}^{m\times n}$ *gilt* $(A+B)^\top = A^\top + B^\top$.
2. *Für alle* $A \in \mathbb{K}^{m\times n}, B \in \mathbb{K}^{n\times q}$ *gilt* $(AB)^\top = B^\top A^\top$.
3. *Für alle* $A \in \mathbb{K}^{m\times n}$ *gilt* $A^{\top\top} = A$.
4. *Für alle invertierbaren* $A \in \mathbb{K}^{n\times n}$ *gilt* $\left(A^\top\right)^{-1} = \left(A^{-1}\right)^\top$.

Beweis: 1., 2. und 3. überprüft man durch direktes Nachrechnen. Zum Beweis von 4.: Aus $E^\top = E$ folgt zuerst wegen 2.

$$E = AA^{-1} = \left(AA^{-1}\right)^\top = \left(A^{-1}\right)^\top A^\top$$

und somit die Behauptung $\left(A^\top\right)^{-1} = \left(A^{-1}\right)^\top$. ■

5.5 Polynome

Gegeben sei ein beliebiger Körper $\mathbb{K}$.

Definition 5.61 Ein **Polynom** ist eine formale Summe der Form

$$f = a_0 + a_1 X + \cdots + a_{n-1}X^{n-1} + a_n X^n, \quad a_i \in \mathbb{K}.$$

Formal bedeutet hier, dass die Unbestimmte X nur als Symbol aufzufassen ist, aber nicht ein konkretes Element aus $\mathbb{K}$ repräsentieren soll. Die Menge aller Polynome über $\mathbb{K}$ bezeichnen wir mit $\mathbb{K}[X]$. Der **Grad** des Polynoms f ist definiert als

$$\deg f := \begin{cases} n & \text{falls } a_n \neq 0 \text{ und } a_k = 0 \text{ für alle } k > n, \\ -\infty & \text{falls } a_k = 0 \text{ für alle } k \geq 0. \end{cases}$$

Auf $\mathbb{K}[X]$ können wir eine Addition koeffizientenweise definieren:
Für $f = a_0 + a_1X^1 + \cdots + a_nX^n$ und $g = b_0 + b_1X + \cdots + b_nX^n$ setzen wir

$$f + g := (a_0 + b_0) + (a_1 + b_1)X + \cdots + (a_{n-1} + b_{n-1})X^{n-1} + (a_n + b_n)X^n.$$

Wir nehmen hier ohne Einschränkung an, dass $m = n$ ist. Denn wir können z.B. im Fall $m < n$ die Koeffizienten $b_{m+1}, \ldots, b_n$ einfach gleich 0 wählen.

Die Multiplikation ist etwas komplizierter: wir setzen

$$f \cdot g = c_0 + c_1X + \cdots + c_{m+n-1}X^{m+n-1} + c_{m+n}X^{m+n},$$

wobei die Koeffizienten c_i gegeben sind durch

$$\begin{aligned} c_0 &:= a_0 b_0, \\ c_1 &:= a_1 b_0 + a_0 b_1, \\ c_2 &:= a_2 b_0 + a_1 b_1 + b_2 a_0, \\ &\vdots \\ c_{m+n} &:= a_n b_m, \end{aligned}$$

oder allgemein

$$c_k := \sum_{i=0}^{k} a_i b_{k-i}.$$

D.h wir erhalten das Produkt von f und g, indem wir beide Ausdrücke unter Verwendung des Distributivgesetzes multiplizieren und die Koeffizienten gleichen Grades sammeln.

Satz 5.62 $(\mathbb{K}[X], +, \cdot)$ *ist ein kommutativer Ring mit Eins.*

Beweis: Ein Polynom $f = \sum_i a_i X^i$ ist durch die endliche Folge $(a_i)_{i\in\mathbb{N}_0}$ seiner Koeffizienten vollständig bestimmt. Die Menge $\mathbb{K}[X]$ lässt sich also äquivalent definieren als die Menge aller Folgen $(a_i)_{i\in\mathbb{N}_0}$ mit $a_i \in \mathbb{K}$, in denen alle bis auf endliche viele a_i gleich 0 sind. Addition und Multiplikation sind dann wie oben über die Koeffizienten definiert.

