Mathematik für Informatiker
Algebraische Strukturen

Vorlesungsmanuskript Wintersemester 2020/21

Janko Böhm

4. Februar 2021

Inhaltsverzeichnis

Abbildungsverzeichnis

Symbolverzeichnis

0

Einleitung

Wir wollen uns mit den Grundlagen der Zahlentheorie und der Algebra, insbesondere der linearen Algebra, beschäftigen. Neben Kombinatorik, Analysis, Geometrie und Topologie sind dies die wichtigsten Themenbereichen der reinen Mathematik, während Stochastik, Statistik und Numerik die wichtigsten Themenbereichen der angewandten Mathematik darstellen. Wir wollen zunächst einen kurzen Überblick über alle diese Teilgebiete bekommen:

Beginnen wir mit der Kombinatorik, die von allen genannten Bereichen mit den einfachsten Grundstrukturen startet (was aber nicht bedeutet, dass die Kombinatorik einfach wäre): Die Kombinatorik beschäftigt sich mit dem Zählen, basiert also auf den natürlichen Zahlen $\mathbb{N} = \{1, 2, 3, ...\}$. Mit Hilfe der Kombinatorik kann man zum Beispiel berechnen, dass es beim Ziehen der Lottozahlen $\binom{49}{6} \approx 14\,000\,000$ mögliche Ergebnisse gibt. Die Kombinatorik ist also eng mit der Wahrscheinlichkeitstheorie verknüpft, der sogenannten Stochastik: Sind alle Ereignisse beim Lotto gleich wahrscheinlich, dann ist die Wahrscheinlichkeit bei einem Spiel zu gewinnen gleich

$$\frac{1}{\binom{49}{6}} \approx \frac{1}{14\,000\,000}.$$

In der Informatik ist ein Teilgebiet der Kombinatorik besonders wichtig, die Graphentheorie. Graphen werden z.B. verwendet um Netzwerke zu beschreiben. Der Graph in Abbildung 1 beschreibt z.B. auf welche Weise vier Internet-Sites untereinander

verlinkt sind. Solche Graphen werden beispielsweise in Googles Page-Rank-Algorithmus verwendet.

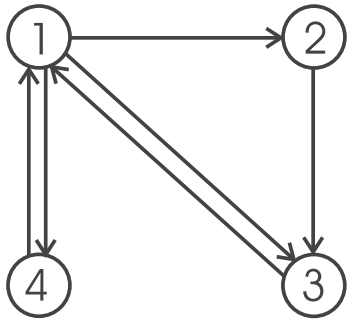


Abbildung 1: Gerichteter Graph von Links zwischen Internetseiten

Es gibt aber mehr ganze Zahlen als nur die in $\mathbb{N}$. Wie der Name Zahlentheorie schon andeutet, beschäftigen sich die Zahlentheoretiker mit den Eigenschaften der ganzen Zahlen in

$$\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$$

insbesondere mit der Beziehung zwischen der Addition und der Multiplikation. Viele zahlentheoretische Probleme können sehr einfach formuliert, aber nur sehr schwer gelöst werden. Das bekannteste Beispiel ist sicherlich Fermats letzter Satz von 1637: Es gibt für $n \geq 3$ keine (nichttriviale) ganzzahlige Lösung der Gleichung

$$x^n + y^n = z^n$$

Fermats letzter Satz wurde erst 1995 (von A. Wiles) bewiesen nach 350-jährigen Vorarbeiten, bei denen viele neue Konzepte in der Mathematik entwickelt wurden. Heute bestehen enge Beziehungen der Zahlentheorie zum Beispiel zur algebraischen Geometrie, Kombinatorik, Kryptographie und Codierungstheorie.

Was ist Algebra? Die Algebra ist ein umfangreiches Gebiet der Mathematik, das sich mit für alle Bereiche der Mathematik grundlegenden algebraischen Strukturen, wie Gruppen, Ringen und Körpern beschäftigt, d.h. mit der Frage, wie man auf Mengen Verknüpfungen einführen kann, wie z.B. die Addition und

Multiplikation von ganzen Zahlen. Die Public-Key Kryptographie verwendet z.B. Ergebnisse aus der Zahlentheorie und der Algebra. Ein weiterer wichtiger Berührungsbereich der Algebra besteht neben der Zahlentheorie mit der algebraischen Geometrie. Diese beschäftigt sich mit den Lösungsmengen von polynomialen Gleichungssystemen in mehreren Variablen über einem Körper K (zum Beispiel $K = \mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ der Körper der rationalen, reellen oder komplexen Zahlen). Zum Beispiel besteht die gemeinsame Lösungsmenge von $x^2 + 2y^2 = 3$ und $2x^2 + y^2 = 3$, d.h. der Durchschnitt von zwei Ellipsen, aus den 4 Punkten $(1,1), (-1,1), (1,-1), (-1,-1)$, siehe Abbildung 2. Bei algebrai-

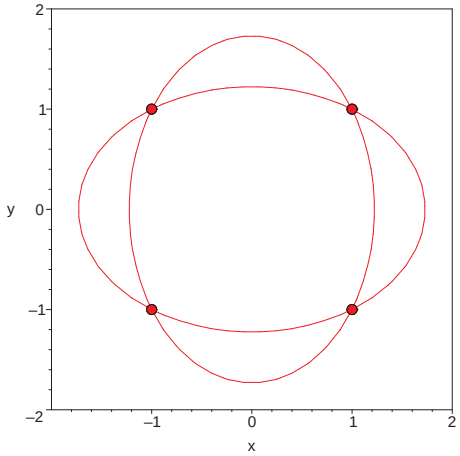


Abbildung 2: Vier Punkte

scher Geometrie über $K = \mathbb{Q}$ kommt die Zahlentheorie ins Spiel.

Der einfachste (aber in der Praxis sehr wichtige) Spezialfall sind lineare Gleichungssysteme über einem Körper K, das Kernthema der linearen Algebra. Hier lösen wir

$$\begin{aligned} a_{1,1}x_1 + \ldots + a_{1,m}x_m &= b_1 \\ &\vdots \\ a_{n,1}x_1 + \ldots + a_{n,m}x_m &= b_n \end{aligned}$$

mit $a_{ij} \in K$, $b_i \in K$ nach $x_j \in K$ (mit $i = 1, \ldots, n$ und $j = 1, \ldots m$). Lineare Algebra erlaubt uns z.B. aus den Link-Graphen wie in Abbildung 1 ein Page-Ranking für Suchmaschinen zu erstellen.

Als Anwendung der linearen Algebra werden wir fehlerkorrigierende Codes behandeln.

Wir wollen noch einen anderen wichtigen Spezialfall erwähnen, der jedoch über den hier betrachteten Stoff hinausgeht, Polynomgleichungen höheren Grades in einer einzigen Variablen x. Zum Beispiel kann man nach der Lösungsmenge der quadratischen Gleichung

$$ax^2 + bx + c = 0$$

fragen. Diese kann mit Wurzeln dargestellt werden durch

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Ebenso lassen sich mit Wurzelausdrücken die Lösungen von Gleichungen vom Grad $d = 3$ (Tartaglia 1535, Cardano 1545) und $d = 4$ (Ferrari 1522) darstellen, für $d \geq 5$ können die Lösungen im Allgemeinen nicht mehr mit Wurzeln geschrieben werden. Ein wichtiges Gebiet der Algebra, die Galoistheorie, behandelt die Frage, wann dies möglich ist.

Was ist Topologie? In der Topologie untersucht man Eigenschaften von Objekten, die sich unter stetigen Verformungen nicht ändern. Man sieht etwa, dass sich der Knoten in Abbildung 3 nicht ohne Aufschneiden entwirren läßt. Im Kapitel über

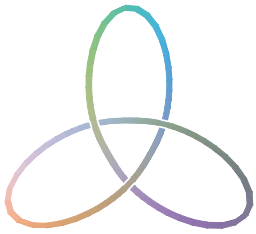


Abbildung 3: Knoten

Analysis werden wir uns mit der Stetigkeit von Abbildungen beschäftigen (d.h. mit stetigen Verformungen einer Geraden in den Graphen einer Funktion). Die Funktion mit dem Graphen in Abbildung 4 ist z.B. stetig, die in Abbildung 5 nicht. Der Begriff der Stetigkeit spielt eine wichtige Rolle in der Analysis und algebraischen Geometrie.

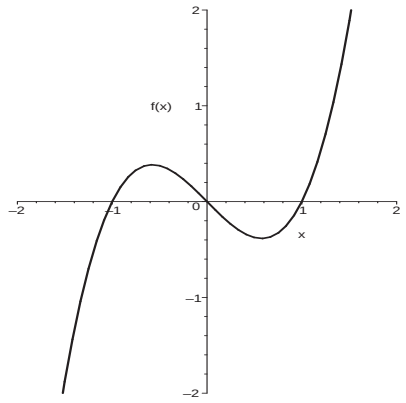


Abbildung 4: Eine stetige Funktion

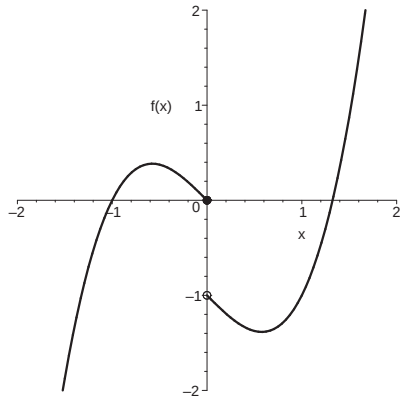


Abbildung 5: Eine unstetige Funktion

Was ist also Analysis? Die moderne Analysis geht auf die Infinitesimalrechnung zurück, die von Leibniz und Newton entwickelt wurde. Im Wesentlichen geht es darum, neben dem Stetigkeitsbegriff, den wir schon gesehen haben, auch einen Begriff der Steigung $f'(x)$ einer Funktion $f(x)$ zu entwickeln, indem man die Tangente (Abbildung 6) an einem gegebenen Punkt durch Sekanten (Abbildung 7) approximiert. Dabei verwenden wir, dass zwei verschiedene Punkte in der (x, y)-Ebene eindeutig eine Gerade festlegen. Für die Tangente würden wir gerne beide Punkte gleichsetzen. Durch einen einzelnen Punkt ist aber keine eindeutige Gerade mehr festgelegt. Wir können den zwei-

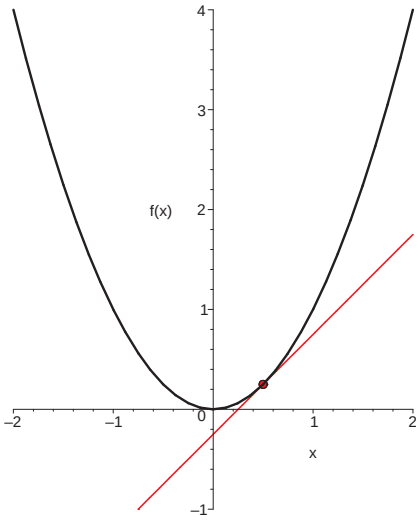


Abbildung 6: Die Tangente an $f(x) = x^2$ in $x = \frac{1}{2}$

ten Punkt also nur beliebig nahe an den Punkt heranführen, an dem wir die Tangente bestimmen wollen. Liefert dieser sogenannte Grenzwertprozess ein eindeutiges Ergebnis (unabhängig davon wie sich der zweite Punkt annähert), dann existiert eine Tangente und die Funktion heißt differenzierbar[1].