Das Nullelement (also das neutrale Element bezüglich der Addition) ist das Nullpolynom $0 := (0, 0, 0, \ldots)$. Die Assoziativität von $+$ überträgt sich komponentenweise von $\mathbb{K}$ auf $\mathbb{K}[X]$. Zu $(a_0, a_1, a_2, a_3, \ldots)$ ist $(-a_0, -a_1, -a_2, -a_3, \ldots)$ das additive Inverse. Durch direktes Nachrechnen erhält man die Assoziativität der Multiplikation und die Distributivgesetze. Das Einselement ist $1 := (1, 0, 0, 0, \ldots)$, wie man leicht nachprüft. Die Kommutativität folgt so:

$$(a_i)\cdot(b_i) = \left(\sum_{k=0}^{i} a_k b_{i-k}\right)_{i\in\mathbb{N}_0} \overset{l:=i-k}{=} \left(\sum_{l=0}^{i} a_{i-l} b_l\right)_{i\in\mathbb{N}_0} = \left(\sum_{l=0}^{i} b_l a_{i-l}\right)_{i\in\mathbb{N}_0} = (b_i)\cdot(a_i).$$

■

Bemerkung 5.63 (a) Für $f, g \in \mathbb{K}[X]$ ist

$$\deg(fg) = \deg f + \deg g.$$

(b) Die Abbildung

$$\Phi : \mathbb{K} \to \mathbb{K}[X], \quad a \mapsto (a, 0, 0, \ldots)$$

ist ein Ring-Homomorphismus, d.h. es gilt für alle $a, b \in \mathbb{K}$:

$$\Phi(a+b) = \Phi(a) + \Phi(b), \quad \Phi(a\,b) = \Phi(a) \cdot \Phi(b) \quad \text{und} \quad \Phi(1) = 1.$$

Außerdem ist Φ injektiv. Man kann deshalb a mit $(a, 0, 0, \ldots)$ identifizieren und erhält die „Einbettung“ $\mathbb{K} \subset \mathbb{K}[X]$. Insbesondere kann man das Einselement in $\mathbb{K}[X]$ mit $1 \in \mathbb{K}$ identifizieren.

5.6 *Kryptographie

Das Wort Kryptographie setzt sich aus den griechischen Worten „$\kappa\varrho\upsilon\pi\tau o\varsigma$(*kryptos*) = versteckt, geheim“ und „$\gamma\varrho\alpha\varphi\varepsilon\iota\nu$(grafein) = schreiben“ zusammen. Die Grundidee der Kryptographie ist es, gegebene Zeichen durch andere Zeichen zu ersetzen. Die Entschlüsselung muss dann diesen Vorgang wieder rückgängig machen.

Schon Cäsar soll schriftliche Befehle verschlüsselt haben. Er ersetzte dazu jeden Buchstaben durch den im Alphabet drei Positionen weiter hinten stehenden Buchstaben, also an Stelle von „a“ setzte er „d“, statt „b“ schrieb er „e“ usw. Wer das wusste, konnte diese Nachrichten dann wieder entschlüsseln.

Dieses einfache Verfahren bietet natürlich im Zeitalter moderner Computer keinen Schutz vor unberechtigtem Lesen der Nachricht. Man beschränkt sich heute auch nicht auf die 26 Zeichen des Alphabets, sondern fasst mehrere Zeichen zu einer Zeichenfolge zusammen und ordnet dieser eine Zahl a zu. Die Aufgabe der Kryptographie besteht darin, diese in eine Zahl $\mathrm{ch}(a)$ zu verschlüsseln - ein Vorgang, der durch die Dechiffrierung wieder rückgängig gemacht werden soll. An dieser Stelle kommt die Kongruenzrechnung modulo einer natürlichen Zahl n ins Spiel. Die entsprechenden Klassen haben einen Repräsentanten im Bereich $0, \ldots, n-1$, die wir als geeignete Kandidaten für die Kryptographie kennenlernen werden.

Wir haben gesehen, dass $(\mathbb{Z}/n\mathbb{Z}, \cdot)$ im Allgemeinen keine Gruppe ist, da nicht jedes Element ein Inverses besitzen muss. Zum Beispiel besitzt in $\mathbb{Z}/6\mathbb{Z}$ die Klasse $\tilde{3}$ mit Repräsentant 3 kein Inverses. Denn Multiplikation von 3 mit einer geraden Zahl g führt auf ein Vielfaches von 6, womit $\widetilde{g \cdot 3} = \tilde{0}$ gilt; Multiplikation von 3 mit einer ungeraden Zahl u führt auf $\widetilde{u \cdot 3} = \tilde{3}$, so dass es keine Zahl $z \in \mathbb{Z}$ gibt mit $\widetilde{z \cdot 3} = \tilde{1}$. Der Grund liegt darin, dass $\tilde{3}$ ein *Nullteiler* ($\underbrace{\tilde{2}}_{\neq \tilde{0}} \cdot \underbrace{\tilde{3}}_{\neq \tilde{0}} = \tilde{0}$) in $\mathbb{Z}/6\mathbb{Z}$ ist. Obwohl $\tilde{3} \neq \tilde{1}$ ist, gilt die Gleichung $\tilde{3} \cdot \tilde{3} = \tilde{3}$.

5.6.1 *Teilbarkeit

Um die Struktur von $(\mathbb{Z}/n\mathbb{Z}, \cdot)$ besser verstehen zu können, beginnen wir mit folgenden Begriffsbildungen.

Definition 5.64 Seien $a, b \in \mathbb{Z}\backslash\{0\}$. Dann heißt b **Teiler** von a, wenn es eine ganze Zahl $n \in \mathbb{Z}$ gibt mit $a = nb$. Man nennt dann a durch b teilbar und schreibt $b \,|\, a$.

Der Begriff der Teilbarkeit lässt sich noch für andere Ringe außer $(\mathbb{Z}, +, \cdot)$ in natürlicher Weise einführen, etwa für den Ring der Polynome $\mathbb{K}[X]$ über einem Körper $\mathbb{K}$. Der im Folgenden vorgestellte *Euklidische Algorithmus* zur Bestimmung des größten gemeinsamen Teilers lässt sich für Polynome in analoger Weise durchführen.

Definition 5.65 Seien $a, b \in \mathbb{Z}\backslash\{0\}$. $g \in \mathbb{N}$ heißt **größter gemeinsamer Teiler** von a und b, geschrieben $\mathrm{ggT}(a, b)$, falls gilt:

(i) $g \,|\, a$ und $g \,|\, b$

(ii) g ist die größte Zahl mit dieser Eigenschaft.

Gilt $\mathrm{ggT}(a, b) = 1$, so heißen a und b **teilerfremd**.

Bemerkung 5.66 Berechnen lässt sich der größte gemeinsame Teiler $\mathrm{ggT}(a, b)$ für $|a| > |b|$ mit Hilfe des **Euklidischen Algorithmus**, den wir hier kurz vorstellen. Zunächst gibt es zu zwei ganzen Zahlen $a, b \in \mathbb{Z}\backslash\{0\}$ mit $|a| \geq |b|$ stets eine ganze Zahl k_0 und eine natürliche Zahl r_0 mit der folgendenden Eigenschaft (**Division mit Rest**):

$$a = k_0 \cdot b + r_0 \quad \text{mit} \quad 0 \leq r_0 < |b| \tag{$*$}$$

Gilt $r_0 = 0$, so ist offensichtlich $|b|$ ein Teiler von a, und damit gilt $\mathrm{ggT}(a, b) = |b|$.

Die grundlegende Idee ist es nun zu sehen, dass für $r_0 > 0$ auf Grund der Gleichung $(*)$ gilt

$$g := \mathrm{ggT}(a, b) = \mathrm{ggT}(b, r_0) =: g_0.$$

Denn es ist $g \leq g_0$, da g die Zahlen a und b ohne Rest teilt, also nach Gleichung $(*)$ auch b und r_0. Nimmt man nun an, dass $g_0 > g$ gilt, so ist wieder nach Gleichung $(*)$ g_0 ein Teiler von b und von a, der größer als $g = \mathrm{ggT}(a, b)$ wäre. Dies wäre ein Widerspruch zur Maximalität von g.

Wir können also an Stelle von $\mathrm{ggT}(a, b)$ den $\mathrm{ggT}(b, r_0)$ der betragskleineren Zahlen b und r_0 berechnen. Division mit Rest führt analog zu oben mit einer ganzen Zahl k_1 und einer natürlichen Zahl r_1 auf die Darstellung

$$b = k_1 \cdot r_0 + r_1 \qquad 0 \leq r_1 < r_0.$$

Gilt in dieser Darstellung $r_1 = 0$, so ist $\mathrm{ggT}(b, r_0) = r_0$. Im Fall $r_1 \neq 0$ ist $\mathrm{ggT}(b, r_0) = \mathrm{ggT}(r_0, r_1)$, wobei auch hier wieder $r_1 < r_0$ gilt.