Die Funktion in Abbildung 8 hat in $x = 0$ dagegen offenbar keine vernünftige Tangente, denn wenn sich der zweite Punkt von links bzw. von rechts dem Punkt $(0, 0)$ nähert, erhalten wir unterschiedliche Grenzwerte der Sekantensteigung.

Gegeben eine Funktion $x \mapsto f(x)$ stellt sich natürlich die Frage, ob $x \mapsto f'(x)$ wieder eine Funktion ist, wo sie definiert ist und welche Eigenschaften sie hat. Solche Fragen beantwortet die

[1]Konkret haben wir für $f(x) = x^2$ die Steigung $f'(\frac{1}{2}) = 1$ der Tangente in $x = \frac{1}{2}$. Um diesen Wert zu bestimmen, gehen wir von der Steigung der Sekante durch die Punkte $(\frac{1}{2}, \frac{1}{4})$ und (x, x^2) aus. Deren Steigung ist gegeben durch

$$\frac{f(x) - f(\frac{1}{2})}{x - \frac{1}{2}} = \frac{x^2 - \left(\frac{1}{2}\right)^2}{x - \frac{1}{2}} = x + \frac{1}{2}.$$

Nähert sich nun x dem Wert $\frac{1}{2}$ an, dann nähert sich die Sekante der Tangenten an, und somit die Sekantensteigung der Tangentensteigung. Für $x \to \frac{1}{2}$ erhalten wir $f'(\frac{1}{2}) = \frac{1}{2} + \frac{1}{2} = 1$.

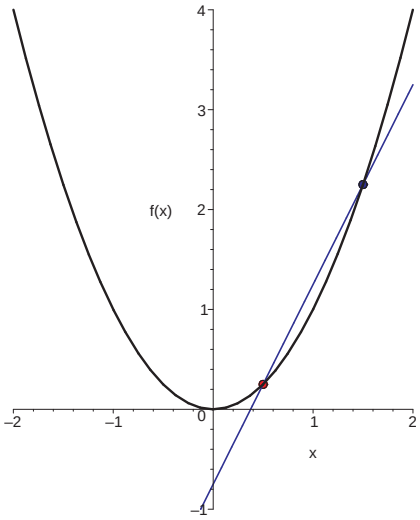


Abbildung 7: Eine Sekante an $f(x) = x^2$ in $x = \frac{1}{2}$

Differentialrechnung. Umgekehrt kann f' gegeben sein und man will f bestimmen. Dies ist ein Problem der Integralrechnung.

Die ursprüngliche Motivation für die Entwicklung der Analysis war das Newtonsche Kraftgesetz. Die Bewegung einer Masse m an einer Feder (siehe Abbildung 9) wird beschrieben durch die Gleichung

$$m \cdot x''(t) = -c \cdot x(t)$$

zwischen der Position $x(t)$ und der zweiten Ableitung $x''(t)$. Die Rückstellkraft der Feder ist dabei direkt proportional zu der Auslenkung $x(t)$ der Feder (mit Proportionalitätskonstante $c > 0$) und führt zu der Beschleunigung $x''(t)$ der Masse $m > 0$. Man spricht von einem sogenannten harmonischen Oszillator. Eine Gleichung dieser Form bezeichnet man auch als Differentialgleichung für die Funktion $x(t)$. Eine mögliche Lösung ist

$$x(t) = \sin(\sqrt{\frac{c}{m}} \cdot t),$$

siehe Abbildung 10, denn

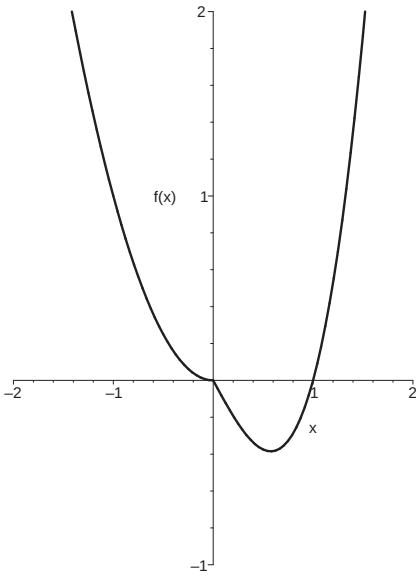


Abbildung 8: Eine Funktion die in $x = 0$ keine Tangente besitzt

$$x'(t) = \sqrt{\frac{c}{m}}\cos(\sqrt{\frac{c}{m}} \cdot t)$$
$$x''(t) = -\frac{c}{m}\sin(\sqrt{\frac{c}{m}} \cdot t).$$

Mit den Methoden der Analysis kann man die Menge aller möglichen Lösungen der Differentialgleichung beschreiben.

Was ist Numerik? Die Numerik versucht für Probleme der reinen Mathematik, die mit Hilfe von reellen oder komplexen Zah-

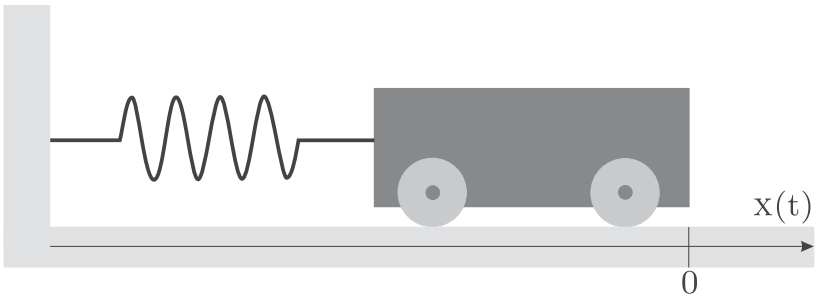


Abbildung 9: Harmonischer Oszillator

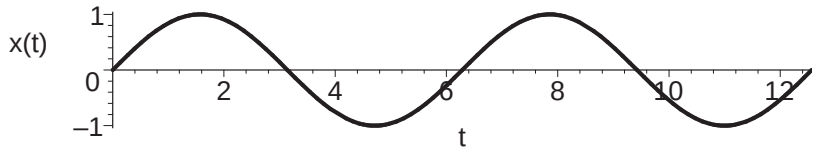


Abbildung 10: Eine Lösung für den harmonischen Oszillator

len formuliert werden, approximative Lösungen zu finden. Diese kann z.B. die Frage nach der Lösungsmenge eines Gleichungssystems oder einer Differenzialgleichung sein. Eine der wichtigsten Anwendungsfälle in der Numerik ist das Lösen von linearen Gleichungssystemen. Nichtlineare Probleme werden oft durch lineare approximiert. Beispielsweise kann man approximativ eine Nullstelle einer Funktion $x \mapsto f(x)$ mit Hilfe des Newtonverfahrens bestimmen: Ausgehend von einem Startwert x_1 berechnet man iterativ

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$$

d.h. x_{n+1} ist die Nullstelle der Tangente von

$$f(x) = x^2 - 2$$

in x_n, siehe Abbildung 11. Wie wir sehen werden, sind solche Approximationsverfahren eng verknüpft mit der Frage, was eine reelle Zahl wie etwa die Nullstelle $\sqrt{2}$ der obigen Funktion überhaupt ist. Zunächst werden wir beweisen, dass sich $\sqrt{2}$ nicht als Bruch von ganzen Zahlen darstellen lässt, also keine rationale Zahl ist.

Andererseits nimmt man in der Praxis in der Numerik den pragmatischen Standpunkt ein, dass wir oft sowieso nur eine Näherung der Nullstelle finden können. Deshalb werden auf dem Computer solche Rechnungen üblicherweise mit Fließkommazahlen durchgeführt, d.h. wir schreiben etwa

$$\sqrt{2} \approx 1.414213562.$$

Was ist Stochstik? Die Stochastik (oder auch Wahrscheinlichkeitstheorie) ist die mathematische Sprache zur Quantifizierung von zufälligen Prozessen. Dies reicht von Wurf einer Münze, über

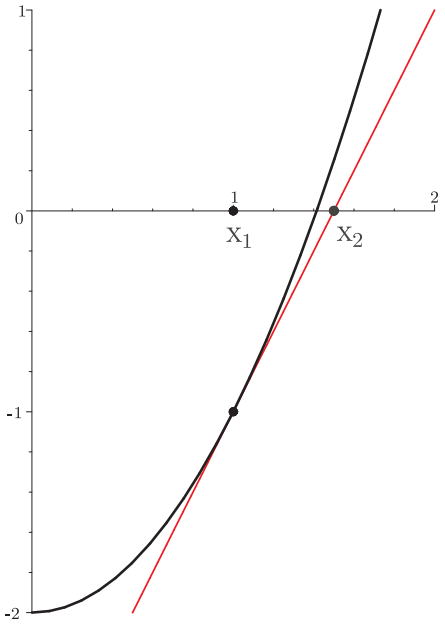


Abbildung 11: Newtonverfahren

die Beschreibung von Lotto über eine sogenannte Gleichverteilung (d.h. alle Ergebnisse einer Lottoziehung sind gleich wahrscheinlich, siehe oben), bis hin zur Analyse von Algorithmen. Neben der Gleichverteilung ist die bekannteste und wichtigste Zufallsverteilung die Gaußverteilung (oder auch Normalverteilung), die es sogar auf den 10 DM Schein geschafft hat, siehe Abbildung 12. Beispielsweise gehorchen die Körpergrößen von Menschen einer Gaußverteilung. Wie man schon an der Verwendung von Funktionen sieht, baut die Stochastik wesentlich auf den Methoden der Analysis auf.