Setzt man dieses Verfahren weiter fort, so erhält man eine Folge von natürlichen Zahlen r_i, die immer kleiner werden: $r_0 > r_1 > r_2 \cdots$. Da das Verfahren bei einer

Zahl $r_0 \neq 0$ begonnen hat, muss irgendwann der Rest 0 auftreten. Es gibt also einen Index j mit der folgenden Eigenschaft:

$$\begin{aligned} r_{j-2} &= k_j \cdot r_{j-1} + r_j \quad , \quad r_j \neq 0 \\ r_{j-1} &= k_{j+1} \cdot r_j \end{aligned}$$

Analog zum oben Gesagten gilt dann $r_j = \mathrm{ggT}(r_{j-1}, r_j) = \mathrm{ggT}(r_{j-2}, r_{j-1})$. Nach dem Prinzip der vollständigen Induktion folgt damit

Hilfssatz 5.67 *Mit den obigen Notationen gilt* $\mathrm{ggT}(a, b) = r_j$.

Beispiel 5.68 Es gilt $\mathrm{ggT}(155, 9) = 1$, d.h. 155 und 9 sind teilerfremd.

$$\begin{aligned} 155 &= 17 \cdot 9 + 2 \\ 9 &= 4 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 \end{aligned}$$

Hilfssatz 5.69 (Lemma von Bézout) *Seien* $a, b \in \mathbb{Z}$ *und* $g = ggT(a, b)$. *Dann gibt es Zahlen* $s, t \in \mathbb{Z}$ *mit*

$$g = s \cdot a + t \cdot b.$$

Beweis: Setzen wir $r_0 := a$ und $r_1 := b$, so liefert der Euklidische Algorithmus eine Folge von Resten

$$r_{i+1} = r_{i-1} - q_i r_i, \quad i = 1, \ldots, n,$$

wobei nach dem n-ten Schritt der Rest $r_{n+1} = 0$ bleibt und $g = r_n$ der $\mathrm{ggT}(a, b)$ ist. Diese Gleichung lässt sich bequem durch Matrizen ausdrücken:

$$\begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \cdot \begin{pmatrix} r_{i-1} \\ r_i \end{pmatrix}.$$

Somit lässt sich der Euklidische Algorithmus durch eine Folge von Matrizen-Multiplikationen ausdrücken. Setzt man

$$Q_i := \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \quad \text{und} \quad S := Q_n Q_{n-1} \cdots Q_1,$$

so erhält man

$$\begin{pmatrix} g \\ 0 \end{pmatrix} = \begin{pmatrix} r_n \\ r_{n+1} \end{pmatrix} = Q_n Q_{n-1} \cdots Q_1 \cdot \begin{pmatrix} r_0 \\ r_1 \end{pmatrix} = S \cdot \begin{pmatrix} a \\ b \end{pmatrix}.$$

Ist $S = \begin{pmatrix} s & t \\ u & v \end{pmatrix}$, so erhält man sofort die gesuchte Gleichung

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

aus der ersten Zeile von S. ■

Bemerkung 5.70 Speziell für *teilerfremde* Zahlen $a, b \in \mathbb{Z}$ folgt daraus: Es gibt $s, t \in \mathbb{Z}$ mit $1 = s \cdot a + t \cdot b$.

Beispiel 5.71 Mit den in Beispiel 5.68 benutzten Zahlen gilt

$$1 = 9 - 4 \cdot 2 = 9 - 4 \cdot (155 - 17 \cdot 9) = 69 \cdot 9 - 4 \cdot 155.$$

5.6.2 *Die Einheitengruppe von $\mathbb{Z}/n\mathbb{Z}$

Nach diesen Vorarbeiten wenden wir uns wieder dem anfangs gestellten Problem zu.

Satz 5.72 *Die Menge der invertierbaren Elemente*

$$\mathbb{Z}/n\mathbb{Z}^* := \{\tilde{x} \in \mathbb{Z}/n\mathbb{Z} \mid \tilde{x} \text{ ist invertierbar}\}$$

ist bezüglich der Multiplikation $\cdot$ in $\mathbb{Z}/n\mathbb{Z}$ eine kommutative Gruppe.

Beweis: Zunächst ist $\mathbb{Z}/n\mathbb{Z}^* \neq \emptyset$, da das selbstinverse Element $\tilde{1}$ in $\mathbb{Z}/n\mathbb{Z}^*$ liegt. Weiter ist die Verknüpfung $\cdot$ auf $\mathbb{Z}/n\mathbb{Z}^*$ als Teilmenge von $\mathbb{Z}/n\mathbb{Z}$ assoziativ. Es bleibt zu zeigen, dass $\mathbb{Z}/n\mathbb{Z}^*$ abgeschlossen ist. Zunächst besteht $\mathbb{Z}/n\mathbb{Z}^*$ aus allen Elementen, die ein inverses Element haben. Damit gehört neben $\tilde{x} \in \mathbb{Z}/n\mathbb{Z}^*$ auch $\tilde{x}^{-1}$ zu $\mathbb{Z}/n\mathbb{Z}^*$, da deren Inverses wieder $\tilde{x}$ ist. Sind $\tilde{x}, \tilde{y} \in \mathbb{Z}/n\mathbb{Z}^*$, dann ist auch $\tilde{x} \cdot \tilde{y} \in \mathbb{Z}/n\mathbb{Z}^*$, da $\tilde{y}^{-1} \cdot \tilde{x}^{-1}$ Inverses dazu ist. Kommutativ ist die Gruppe, da das Verknüpfungsgebilde $(\mathbb{Z}/n\mathbb{Z}, \cdot)$ kommutativ ist. ■

Definition 5.73 $(\mathbb{Z}/n\mathbb{Z}^*, \cdot)$ heißt die **Einheitengruppe** von $(\mathbb{Z}/n\mathbb{Z}, \cdot)$. Die Elemente von $\mathbb{Z}/n\mathbb{Z}^*$ heißen **Einheiten** in $\mathbb{Z}/n\mathbb{Z}$.

Satz 5.74 *Es gilt*

$$\mathbb{Z}/n\mathbb{Z}^* = \{\tilde{x} \in \mathbb{Z}/n\mathbb{Z} \mid x \text{ und } n \text{ sind teilerfremd (d.h. } \mathrm{ggT}(x, n) = 1)\}.$$

Beweis:

„$\supset$“ $\mathrm{ggT}(x, n) = 1 \implies \exists s, t \in \mathbb{Z} : 1 = s \cdot x + t \cdot n \implies \exists \tilde{s}, \tilde{t} \in \mathbb{Z}/n\mathbb{Z} : \tilde{1} = \tilde{s} \cdot \tilde{x} + \tilde{t} \cdot \tilde{0} \implies \tilde{s} = \tilde{x}^{-1}$, es gibt also ein multiplikatives Inverses $\tilde{s}$ von $\tilde{x}$. Damit ist $\tilde{x} \in \mathbb{Z}/n\mathbb{Z}^*$.

„$\subset$“ Indirekt: Wir betrachten oBdA die Repäsentanten x in $\{0, ..., n-1\}$. Annahme $g := \mathrm{ggT}(x, n) > 1 \implies x = g \cdot u$ und $n = g \cdot l$, wobei u und l teilerfremd sind. Für das Produkt dieser Zahlen gilt $x \cdot l = g \cdot u \cdot l = n \cdot u$, woraus $\tilde{x} \cdot \tilde{l} = \tilde{0}$ folgt. Wegen $g > 1$ ist $\tilde{l} \neq \tilde{0}$ und damit $\tilde{x}$ ein Nullteiler in $(\mathbb{Z}/n\mathbb{Z}, \cdot)$, der nicht invertierbar ist. ■

Beispiel 5.75 Es gilt $\mathbb{Z}/6\mathbb{Z}^* = \{\tilde{1}, \tilde{5}\}$ und $\mathbb{Z}/10\mathbb{Z}^* = \{\tilde{1}, \tilde{3}, \tilde{7}, \tilde{9}\}$.

Bemerkung 5.76 Bemerkung 5.70 kann ausgenutzt werden, um die Inverse einer Zahl modulo n zu bestimmen (vgl. Beweis von Satz 5.74). Nach Beispiel 5.68 gilt

$$1 = 69 \cdot 9 - 4 \cdot 155 \quad \text{bzw.} \quad \tilde{1} = \widetilde{69} \cdot \tilde{9} - \tilde{4} \cdot \underbrace{\widetilde{155}}_{=\tilde{0}} = \widetilde{69} \cdot \tilde{9},$$

woraus sich $\tilde{9}^{-1} = \widetilde{69} \in \mathbb{Z}/155\mathbb{Z}$ ergibt.