Was ist Statistik? Die Statistik befasst sich mit dem Sammeln und Analysieren von Daten. Während wir also in der Stochastik untersuchen, was wir über die Eigenschaften des Resultats eines gegebenen datenerzeugenden Prozesseses sagen können, ist die Kernfragestellung der Statistik das dazu inverser Problem: Gegeben eine Menge an Daten, was können wir über den Prozess sagen, der diese Daten erzeugt hat. Das Gegenstück zur Statistik ist in der Informatik ist das Data Mining und das Machine Learning, wobei hier weniger Gewicht auf die exakte mathemati-

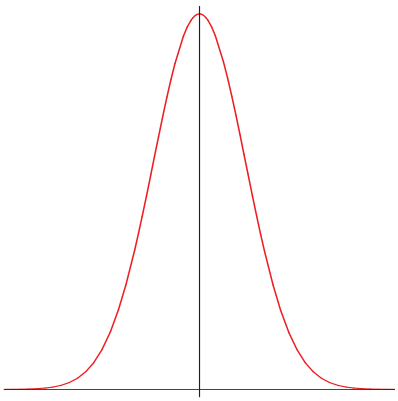


Abbildung 12: Normalverteilung

sche Beschreibung als vielmehr auf die Effizienz der verwendeten Algorithmen gelegt wird. Ein typisches Problem ist es, in einer Klasse von Funktionen eine Funktion zu finden, deren Funktionsgraph eine gegebene Datenmenge am besten beschreibt. In Abbildung 13 sehen wir die parallele Effizienz eines Computerprogramms, d.h. den Beschleunigungsfaktor geteilt durch die Anzahl der verwendeten Rechenkerne auf einem High-Performance-Computing Cluster und eine möglichst gute Approximation der Daten durch eine lineare Funktion

$$f(x) = a + b \cdot x$$

mit zwei geeignet gewählten Parametern a und b. Während ein solches univariates lineares Regressionsproblem leicht zu lösen ist, können moderne Algorithmen statistische Fragestellungen mit Millionen von Variablen und Tausenden von Parametern behandeln.

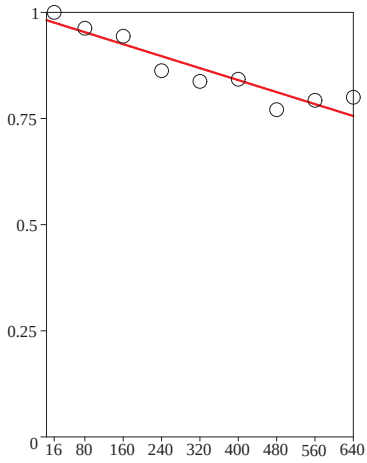


Abbildung 13: Lineare Regression

1

Elementare Logik

Die Basis jeder mathematischen Erkenntnis ist die Herleitung logischer Schlußfolgerungen, d.h. das Aufstellen und der Beweis von mathematischen Sätzen. Auch in der Informatik spielen Beweise eine zentrale Rolle. Hat man z.B. einen neuen Algorithmus entwickelt, so muss man zwei Dinge zeigen: Der Algorithmus ist korrekt, und er terminiert nach endlich vielen Schritten. Andere Anwendungen der Logik in der Informatik sind das automatische Beweisen und die Verifikation der Korrektheit von Software und Hardware. Letzteres ist besonders wichtig bei kritischen technischen Systemen, wie z.B. Flugzeugen. Wir führen zunächst kurz das Konzept von Aussagen ein und diskutieren dann die grundlegenden Beweisverfahren.

1.1 Aussagen, Mengen, Folgerungen

In Programmiersprachen (wir verwenden im Folgenden die Syntax von Maple [21]) spielen bedingte Anweisungen eine entscheidende Rolle, z.B.

```
if x>1 then
    ...
fi;
```

führt die Anweisungen `...` aus, falls die Variable x einen Wert größer als 1 annimmt. Der Ausdruck $x > 1$ kann genau zwei Werte annehmen: wahr oder falsch.

Definition 1.1.1 *Eine **Aussage** ist ein Objekt (mathematischer*

Ausdruck, sprachliches Gebilde), dem genau der Wahrheitswert ***wahr*** *oder* ***falsch*** *zugeordnet werden kann. Für wahr schreiben wir auch* ***true*** *oder* 1*, für falsch auch* ***false*** *oder* 0*.*

Beispiel 1.1.2 $1 + 2 = 3$ *ist eine (wahre) Aussage.*

Keine Aussage im mathematischen Sinne ist: Hallo!

Der Wahrheitswert der Aussage "Jede gerade Zahl > 2 *ist die Summe von zwei Primzahlen" ist unbekannt. Man bezeichnet sie als die Goldbachsche Vermutung.*

Der Ausdruck $x > 1$ ist auch keine Aussage, da wir erst x festlegen müssen, um zu entscheiden ob er wahr oder falsch ist. Dazu muss man natürlich erst sagen, welche Werte x zugelassen sind.

Definition 1.1.3 (Cantor) *Eine* ***Menge*** *ist eine Zusammenfassung* M *von bestimmten wohlunterschiedenen Objekten* m *unserer Anschauung oder unseres Denkens (die* ***Elemente*** *von* M *genannt werden) zu einem Ganzen.*

Ist m ein Element von M schreiben wir $m \in M$, die Menge M mit den Elementen $m_1, m_2, ...$ als

$$M = \{m_1, m_2, ...\}.$$

Die Menge ohne Elemente heißt **leere Menge** $\varnothing = \{\ \}$.

Bemerkung 1.1.4 *Die Definition interpretieren wir folgendermaßen: Objekte sind mathematische Objekte und die Zusammenfassung zu einem Ganzen ein neues Objekt. Wohlunterschieden bedeutet, dass man entscheiden kann, ob zwei gegebene Elemente* $a, b \in M$ *gleich* $(a = b)$ *oder verschieden* $(a \neq b)$ *sind.*

Dasselbe Objekt kann also nicht mehrfach ein Element einer Menge sein. Fassen wir z.B. die Zahlen $1, 1, 2$ zu einer Menge zusammen, erhalten wir

$$\{1, 1, 2\} = \{1, 2\}.$$

Weiter haben die Elemente einer Menge haben keine Reihenfolge. Es gilt also z.B.

$$\{1, 2\} = \{2, 1\}.$$

Beispiel 1.1.5 *Mengen sind beispielsweise die Menge der Ziffern*

$$\{0, 1, 2, ..., 9\},$$

die natürlichen Zahlen

$$\mathbb{N} = \{1, 2, 3, ...\}$$
$$\mathbb{N}_0 = \{0, 1, 2, 3, ...\},$$

die ganzen Zahlen

$$\mathbb{Z} = \{0, 1, -1, 2, -2, ...\}.$$

Damit können wir präzise machen, was der Ausdruck $x > 1$ ist:

Definition 1.1.6 *Eine* ***Aussageform*** *auf einer Menge M ist eine Zuordnung einer Aussage $A(x)$ zu jedem Element $x \in M$.*

In Programmiersprachen bezeichnet man eine Aussage oder Aussageform als **boolschen Ausdruck** (**boolean expression**). Der Wert eines solchen Ausdrucks (0 oder 1) wird in dem Datentyp **Boolean** gespeichert.

Definition 1.1.7 *Eine Aussageform, die nie wahr ist, heißt* ***unerfüllbar****, anderenfalls* ***erfüllbar****. Eine* ***Tautologie*** *ist eine Aussageform, die immer wahr ist.*

Beispiel 1.1.8 *Für $x \in \mathbb{Z}$ ist*

$$x^2 < 0$$

unerfüllbar,

$$x^2 > 0$$

erfüllbar (wahr für $x \neq 0$, falsch für $x = 0$), und

$$x^2 \geq 0$$

eine Tautologie.

Man beachte, dass Aussageformen und damit die Erfüllbarkeit von der zugrundeliegenden Menge abhängen: Auf $x \in \mathbb{C}$ ist $x^2 < 0$ erfüllbar, denn für die imaginäre Einheit i gilt $i^2 = -1$.

Gegeben mehrere bedingte Anweisungen, will man oft herausfinden, ob die eine aus der anderen folgt, z.B. können wir in

```
if x>1 then
    if x^2>1 then
        ...
    fi;
fi;
```

die zweite if-Abfrage weglassen, da aus $x > 1$ schon $x^2 > 1$ folgt. Dies ist eine **logische Schlussfolgerung**. Logische Schlussfolgerungen sind die Basis der Mathematik. Um präzise zu sein, müssen wir spezifizieren, in welcher Menge x liegt:

Für alle $x \in \mathbb{Z}$ gilt: Aus $x > 1$ wahr folgt, dass $x^2 > 1$ wahr.

Es ist ebenso möglich Aussagen der Form

$$\text{es existiert ein } x \in \mathbb{Z} \text{ mit } x < 0$$

bilden. Den Ausdruck "für alle" kürzt man auch mit $\forall$ ab, den Ausdruck "es existiert" mit $\exists$.

Aussagen, die mit Hilfe der Ausdrücke $\forall$, $\exists$ und Aussageformen formuliert werden können, nennt man Aussagen der **Prädikatenlogik**.

Eine wahre Aussage in der Prädikatenlogik bezeichnet man als **Satz**, ihre Herleitung als einen **Beweis**. Um die Wichtigkeit eines Satzes einzuordnen gibt es auch alternative Bezeichnungen: Bei einem Zwischenergebnis spricht man von einem **Lemma**, bei nicht so zentralen Ergebnissen, die aber trotzdem für sich genommen interessant sind, von einer **Proposition**. Erhält man einen Satz als Folgerung aus einem anderen Satz, so spricht man von einem **Corollar**.