Definition 5.77 Die Funktion

$$\varphi : \mathbb{N} \to \mathbb{N} \text{ mit } \varphi(n) := \text{ Anzahl der Elemente von } \mathbb{Z}/n\mathbb{Z}^*$$

heißt **Eulersche φ-Funktion**.

Beispiel 5.78 Für eine Primzahl p gilt $\varphi(p) = p - 1$. Sind p, q verschiedene Primzahlen, so gilt für $n = p \cdot q$ gerade $\varphi(n) = (p-1)(q-1)$.

Wie dieses Beispiel zeigt, lässt sich $\varphi(n)$ für spezielles n leicht berechnen. Die Bedeutung dieser Zahlen zeigt der folgende Satz:

Satz 5.79 (Euler-Fermat) *Für alle Einheiten $\tilde{a} \in \mathbb{Z}/n\mathbb{Z}^*$ gilt $\tilde{a}^{\varphi(n)} = \tilde{1}$.*

Beweis: Die abelsche Gruppe $(\mathbb{Z}/n\mathbb{Z}^*, \cdot)$ besitze die $\varphi(n)$ verschiedenen Elemente $\tilde{x}_1, \ldots, \tilde{x}_{\varphi(n)}$. Dann sind für jedes $\tilde{a} \in \mathbb{Z}/n\mathbb{Z}^*$ die Elemente $\tilde{x}_1 \cdot \tilde{a}, \ldots, \tilde{x}_{\varphi(n)} \cdot \tilde{a}$ paarweise verschieden (Das ergibt sich leicht durch Multiplikation von rechts mit $\tilde{a}^{-1}$) und es gilt

$$\tilde{x}_1 \cdot \ldots \cdot \tilde{x}_{\varphi(n)} = \tilde{x}_1 \cdot \tilde{a} \ldots \cdot \tilde{x}_{\varphi(n)} \cdot \tilde{a} = \tilde{x}_1 \cdot \ldots \cdot \tilde{x}_{\varphi(n)} \cdot \tilde{a}^{\varphi(n)}.$$

Wegen Hilfssatz 5.12 folgt daraus $\tilde{a}^{\varphi(n)} = \tilde{1}$. ■

Bemerkung 5.80 Aus Satz 5.79 folgt für $k \in \mathbb{N}$

$$\tilde{a}^{k\varphi(n)} = (\tilde{a}^{\varphi(n)})^k = \tilde{1}^k = \tilde{1}.$$

Da $\tilde{a}^{\varphi(n)} = \widetilde{a^{\varphi(n)}}$ kann Satz 5.79 für alle diejenigen $a \in \mathbb{Z}$ mit $\tilde{a} \in \mathbb{Z}/n\mathbb{Z}^*$ umgeschrieben werden in die Form

$$a^{k\varphi(n)+1} \equiv a \mod n\,.$$

Man ist nun daran interessiert, diese Darstellung möglichst für *alle* Zahlen $a \in \mathbb{Z}$ zu bekommen. Dazu beschränken wir uns auf bestimmte Gruppen.

Satz 5.81 *Seien $p \neq q$ Primzahlen und $n = p \cdot q$. Dann gilt für alle $a \in \mathbb{Z}$*

$$a^{\varphi(n)+1} \equiv a \mod n\,.$$

Beweis: Nach Bemerkung 5.80 haben wir die Gleichung nur noch für Zahlen $a \in \{0, \ldots, n-1\}$ nachzuweisen, die nicht teilerfremd zu n sind, also p oder q als Teiler haben. Sind p *und* q Teiler von a, so gilt $\tilde{a} = \tilde{0} \in \mathbb{Z}/n\mathbb{Z}$ und es ist $\tilde{a}^{\varphi(n)+1} = \tilde{0} = \tilde{a}$.

Sei p Teiler von a und q kein Teiler von a. Dann gilt modulo q nach Bemerkung 5.70

$$a, q \text{ teilerfremd} \implies a^{p-1}, q \text{ teilerfremd} \implies (a^{p-1})^{q-1} = a^{\varphi(n)} \equiv 1 \mod q.$$

Multiplikation mit a ergibt $a^{\varphi(n)+1} \equiv a \mod q$.