In der Prädikatenlogik können wir aus gegebenen Aussagen oder Aussageformen neue bilden, z.B.

$$x > 1 \text{ und } x \text{ ist gerade.}$$

Dies ist ein Beispiel einer sogenannten logische Operation. Das Folgende in diesem Abschnitt lässt sich sowohl für Aussagen als auch Aussageformen anwenden. Wir beschränken uns bei der Formulierung auf Aussagen.

Definition 1.1.9 *Eine **logische Operation** verknüpft gegebene Aussagen zu einer neuen Aussage. Wenn wir die Werte der gegebenen Aussagen in einer logischen Operation als Unbestimmte betrachten, dann erhalten wir eine Aussageform, die wir als **logische Formel** bezeichnen.*

Definition 1.1.10 *Für eine Aussage A ist die **Negation** $\neg A$ (**nicht** A) wahr wenn A falsch ist, und falsch, wenn A wahr ist.*

*Für Aussagen A und B ist die **Konjunktion** $A \wedge B$ (A **und** B) wahr, wenn beide Aussagen wahr sind, und falsch sonst.*

*Die **Disjunktion** $A \vee B$ (A **oder** B) ist wahr, wenn mindestens eine der beiden Aussagen wahr ist, und falsch sonst.*

In einem Programm würden wir typischerweise schreiben

```
if not A then ... fi;
if A and B then ... fi;
if A or B then ... fi;
```

Bemerkung 1.1.11 *Eine logische Formel kann man eindeutig festlegen, indem man für alle möglichen Werte der gegebenen Aussagen die Werte der abgeleitenen Aussage angibt, z.B. mit einer sogenannten **Wahrheitswerttafel**:*

1) Nicht:

A	$\neg A$
1	0
0	1

2) Und:

A	B	$A \wedge B$
1	1	1
0	1	0
1	0	0
0	0	0

3) Oder:

A	B	$A \vee B$
1	1	1
0	1	1
1	0	1
0	0	0

Auch die logische Schlussfolgerung kann man mit Hilfe einer logischen Operation ausdrücken.

Definition 1.1.12 *Die **Implikation** $A \Rightarrow B$ ist falsch, wenn A wahr und B falsch ist. Anderenfalls ist sie wahr.*

A	B	$A \Rightarrow B$
1	1	1
0	1	1
1	0	0
0	0	1

*Für zwei Aussagen A und B ist die **Äquivalenz** $A \Leftrightarrow B$ wahr, wenn $A \Rightarrow B$ und $B \Rightarrow A$ wahr sind. Anderenfalls ist die Äquivalenz falsch.*

A	B	$A \Rightarrow B$	$B \Rightarrow A$	$A \Leftrightarrow B$
1	1	1	1	1
0	1	1	0	0
1	0	0	1	0
0	0	1	1	1

*Ist die Äquivalenz für gegebene Ausagen A und B wahr, so heißen diese **äquivalent**. Analog ist $A(x) \Leftrightarrow B(x)$ für Aussageformen $A(x)$ und $B(x)$ auf der Menge M eine Tautologie, so heißen diese Aussageformen äquivalent.*

Durch

$$(A \wedge (A \Rightarrow B)) \Rightarrow B$$

ist eine Tautologie gegeben, wie wir anhand der Wahrheitswerttafel überprüfen können:

A	B	$A \Rightarrow B$	$A \wedge (A \Rightarrow B)$	B	$(A \wedge (A \Rightarrow B)) \Rightarrow B$
1	1	1	1	1	1
0	1	1	0	1	1
1	0	0	0	0	1
0	0	1	0	0	1

Mit Hilfe der Tautologie $(A \wedge (A \Rightarrow B)) \Rightarrow B$ kann man die logische Schlussfolgerung durch die Implikation ausdrücken:

Bemerkung 1.1.13 *Für Aussageformen $A(x)$ und $B(x)$ mit $x \in M$ sind die folgenden Aussagen äquivalent:*

1) *Für alle $x \in M$ mit $A(x)$ wahr, ist $B(x)$ wahr.*

2) *Die Aussageform $A(x) \Rightarrow B(x)$ auf M ist eine Tautologie (d.h. für alle $x \in M$ ist $A(x) \Rightarrow B(x)$ wahr.).*

*Wir sagen, dass $x \in M$ ein **Gegenbeispiel** zu der Gültigkeit dieser Aussagen ist, wenn $B(x)$ den Wahrheitswert falsch, aber $A(x)$ den Wert wahr hat.*

Beispiel 1.1.14 *Ein Gegenbeispiel zu der Gültigkeit der Aussage*

$$\text{für alle } x \in \mathbb{Z} \text{ gilt } x > 0 \Rightarrow x > 1$$

ist $x = 1$.

Bemerkung 1.1.15 *Aus falschen Aussagen können richtige folgen, z.B. folgt durch Quadrieren*

$$1 = -1 \Longrightarrow 1 = 1^2 = (-1)^2 = 1.$$

In der Mathematik ist es dennoch sehr wichtig, auch aus möglicherweise falschen Aussagen Folgerungen ziehen zu können, um diese am Ende (wenn man geschickt vorgegangen ist, nicht so wie gerade beim Quadrieren) als falsch zu erkennen:

$$7 - 9 > 1 \Longrightarrow -2 > 1 \Longrightarrow -3 > 0$$

Hier steht also: Falls $7-9 > 1$ wahr ist, dann ist auch $-2 > 1$ wahr, und falls $-2 > 1$ wahr ist, dann ist auch $-3 > 0$ wahr. Letzteres ist falsch, also muss auch $-2 > 1$ falsch sein, also auch $7 - 9 > 1$. Dieses Beweisprinzip (den Beweis durch Kontraposition) werden wir noch ausführlich in Abschnitt 1.2 diskutieren.

Es gelten auch die Implikationen in der anderen Richtung, also haben wir sogar Äquivalenzen

$$7 - 9 > 1 \Longleftrightarrow -2 > 1 \Longleftrightarrow -3 > 0.$$

Hier stehen also 3 falsche Aussagen

$$7 - 9 > 1 \qquad -2 > 1 \qquad -3 > 0$$

und 2 *wahre Aussagen*

$$7 - 9 > 1 \Longleftrightarrow -2 > 1 \qquad -2 > 1 \Longleftrightarrow -3 > 0,$$

die wir durch Verknüpfung von falschen Aussagen mittels $\Leftrightarrow$ *erhalten.*

Tatsächlich liefert die obige Kette von Äquivalenzen eine weitere wahre Aussage, nämlich die Äquivalenz

$$7 - 9 > 1 \Longleftrightarrow -3 > 0.$$

Über das Beweisprinzip einer solchen Kette von Implikationen oder Äquivalenzen werden wir auch noch allgemein in Abschnitt 1.2 sprechen.

Auch die folgende unerfüllbare logische Formel und die nachfolgende Tautologie werden in allgemeinen Beweisprinzipien eine wichtige Rolle spielen:

Beispiel 1.1.16 *Sei* A *eine Aussage. Dann ist logische Formel* $A \wedge \neg A$ *unerfüllbar:*

A	$\neg A$	$A \wedge \neg A$
1	0	0
0	1	0

Beispiel 1.1.17 *Die logische Formel*

$$(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$$

ist unabhängig von den Werten der Aussagen A *und* B *immer wahr, also eine Tautologie. Die Aussagen*

$$A \Rightarrow B$$

und

$$\neg B \Rightarrow \neg A$$

sind somit äquivalent.

Beweis. Wir zeigen dies mit Hilfe einer Wahrheitswerttafel:

A	B	$A \Rightarrow B$	$\neg B$	$\neg A$	$\neg B \Rightarrow \neg A$	$(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$
1	1	1	0	0	1	1
1	0	0	1	0	0	1
0	0	1	1	1	1	1
0	1	1	0	1	1	1

■

Zum Abschluss leiten wir noch einige allgemein nützliche Tautologien her:

Satz 1.1.18 *Seien A, B und C Aussagen. Dann sind folgenden logischen Formeln Tautologien:*

1) Für $\wedge$:

(a) Assoziativgesetz $A \wedge (B \wedge C) \Leftrightarrow (A \wedge B) \wedge C$.

(b) Kommutativgesetz $A \wedge B \Leftrightarrow B \wedge A$.

2) Für $\vee$:

(a) Assoziativgesetz $A \vee (B \vee C) \Leftrightarrow (A \vee B) \vee C$.

(b) Kommutativgesetz $A \vee B \Leftrightarrow B \vee A$.

3) Distributivgesetze für $\wedge$ und $\vee$:

$$A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C)$$
$$A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$$

4) Idempotenz:

$$(A \wedge A) \Leftrightarrow A \qquad (A \vee A) \Leftrightarrow A$$

5) Für die Negation:

$$\neg(\neg A) \Leftrightarrow A \qquad A \vee \neg A$$

6) De Morgansche Gesetze der Aussagenlogik:

$$\neg(A \wedge B) \Leftrightarrow (\neg A \vee \neg B) \qquad \neg(A \vee B) \Leftrightarrow (\neg A \wedge \neg B)$$

7) Für die Implikation:

$$(A \Rightarrow B) \Leftrightarrow (\neg A \vee B)$$

Beweis. Wir zeigen beispielhaft einige der Tautologien:

A	$\neg A$	$A \vee \neg A$
1	0	1
0	1	1

A	$\neg A$	$\neg(\neg A)$	$\neg(\neg A) \Leftrightarrow A$
1	0	1	1
0	1	0	1

Für die weiteren Aussagen siehe Übung 1.1. ■

1.2 Elementare Beweismethoden

Um zu zeigen, dass

$$A(x) \Rightarrow B(x)$$

für alle x gilt, kann man diese Implikation in eine Verkettung von einfacheren Implikationen

$$A(x) \Rightarrow C(x) \Rightarrow B(x)$$

zerlegen, solange bis man das Problem auf bekannte Implikationen zurückgeführt hat. Formal gesprochen verwenden wir also, dass

$$(A \Rightarrow C \ \wedge \ C \Rightarrow B) \Rightarrow (A \Rightarrow B)$$

für beliebige Aussagen A, B, C eine Tautologie ist (zeigen Sie dies als Übung). Eine solche Strategie bezeichnet man als **direkten Beweis**. Ein Beispiel gibt der der Beweis des folgenden Satzes:

Satz 1.2.1 *Für alle $n, m \in \mathbb{N}$ gilt: Ist n gerade $(2, 4, 6, ...)$ und m ungerade $(1, 3, 5, ...)$, dann ist $n + m$ ungerade.*

Beweis. n gerade und m ungerade $\Rightarrow$ es gibt $s, t \in \mathbb{N}$ mit $n = 2s$ und $m = 2t - 1 \Rightarrow$ es gibt $s, t \in \mathbb{N}$ mit

$$n + m = 2(s + t) - 1$$

$\Rightarrow n+m$ ist ungerade. ■

Manchmal ist es einfacher die äquivalente negierte Aussage zu zeigen. Wegen der Tautologie

$$(A \Rightarrow B) \Longleftrightarrow (\neg B \Rightarrow \neg A)$$

aus Beispiel 1.1.17 können wir statt

$$A(x) \text{ wahr} \Rightarrow B(x) \text{ wahr}$$

auch

$$B(x) \text{ falsch} \Rightarrow A(x) \text{ falsch}$$

zeigen. Dies bezeichnet man auch als Beweis durch **Kontraposition** (indirekter Beweis). Der Beweis von folgendem Lemma gibt ein Beispiel:

Lemma 1.2.2 *Für alle $n \in \mathbb{N}$ gilt: Ist n^2 gerade, dann ist auch n gerade.*

Beweis. Sei n ungerade, also $n = 2t - 1$ mit einer natürlichen Zahl $t \in \mathbb{N}$. Dann ist

$$n^2 = 4t^2 - 4t + 1$$

also ungerade. ■

Bei dem **Widerspruchsbeweis** der Aussage A nehmen wir an, dass A nicht wahr ist und führen dies zu einem Widerspruch. Dazu zeigen wir, dass eine Aussage B und ebenso $\neg B$ gilt. Dies ist aber nicht möglich, da $B \wedge \neg B$ immer falsch ist. Somit muss A wahr sein.

Der Beweis des folgenden Satzes gibt ein typisches Beispiel eines Widerspruchsbeweises:

Satz 1.2.3 *$\sqrt{2}$ ist **irrational**, d.h. keine rationale Zahl.*

Beweis. Angenommen $\sqrt{2}$ ist eine rationale Zahl, äquivalent $\sqrt{2}$ ist ein gekürzter Bruch $\frac{a}{b}$ von natürlichen Zahlen $a, b \in \mathbb{N}$. Aus $\sqrt{2} = \frac{a}{b}$ folgt

$$2b^2 = a^2$$

d.h. a^2 ist gerade, mit Lemma 1.2.2 ist also auch a gerade. Somit können wir schreiben $a = 2s$ mit einer natürlichen Zahl s, also

$$2b^2 = 4s^2.$$

Damit ist

$$b^2 = 2s^2$$

gerade, also mit Lemma 1.2.2 auch b gerade. Somit können wir schreiben $b = 2t$ mit einer natürlichen Zahl t, also war

$$\frac{a}{b} = \frac{2s}{2t}$$

nicht gekürzt. Wir haben also gezeigt: Ist $\frac{a}{b}$ gekürzt, dann ist $\frac{a}{b}$ nicht gekürzt, ein Widerspruch. Einen Widerspruch kennzeichnet man auch kurz mit dem Blitzsymbol $\lightning$. ■

Die verschiedenen Beweismethoden lassen sich natürlich auch miteinander kombinieren.

1.3 Vollständige Induktion

Angenommen wir wollen für jede natürliche Zahl $n \in \mathbb{N}$ eine Aussage $A(n)$ zeigen. Haben wir bewiesen, dass gilt:

1) **Induktionsanfang**: $A(1)$ ist wahr,

2) **Induktionsschritt**: Die Implikation $A(n) \Rightarrow A(n+1)$ ist wahr für alle $n \in \mathbb{N}$,

dann liefert dies eine Kette

$$A(1) \text{ wahr } \Rightarrow A(2) \text{ wahr } \Rightarrow A(3) \text{ wahr } \Rightarrow \dots,$$

es ist also $A(n)$ wahr für jede natürliche Zahl n. Anschaulich zeigen wir also eine Aufpunktaussage und einen Vektor von Aussagen, den wir unendlich oft auf den Aufpunkt addieren.

Im Induktionsschritt bezeichnen wir $A(n)$ wahr auch als die **Induktionsvoraussetzung**.

Als Beispiel für einen Beweis mittels vollständiger Induktion zeigen wir eine Aussage über Summen.

Notation 1.3.1 *Für Zahlen $a_n, a_{n+1}, ..., a_{m-1}, a_m$ mit $n \leq m$ schreiben wir*

$$\sum_{k=n}^{m} a_k := a_n + a_{n+1} + ... + a_{m-1} + a_m$$

für deren ***Summe****.*

Genauso verwenden wir

$$\prod_{k=n}^{m} a_k := a_n \cdot ... \cdot a_m$$

für das ***Produkt****.*

Bemerkung 1.3.2 *Gegeben eine Liste $a = (a_1, ..., a_m)$ berechnet z.B. das folgende Computerprogramm die Summe $s = \sum_{k=1}^{m} a_k$:*

```
s:=0;
for k from 1 to m do
    s:=s+a[k];
od;
```

Beispiel 1.3.3 *Es ist*

$$\sum_{k=2}^{4} 1 = 1 + 1 + 1 = 3$$
$$\prod_{k=1}^{4} k = 1 \cdot 2 \cdot 3 \cdot 4 = 24$$
$$\sum_{k=1}^{4} k = 1 + 2 + 3 + 4 = 10.$$

Können wir eine allgemeine Formel für $\sum_{k=1}^{n} k$ finden?

Satz 1.3.4 *Für alle natürlichen Zahlen gilt*

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

Beweis. *Induktionsanfang* $n = 1$: Es ist

$$\sum_{k=1}^{1} k = 1 = \frac{1 \cdot (1+1)}{2}.$$

Induktionsschritt n nach $n+1$: Es ist

$$\sum_{k=1}^{n+1} k = \sum_{k=1}^{n} k + (n+1)$$

also folgt mit der Induktionsvoraussetzung

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

dass

$$\begin{aligned}\sum_{k=1}^{n+1} k &= \frac{n(n+1)}{2} + (n+1) \\ &= \frac{n(n+1)+2(n+1)}{2} \\ &= \frac{(n+1)(n+2)}{2}.\end{aligned}$$

■

Für weitere Beispiele siehe auch die Übungen 1.2, 1.3, 1.4, und 1.5.

Bemerkung 1.3.5 *Das Analogon zum Induktionsbeweis in der Informatik ist der* ***rekursive Algorithmus****. Beispielsweise berechnet das folgende Programm die Summe*

$$\sum_{k=1}^{n} k$$

rekursiv:

```
sumk:=proc(n)
    if n=1 then return(1);fi;
    return(sumk(n-1)+n);
end proc;
```

Die erste Zeile innerhalb der Prozdur enspricht dem Induktionsanfang $n = 1$*, die zweite Zeile dem Induktionsschritt* $n-1$ *nach* n *für* $n \geq 2$*.*

Für ein weiteres Beispiel siehe auch die Übungsaufgaben 1.8 und 1.9.

1.4 Übungsaufgaben

Übung 1.1 *Zeigen Sie, dass folgenden logischen Formeln immer wahr (d.h. Tautologien) sind:*

1) Für $\wedge$:

(a) Assoziativität $A \wedge (B \wedge C) \Leftrightarrow (A \wedge B) \wedge C$.

(b) Kommutativität $A \wedge B \Leftrightarrow B \wedge A$.

2) Für $\vee$:

(a) Assoziativität $A \vee (B \vee C) \Leftrightarrow (A \vee B) \vee C$.

(b) Kommutativität $A \vee B \Leftrightarrow B \vee A$.

3) Distributivgesetze für $\wedge$ und $\vee$:

$$A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C)$$
$$A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$$

4) Idempotenz:

$$(A \wedge A) \Leftrightarrow A \qquad (A \vee A) \Leftrightarrow A$$

5) Für das Komplement:

$$\neg(\neg A) \Leftrightarrow A \qquad A \vee \neg A \qquad \neg(A \wedge \neg A)$$

6) De Morgansche Gesetze der Aussagenlogik:

$$\neg(A \wedge B) \Leftrightarrow (\neg A \vee \neg B)$$
$$\neg(A \vee B) \Leftrightarrow (\neg A \wedge \neg B)$$

7) Für die Implikation:

$$(A \Rightarrow B) \Leftrightarrow (\neg A \vee B)$$

Übung 1.2 *Zeigen Sie mit vollständiger Induktion, dass*

$$\sum_{k=1}^{n} k^2 = \frac{n\,(n+1)\,(2n+1)}{6}$$

für jedes $n \in \mathbb{N}$ gilt.

Übung 1.3 *Sei $n \in \mathbb{N}$. Stellen Sie eine Formel für*

$$\sum_{k=1}^{n} k^3$$

auf und beweisen Sie diese.

Übung 1.4 *Zeigen Sie mit vollständiger Induktion*

$$\sum_{k=1}^{n} k^3 = \left(\sum_{k=1}^{n} k\right)^2$$

für jedes $n \in \mathbb{N}$.

Übung 1.5 *Eine Zahl $a \in \mathbb{Z}$ heißt Teiler von $m \in \mathbb{Z}$, wenn es ein $b \in \mathbb{Z}$ gibt mit*

$$m = a \cdot b.$$

Zeigen Sie: Für jedes $n \in \mathbb{N}$, ist 3 ein Teiler von

$$n^3 - n.$$

Hinweis: Vollständige Induktion.

Übung 1.6 *Bestimmen Sie für beliebiges $n \in \mathbb{N}$ das Produkt*

$$\prod_{k=1}^{n} 2^k.$$

Übung 1.7 *1) Schreiben Sie jeweils ein Programm, das für eine Liste $a = (a_1, \ldots, a_n) \in \mathbb{Z}^n$ die Summe*

$$\sum_{k=1}^{n} a_k$$

bzw. das Produkt

$$\prod_{k=1}^{n} a_k$$

berechnet.