Andererseits gilt modulo p, da a durch p teilbar ist, $a \equiv 0 \mod p$, also auch $a^{\varphi(n)+1} \equiv 0 \mod p$ und damit $a^{\varphi(n)+1} \equiv a \mod p$.

Damit ist $(a^{\varphi(n)+1} - a)$ sowohl durch p als auch durch q teilbar. Da die Primzahlen p und q verschieden waren, muss auch $p \cdot q = n$ die Zahl $(a^{\varphi(n)+1} - a)$ teilen, was eine Umformulierung der Behauptung ist. Der Fall, dass q Teiler von a und p kein Teiler ist, verläuft analog. ■

5.6.3 *Der RSA-Algorithmus

Auf der Darstellung aus Satz 5.81 beruht ein bekanntes Verfahren der Kryptographie. Die Grundidee ist folgende:

Potenziert man eine Zahl a mit dem Exponenten $k \cdot \varphi(n) + 1$, so erhält man modulo n wieder a zurück. Dieses Potenzieren zerlegt man in zwei Schritte, indem man die Zahl $k \cdot \varphi(n) + 1$ als Produkt zweier Zahlen e (*encryption=Verschlüsselung*) und d (*decryption=Entschlüsselung*) schreibt:

$$e \cdot d = k \cdot \varphi(n) + 1.$$

Potenziert man nun ein beliebiges $\tilde{a}$ mit dem Exponenten e, so ergibt sich $a^e \mod n$. Weiteres Potenzieren mit d führt auf

$$\widetilde{a^e}^d = \tilde{a}^{e \cdot d} = \tilde{a}^{k\varphi(n)+1} = \tilde{a}.$$

Damit kann das Potenzieren mit e als Verschlüsselung aufgefasst werden, das weitere Potenzieren mit d als Entschlüsselung.

Bemerkung 5.82 Damit die oben beschriebene Ver- und Entschlüsselung möglich ist, müssen sowohl e als auch d zu $\varphi(n)$ teilerfremd sein. Modulo $\varphi(n)$ gilt also $\tilde{d} = \tilde{e}^{-1}$.

Dieses Verfahren ist der sogenannte **RSA-Algorithmus** aus dem Jahre 1977, der nach seinen Entwicklern Rivest, Shamir und Adleman benannt ist:

1. Wähle verschiedene Primzahlen p und q und setze $n := p \cdot q$. Damit gilt $\varphi(n) = (p-1) \cdot (q-1)$.

2. Wähle e mit $\mathrm{ggT}(e, \varphi(n)) = 1$ als Chiffrierschlüssel. Das Zahlenpaar (n, e) heißt **öffentlicher Schlüssel**.

3. Berechne Dechiffrierschlüssel d mit $d = e^{-1} \mod \varphi(n)$. Das Zahlenpaar (n, d) heißt **privater Schlüssel**.

4. Chiffriere eine natürliche Zahl a mit $0 \leq a < n$ mit dem öffentlichen Schlüssel durch $\mathrm{ch}(a) := a^e \mod n$

5. Dechiffriert wird $\mathrm{ch}(a)$ mit dem privaten Schlüssel durch $a := \mathrm{ch}(a)^d \mod n$.

Wir veranschaulichen den Algorithmus an einem Beispiel. Um einen Text in natürliche Zahlen zu transformieren, verwenden wir der Einfachheit halber nur Großbuchstaben und ordnen jedem Buchstaben die Position im Alphabet zu. Damit gilt die Ersetzung A $\to$ 1, B $\to$ 2,..., Y $\to$ 25, Z $\to$ 26. Bei Bedarf können Leerzeichen und Interpunktionszeichen weitere Zahlen zugeordnet werden.

Beispiel 5.83

1. Wähle $p := 11$ und $q := 7$. Damit gilt $n = p \cdot q = 77$ und $\varphi(77) = (p-1) \cdot (q-1) = 10 \cdot 6 = 60$.

2. Wähle e teilerfremd zu $\varphi(77) = 60$, etwa $e := 17$.

3. Bestimme d mit $\tilde{d} = \tilde{e}^{-1} \mod 60$ gemäß Bemerkung 5.76. In diesem Zahlenbeispiel gilt $d = 53$, was man mit $17 \cdot 53 = 901 \equiv 1 \mod 60$ leicht verifiziert.

4. Zur Verschlüsselung mit (77,17) wählen wir das Wort KRYPTOGRAPHIE bzw. die Zahlenfolge

   11 18 25 16 20 15 7 18 1 16 8 9 5.