2) Vergleichen Sie für verschiedene n Ihr Ergebnis aus Aufgabe 1.6 mit dem Ihres Programms.

Übung 1.8 *Das Spiel "Die Türme von Hanoi" besteht aus* 3 *Spielfeldern, auf denen n Scheiben paarweise verschiedener Größe gestapelt werden können (siehe Abbildung 1.1).*

Zu Beginn des Spiels sind alle Scheiben auf einem der Spielfelder der Größe nach zu einem Turm gestapelt. Ziel des Spiels ist, den Anfangsstapel auf ein anderes Feld zu versetzen.

Dazu darf in jedem Spielzug die oberste Scheibe eines beliebigen Turms auf einen anderen Turm, der keine kleinere Scheibe enthält, gelegt werden.

Geben Sie einen Algorithmus an, der dieses Spiel löst, stellen Sie eine Formel für die Anzahl der notwendigen Züge auf, und beweisen Sie diese mit vollständiger Induktion.

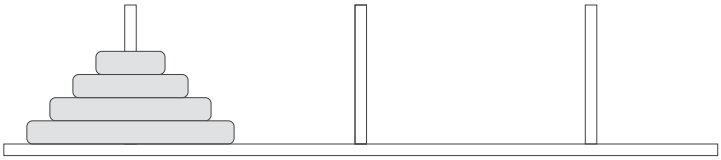


Abbildung 1.1: Die Türme von Hanoi.

Übung 1.9 *Schreiben Sie ein rekursives Programm, das das Spiel "Die Türme von Hanoi" löst.*

2

Grundkonstruktionen

In diesem Abschnitt behandeln wir Grundkonstruktionen mit denen wir aus gegebenen mathematischen Objekten neue konstruieren können. Allgemein erlaubt uns der Mengenbegriff ein neues mathematisches Objekt durch Zusammenfassen von gegebenen Objekten zu bilden. Zum Beispiel fasst man alle natürlichen Zahlen in der Menge

$$\mathbb{N} = \{1, 2, 3, ...\}$$

zusammen. Dazu diskutieren wir zunächst einige Grundkonstruktionen mit denen man aus gegebenen Mengen eine neue Menge bilden kann. Ausgehend vom Mengenbegriff beschäftigen wir uns dann mit mit der Frage, wie man zwei gegebene Mengen in Beziehung setzen kann, insbesondere mit Abbildungen zwischen Mengen und Äquivalenzrelationen auf Mengen.

2.1 Elementare Mengenkonstruktionen

Notation 2.1.1 *Sei N eine Menge und $A(x)$ eine Aussageform auf N. Oft wollen wir Objekte $x \in N$, die $A(x)$ erfüllen, zu einer Menge*

$$M = \{x \in N \text{ mit } A(x) \text{ wahr}\}$$

zusammenfassen. Dies kürzen wir mit

$$M = \{x \in N \mid A(x)\}.$$

ab.

Beispiel 2.1.2 *Zum Beispiel ist*

$$\{x \in \mathbb{Z} \mid x^2 = 1\} = \{-1, 1\}.$$

Definition 2.1.3 *Ist jedes Element der Menge N auch Element der Menge M (also $n \in N \Rightarrow n \in M$), dann heißt N* ***Teilmenge*** *von M, geschrieben*

$$N \subset M$$

oder auch $N \subseteq M$. Zwei Mengen M_1 und M_2 heißen gleich, sie die selben Elemente haben, d.h. wenn $M_1 \subset M_2$ und $M_2 \subset M_1$, also

$$M_1 = M_2 \Longleftrightarrow (M_1 \subset M_2 \text{ und } M_2 \subset M_1)$$

Wollen wir ausdrücken, dass die Teilmenge N von M echt kleiner ist, schreiben wir $N \subsetneq M$.

Beispiel 2.1.4 *Es gelten die Inklusionen*

$$\{0, ..., 9\} \subset \mathbb{N}_0$$

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$$

Die rationalen Zahlen sind

$$\mathbb{Q} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z},\ b \neq 0 \right\}.$$

Verschiedene Brüche können dieselbe rationale Zahl (also dasselbe Element von $\mathbb{Q}$) darstellen, z.B. ist

$$\frac{1}{2} = \frac{3}{6}.$$

Was genau eine rationale Zahl ist, werden wir mittels Äquivalenzrelationen im nächsten Kapitel präzisieren.

Die reellen Zahlen $\mathbb{R}$ sollen die Punkte einer Geraden in unserem Anschauungsraum mathematisch repräsentieren. Jede reelle Zahl lässt sich durch einen unendlichen Dezimalbruch darstellen, z.B.

$$\frac{3}{10} = 0.300...$$
$$\frac{1}{3} = 0.333...$$

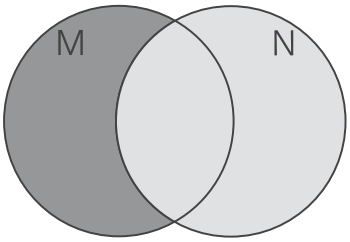


Abbildung 2.1: Komplement

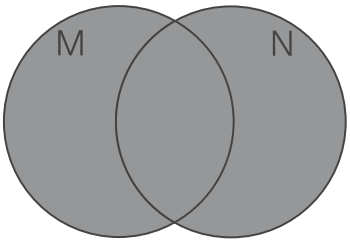


Abbildung 2.2: Vereinigung

Dieser muss nicht notwendig periodisch sein, z.B.

$$\sqrt{2} = 1.414213562...$$

Wir werden auch die reellen Zahlen mathematisch präzise mittels Äquivalenzrelationen einführen, denn verschiedene Dezimalbrüche können dieselbe reelle Zahl darstellen, z.B.

$$1.000... = 0.999...$$

Definition 2.1.5 *Sind M, N Mengen, dann ist*

$$M \backslash N = \{m \in M \mid m \notin N\}$$

*das **Komplement** von N in M, als sogenanntes Venn-Diagramm siehe Abbildung 2.1. Weiter heißt*

$$M \cup N = \{m \mid m \in M \text{ oder } m \in N\}$$

***Vereinigung** von M und N, siehe Abbildung 2.2, und*

$$M \cap N = \{m \mid m \in M \text{ und } m \in N\}$$

***Durchschnitt** von M und N, siehe Abbildung 2.3.*

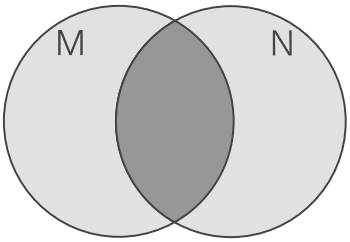


Abbildung 2.3: Durchschnitt

Mit Hilfe der Tautologien der Aussagenlogik zeigt man leicht die Rechenregeln für Komplement, Vereinigung und Durchschnitt in Aufgabe 2.3.

Notation 2.1.6 *Für eine Indexmenge $I \neq \varnothing$ und Mengen M_i, $i \in I$ schreibe*

$$\bigcap_{i \in I} M_i = \{m \mid m \in M_i \text{ für alle } i \in I\}$$

für den Durchschnitt der M_i, $i \in I$, und

$$\bigcup_{i \in I} M_i = \{m \mid \text{es existiert } i \in I \text{ mit } m \in M_i\}$$

für die Vereinigung der M_i, $i \in I$.

Definition 2.1.7 *Wir schreiben $|M|$ oder $\#M$ für die **Anzahl der Elemente** einer endlichen Menge M und, falls M unendlich viele Elemente hat, $|M| = \infty$.*

Beispiel 2.1.8 *Es ist $|\varnothing| = 0$, $|\{0, ..., 9\}| = 10$, $|\{0\}| = 1$, und $|\mathbb{N}| = \infty$.*

Definition 2.1.9 *Sei M eine Menge. Die **Potenzmenge** von M ist*

$$2^M = \mathcal{P}(M) = \{A \mid A \subset M\}.$$

Beispiel 2.1.10 *Potenzmengen:*

$$\begin{aligned} 2^{\varnothing} &= \{\varnothing\} \\ 2^{\{1\}} &= \{\varnothing, \{1\}\} \\ 2^{\{1,2\}} &= \{\varnothing, \{1\}, \{2\}, \{1,2\}\}. \end{aligned}$$

Wir beobachten:

$$|2^{\varnothing}| = 2^0$$
$$|2^{\{1\}}| = 2^1$$
$$|2^{\{1,2\}}| = 2^2$$

Dieses Muster ist allgemein richtig:

Satz 2.1.11 *Sei M eine endliche Menge. Dann gilt*

$$|2^M| = 2^{|M|}.$$

Beweis. Für $M = \varnothing$ haben wir die Behauptung schon in Beispiel 2.1.10 gezeigt. Indem wir die Elemente von $M \neq \varnothing$ durchnummerieren, können wir **ohne Einschränkung der Allgemeinheit** (kurz OE) annehmen, dass $M = \{1, ..., n\}$ mit $n \in \mathbb{N}$. Wir müssen also nur zeigen, dass die Aussage

$$|2^{\{1,...,n\}}| = 2^n$$

für alle $n \in \mathbb{N}$ gilt. Dazu verwenden wir vollständige Induktion:
Induktionsanfang $n = 1$: Haben wir wiederum schon in Beispiel 2.1.10 gesehen.
Induktionsschritt n nach $n+1$: Die Vereinigung

$$\begin{aligned} 2^{\{1,...,n+1\}} &= \{A \subset \{1, ..., n+1\} \mid n+1 \in A\} \dot\cup \\ &\quad \{A \subset \{1, ..., n+1\} \mid n+1 \notin A\} \\ &= \{A' \cup \{n+1\} \mid A' \subset \{1, ..., n\}\} \dot\cup \{A \mid A \subset \{1, ..., n\}\} \end{aligned}$$

ist disjunkt, also gilt mit Induktionsvoraussetzung $|2^{\{1,...,n\}}| = 2^n$, dass

$$|2^{\{1,...,n+1\}}| = 2^n + 2^n = 2^{n+1}.$$

■

Wollen wir ausdrücken, dass die Vereinigung der Mengen M und N **disjunkt** ist (d.h. dass $M \cap N = \varnothing$ gilt), dann schreiben wir auch $M \dot\cup N$ statt $M \cup N$.

Definition 2.1.12 *Sind $M_1, ..., M_r$ Mengen, dann heißt die Menge der geordneten Tupel*

$$M_1 \times ... \times M_r = \{(m_1, ..., m_r) \mid m_i \in M_i \ \forall i = 1, ..., r\}$$

aus Elementen von $M_1, ..., M_r$ das ***kartesische Produkt*** *von $M_1, ..., M_r$. Für $r \in \mathbb{N}$ schreiben wir*

$$M^r = \underbrace{M \times ... \times M}_{r\text{-mal}}$$

Abbildung 2.4 illustriert das kartesische Produkt einer 3-elementigen Menge mit einer 2-elementigen Menge.

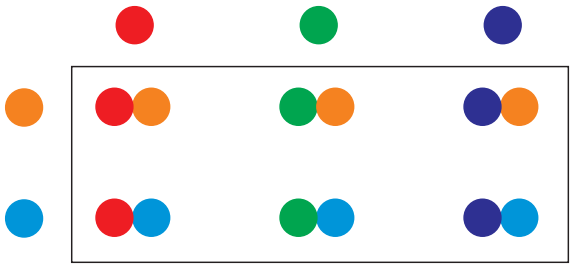


Abbildung 2.4: Kartesisches Produkt einer 3-elementigen und einer 2-elementigen Menge.

Beispiel 2.1.13 *Es ist z.B.*

$$\{1,2,3\} \times \{3,4\} = \{(1,3),(1,4),(2,3),(2,4),(3,3),(3,4)\}.$$

Das Schachbrett ist das Produkt

$$\{1,...,8\} \times \{a,...,h\},$$

der 3-dimensionale Raum

$$\mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R},$$

und die Menge der Wörter mit n Buchstaben in dem Alphabet $\{a,...,z\}$ ist

$$\{a,...,z\}^n.$$

Beispiel 2.1.14 *Von zentraler Bedeutung in der Informatik ist die Menge der* ***r-bit Zahlen***

$$\{0,1\}^r = \{(0,...,0,0),(0,...,0,1),...,(1,...,1,1)\},$$

in heutigen Computern typischerweise für $r = 8, 16, 32, 64$. Da wir für jeden Eintrag des Tupels zwei Möglichkeiten haben, gilt

$$|\{0,1\}^r| = 2^r.$$

2.2 Relationen

Definition 2.2.1 *Eine **Relation** zwischen Mengen M und N ist gegeben durch eine Teilmenge $R \subset M \times N$.*

Beispiel 2.2.2 *Für $M = \{2, 3, 7\}$, $N = \{4, 5, 6\}$ und*

$$R = \{(m, n) \in M \times N \mid m \text{ teilt } n\}$$

gilt

$$R = \{(2, 4), (2, 6), (3, 6)\}\,.$$

Um uns Schreibarbeit zu sparen, führen wir die folgende alternative Darstellung einer Relation ein:

Bemerkung 2.2.3 *Wir können eine Relation $R \subset M \times N$ mit der Aussageform*

$$(m, n) \in R$$

identifizieren. Für diese schreiben wir dann üblichweise kurz

$$m \,\square\, n$$

mit einem geeigneten Symbol, etwa $\square$.

Notation 2.2.4 *Falls $M = N$ sagt man auch, dass R eine Relation **auf** M ist.*

Definition 2.2.5 *Sei M eine Menge. Eine Relation $R \subset M \times M$ auf M heißt*

- ***reflexiv**, wenn $(m, m) \in R$ für alle $m \in M$,*
- ***transitiv**, wenn*

$$(l, m) \in R \text{ und } (m, n) \in R \Longrightarrow (l, n) \in R.$$

- ***antisymmetrisch**, wenn*

$$(n, m) \in R \text{ und } (m, n) \in R \Longrightarrow m = n$$

*Eine reflexive, transitive und antisymmetrische Relation, nennt man auch eine **Halbordnung**. Gilt zusätzlich noch für alle $m, n \in M$, dass $(m, n) \in R$ oder $(n, m) \in R$, so heißt R **Totalordnung**.*

Beispiel 2.2.6 *Relationen sind:*

1) *Sei M eine Menge. Die Inklusion $\subset$ zwischen Teilmengen von M ist eine Halbordnung auf der Potenzmenge 2^M: Für alle $A, B, C \subset M$ gilt*

   - $A \subset A$ *(reflexiv)*
   - $A \subset B$ *und* $B \subset C \Longrightarrow A \subset C$ *(transitiv)*
   - $A \subset B$ *und* $B \subset A \Longrightarrow A = B$ *(antisymmetrisch).*

2) *Auf $\mathbb{R}$ ist $\leq$ eine Totalordnung: Für $x, y, z \in \mathbb{R}$ gilt*

   - $x \leq x$ *(reflexiv)*
   - $x \leq y$ *und* $y \leq z \Longrightarrow x \leq z$ *(transitiv)*
   - $x \leq y$ *und* $y \leq x \Longrightarrow x = y$ *(antisymmetrisch)*
   - $x \leq y$ *oder* $y \leq x$ *(totalgeordnet).*

2.3 Abbildungen

Definition 2.3.1 *Eine **Abbildung** $f : M \to N$ ist eine Relation $R \subset M \times N$, sodass es für jedes $m \in M$ genau ein $f(m) \in N$ gibt mit $(m, f(m)) \in R$. Schreibe*

$$\begin{array}{rccc} f: & M & \to & N \\ & m & \mapsto & f(m) \end{array}$$

*Wir bezeichnen M als **Quelle** und N als **Ziel** von f.*

*Die Relationenmenge R bezeichnet man auch als den **Graphen***

$$\mathrm{Graph}(f) := R = \{(m, f(m)) \mid m \in M\},$$

von f.

Beispiel 2.3.2 *Die Abbildung*

$$\begin{array}{rccc} f: & \mathbb{R} & \to & \mathbb{R} \\ & x & \mapsto & f(x) = x^2 \end{array}$$

ist als Relation aufgefasst der Graph

$$R = \left\{(x, x^2) \mid x \in \mathbb{R}\right\} \subset \mathbb{R} \times \mathbb{R},$$

siehe Abbildung 2.5.

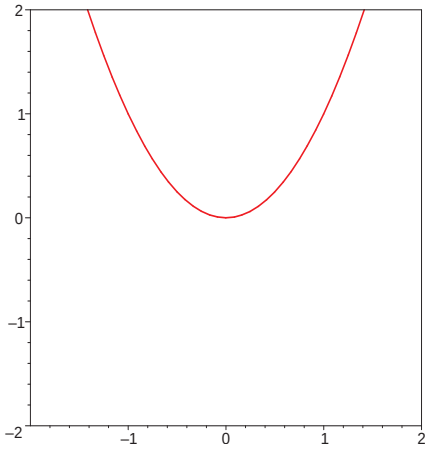


Abbildung 2.5: Graph der Parabel

Beispiel 2.3.3 *Die Relation gegeben durch die Teilmenge* $R \subset \mathbb{R} \times \mathbb{R}$ *wie in Abbildung 2.6 ist keine Abbildung.*

Abbildung 2.6 ist also keine Abbildung...

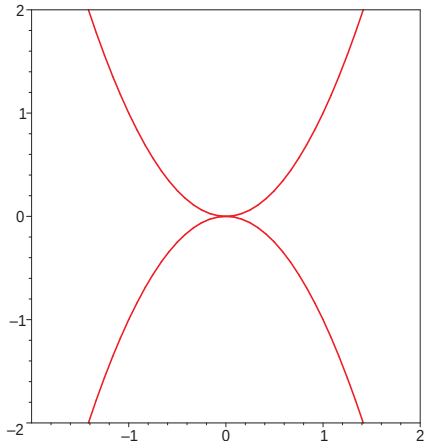


Abbildung 2.6: Relation aber keine Abbildung

Beispiel 2.3.4 *Eine von Aussagen* $A_1, \ldots, A_n$ *abhängige logische Formel* B *ist nichts anderes als eine* ***n-stellige boolsche Funktion****, d.h. eine Funktion*

$$f_B : \{0,1\}^n \longrightarrow \{0,1\}.$$

Beispielsweise ist die logische Formel $A_1 \wedge A_2$ gegeben durch die Funktion

$$\begin{array}{rccc} f_{A_1 \wedge A_2}: & \{0,1\}^2 & \longrightarrow & \{0,1\} \\ & (0,0) & \longmapsto & 0 \\ & (0,1) & \longmapsto & 0 \\ & (1,0) & \longmapsto & 0 \\ & (1,1) & \longmapsto & 1 \end{array}$$

Boolsche Funktionen haben wir schon in Form von Wahrheitswerttafeln kennengelernt.

Definition 2.3.5 *Für eine Teilmenge $A \subset M$ heißt*

$$f(A) := \{f(m) \mid m \in A\} \subset N$$

***Bild** von A unter f, und*

$$\mathrm{Bild}(f) := f(M)$$

das Bild von f.

Für $B \subset N$ heißt

$$f^{-1}(B) := \{m \in M \mid f(m) \in B\} \subset M$$

*das **Urbild** von B unter f.*

Beispiel 2.3.6 *Das Bild der Parabel f aus Beispiel 2.3.2 ist*

$$f(\mathbb{R}) = \mathbb{R}_{\geq 0}$$

und es gilt beispielsweise

$$f^{-1}(\{1,2\}) = \{-1, 1, -\sqrt{2}, \sqrt{2}\}.$$

Definition 2.3.7 *Eine Abbildung $f : M \to N$ heißt **surjektiv**, wenn für das Bild von f gilt*

$$f(M) = N.$$

Falls für alle $m_1, m_2 \in M$ gilt

$$f(m_1) = f(m_2) \Longrightarrow m_1 = m_2,$$

*so heißt f **injektiv**.*

*Eine Abbildung die injektiv und surjektiv ist, heißt **bijektiv**.*

Definition und Satz 2.3.8 *Ist $f : M \to N$ bijektiv, dann gibt es für jedes $y \in N$ genau ein $x \in M$ das die Gleichung*

$$f(x) = y$$

erfüllt (eine Lösung x existiert, da f surjektiv ist, und ist eindeutig, da f injektiv ist). Somit ist durch

$$f^{-1} : N \to M,\ y \mapsto x \text{ mit } f(x) = y$$

eine Abbildung definiert, die ***Umkehrabbildung*** *von f.*

Weiter ist f^{-1} bijektiv.