   Wegen $11^4 \equiv 11 \mod 77$ ist

$$\begin{aligned} \mathrm{ch}(11) &= 11^{17} \mod 77 \\ &= ((11^4 \mod 77)^4 \mod 77)(11 \mod 77) \\ &= (11^2 \mod 77) \\ &= 44 \mod 77 \end{aligned}$$

Auch ohne die Zusatzeigenschaft $11^4 \equiv 11 \mod 77$ ist die Verschlüsselung durch folgendes kleines Programm leicht möglich:

$a := 11$;
$\mathrm{ch}(a) := 1$;
for j := 1 to e do $\mathrm{ch}(a) := \mathrm{ch}(a) \cdot a$ mod n;

Analoges Vorgehen für die restlichen Zahlen der Nachricht führt auf die verschlüsselte Nachricht:

$$44, 72, 9, 25, 48, 71, 28, 72, 1, 25, 57, 4, 3.$$

5. Dechiffriert wird mit dem privaten Schlüssel $(77, 53)$. Wegen $44^4 \equiv 44 \mod 77$ und daraus abgeleitet $44^{16} \equiv 44 \mod 77$ gestaltet sich für dieses Ergebnis die Dechiffrierung einfach. Es ist

$$\begin{aligned} 44^{53} \mod 77 &= ((44^{16} \mod 77)^3 \mod 77)(44^4 \mod 77)(44 \mod 77) \\ &= 44^5 \mod 77 \\ &= (44^4 \mod 77)(44 \mod 77) \\ &= 44^2 \mod 77 \\ &= 11 \mod 77 \end{aligned}$$

Analog zur Verschlüsselung liefert eine kleine Schleife mit dem privaten Schlüssel (diesesmal d statt e) und vertauschten Rollen von a und $\mathrm{ch}(a)$ die entschlüsselten Daten.

$\mathrm{ch}(a) := 44$;
$a := 1$;
for j := 1 to d do $a := a \cdot \mathrm{ch}(a)$ mod n;

Bemerkung 5.84 Allein aus dem Wissen des öffentlichen Schlüssels (e, n), lässt sich der private Schlüssel nicht bestimmen. Denn es geht bei dem Verfahren nicht darum, das inverse Element zu e modulo n zu bestimmen, sondern modulo $\varphi(n)$. Deshalb muss die Zahl $\varphi(n)$ bekannt sein. Diese kann man aber mit gängigen Methoden nur bestimmen, wenn die beiden Primzahlfaktoren von n bekannt sind. Das Knacken des Codes läuft mathematisch auf das Problem hinaus, eine Zahl n in ihre Primzahlen p und q zu faktorisieren. Bei sehr großen Primzahlen kann das auch mit modernsten Rechnern Monate dauern.

Literatur

[1] A. Beutelsbacher
Lineare Algebra
Vieweg Verlag, 1994

[2] E. Brieskorn
Lineare Algebra und Analytische Geometrie I
Vieweg Verlag, 1983

[3] E. Brieskorn
Lineare Algebra und Analytische Geometrie II
Vieweg Verlag, 1985

[4] R. Courant/H. Robbins
Was ist Mathematik?
Springer Verlag, 1967

[5] P. Davis, R. Hersh
Erfahrung Mathematik
Birkhäuser Verlag, 1985

[6] K. Devlin
Muster der Mathematik
Spektrum Verlag, 1998

[7] G. Fischer
Analytische Geometrie
Vieweg Verlag, 2001

[8] G. Fischer
Lineare Algebra
Vieweg Verlag, 2005

[9] T. Gowers
Mathematics, A very short introduction
Oxford University Press, 2002

[10] J. Hadamard
The Psychology of Invention in the Mathematical Field
Princeton University Press, 1945

[11] P.R. Halmos
Naive Mengenlehre
Vandenhoek & Ruprecht, 1976

[12] K. Jänich
Lineare Algebra, 10. Auflage
Springer Verlag, 2008

[13] M. Otte (Hrsg.)
Mathematiker über die Mathematik
Springer Verlag, 1974

[14] G. Polya
Schule des Denkens (engl. How to solve it)
Sammlung Dalp, 1949

[15] D. Ruelle
The Mathematician's brain
Princeton University Press, 2007

[16] A. Tarski
Einführung in die mathematische Logik
Vandenhoeck & Ruprecht, 1977.

Symbole

Index