Beweis. Es bleibt nur die Bijektivität zu zeigen: Die Surjektivität ist klar nach Konstruktion, da für $x \in M$ gilt

$$f^{-1}(f(x)) = x.$$

Die Injektivität folgt da f eine Abbildung ist: Sind $y_1, y_2 \in N$, dann gibt es $x_i \in M$ mit $y_i = f(x_i)$, und es ist $f^{-1}(y_i) = x_i$. Aus

$$f^{-1}(y_1) = f^{-1}(y_2)$$

folgt somit

$$y_1 = f(x_1) = f(f^{-1}(y_1)) = f(f^{-1}(y_2)) = f(x_2) = y_2.$$

■

Für die oben verwendete Formulierung "es existiert genau ein" schreibt man auch das Zeichen $\exists_1$.

Bemerkung 2.3.9 *Die Umkehrabbildung f^{-1} ist die Relation*

$$\mathrm{Graph}(f^{-1}) = \{(f(x), x) \mid x \in M\} \subset N \times M.$$

Beispiel 2.3.10 *Die Parabelfunktion*

$$\mathbb{R} \to \mathbb{R},\ x \mapsto x^2$$

aus Beispiel 2.3.2 ist weder injektiv noch surjektiv. Als Abbildung auf ihr Bild

$$\mathbb{R} \to \mathbb{R}_{\geq 0},\ x \mapsto x^2$$

wird sie surjektiv. Schränken wir auch die Quelle ein, wird die Abbildung

$$\mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0},\ x \mapsto x^2$$

bijektiv mit Umkehrabbildung

$$\mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0},\ y \mapsto \sqrt{y}$$

wie in Abbildung 2.7. Der Graph der Umkehrabbildung entsteht durch Spiegelung an der Diagonalen (siehe Bemerkung 2.3.9).

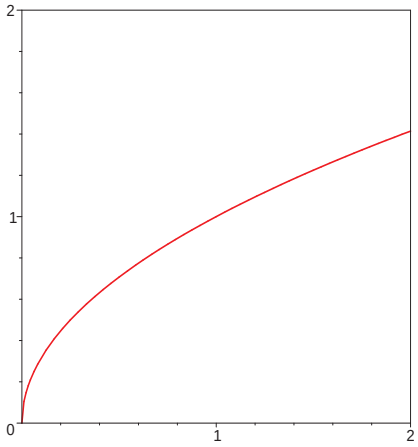


Abbildung 2.7: Wurzel

Die Hyperbel

$$\mathbb{R}\backslash\{0\} \to \mathbb{R},\ x \mapsto \frac{1}{x}$$

ist injektiv, aber nicht surjektiv (siehe Abbildung 2.8).

Satz 2.3.11 (Schubfachprinzip) *Seien M, N endliche Mengen und $f : M \to N$ eine Abbildung. Ist f injektiv, dann gilt $|M| \leq |N|$.*

Die äquivalente negierte Aussage

$$\text{Ist } |M| > |N|, \text{ so kann } f \text{ nicht injektiv sein.}$$

erklärt den Namen: Stellen wir uns N als eine Menge von Fächern vor, auf die die Elemente von M durch die von f gegebene

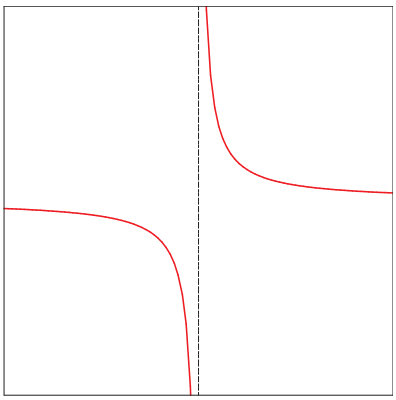


Abbildung 2.8: Hyperbel

Zuordnung verteilt werden, dann gibt es ein Fach mit mindestens zwei Elementen.

Beweis. Es gilt

$$|N| = \sum_{n \in N} 1 \geq \sum_{n \in N} \left| f^{-1}(\{n\}) \right| = |M|,$$

denn $f^{-1}(\{n\})$ hat genau 1 Element, wenn n im Bild von f liegt (da f injektiv ist), und ist leer sonst. Die letzte Gleichheit gilt, da für jede Abbildung f die Vereinigung

$$M = \bigcup_{n \in N} f^{-1}(\{n\})$$

disjunkt ist, d.h. die Mengen in der Vereinigung sich paarweise nicht schneiden (siehe auch Aufgabe 2.4). Man beachte dazu: Jedes $m \in M$ hat ein Bild $n = f(m)$ und liegt somit in $f^{-1}(\{n\})$. Weiter folgt aus $m \in f^{-1}(\{n_1\}) \cap f^{-1}(\{n_2\})$, dass $n_1 = f(m) = n_2$. ■

Notation 2.3.12 *Für Zahlen a_n indiziert durch eine endliche Menge N schreiben wir*

$$\sum_{n \in N} a_n$$

für die Summe der a_n.

*Die a_n können Elemente einer beliebigen Menge R mit einer Verknüpfung $+$ sein, die **assoziativ** ist, d.h. mit $r_1 + (r_2 + r_3) =$*

$(r_1 + r_2) + r_3$ *für alle* $r_i \in M$, *und* ***kommutativ*** *ist, d.h. mit* $r_1 + r_2 = r_2 + r_1$ *für alle* $r_i \in M$.

Indiziert *bedeutet, dass für jedes* $n \in N$ *eine Zahl* a_n *gegeben ist, d.h. eine Abbildung* $N \to R$, $n \mapsto a_n$.

Satz 2.3.13 *Sind* M, N *endliche Mengen und* $f : M \to N$ *eine surjektive Abbildung, dann gilt* $|M| \geq |N|$.

Beweis. Da f surjektiv ist, gilt

$$N = \{f(m) \mid m \in M\} = \bigcup_{m \in M} \{f(m)\}$$

(nicht notwendig disjunkt), also

$$|N| \leq \sum_{m \in M} |\{f(m)\}| = \sum_{m \in M} 1 = |M|\,.$$

■

Mit der Antisymmetrie von $\leq$ erhalten wir aus den Sätzen 2.3.11 und 2.3.13 sofort:

Corollar 2.3.14 *Sind* M, N *endliche Mengen und* $f : M \to N$ *eine bijektive Abbildung, dann gilt* $|M| = |N|$.

Siehe auch die Übungsaufgaben 2.5, 2.6, 2.7, 2.8, 2.9 und 2.10.

Definition 2.3.15 *Seien* $f : M \to N$ *und* $g : N \to L$ *Abbildungen, dann ist die* ***Komposition*** *von* ***g nach f*** *(oder auch* ***g und f****) ist definiert als*

$$\begin{array}{rccc} g \circ f : & M & \to & L \\ & m & \mapsto & g(f(m)) \end{array}$$

Beispiel 2.3.16 *Die Komposition* $g \circ f$ *von*

$$f : \mathbb{R} \to \mathbb{R},\ x \mapsto x + 1$$
$$g : \mathbb{R} \to \mathbb{R},\ x \mapsto x^2$$

gibt

$$g \circ f : \mathbb{R} \to \mathbb{R},\ x \mapsto (x+1)^2 = x^2 + 2x + 1.$$

Lemma 2.3.17 *Die Komposition von Abbildungen ist assoziativ, das heißt für Abbildungen*

$$M \overset{f}{\to} N \overset{g}{\to} L \overset{h}{\to} K$$

gilt

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

Zum Beweis siehe Übungsaufgabe 2.11.

Beispiel 2.3.18 *Selbst wenn $f : M \to M$ und $g : M \to M$ ist im Allgemeinen $f \circ g \neq g \circ f$. In Beispiel 2.3.16 können wir auch die Komposition*

$$f \circ g : \mathbb{R} \to \mathbb{R},\ x \mapsto x^2 + 1$$

bilden und diese stimmt nicht mit

$$g \circ f : \mathbb{R} \to \mathbb{R}, x \mapsto (x+1)^2 = x^2 + 2x + 1$$

überein, denn es ist z.B.

$$(f \circ g)(1) = 2 \neq 4 = (g \circ f)(1).$$

Dieselbe Situation haben wir auch für die Abbildungen

$$f : \mathbb{R}^2 \to \mathbb{R}^2,\ (x, y) \mapsto (x + y, y)$$
$$g : \mathbb{R}^2 \to \mathbb{R}^2,\ (x, y) \mapsto (x, x + y),$$

für die wir die Kompositionen

$$f \circ g : \mathbb{R}^2 \to \mathbb{R}^2,\ (x, y) \mapsto (2x + y, x + y)$$
$$g \circ f : \mathbb{R}^2 \to \mathbb{R}^2,\ (x, y) \mapsto (x + y, x + 2y),$$

erhalten.

Definition 2.3.19 *Sei M eine Menge. Die **identische Abbildung** auf M ist*

$$\begin{array}{rccc} \mathrm{id}_M : & M & \to & M \\ & m & \mapsto & m \end{array}$$

Beispiel 2.3.20 *Abbildung 2.9 zeigt den Graphen von $\mathrm{id}_{\mathbb{R}}$.*

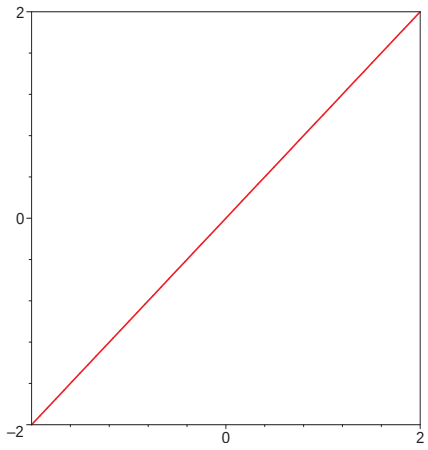


Abbildung 2.9: Identische Abbildung $\mathbb{R} \to \mathbb{R}$

Satz 2.3.21 *Sind $M, N \neq \emptyset$ und $f : M \to N$ eine Abbildung, dann ist*

1) *f injektiv genau dann, wenn es eine Abbildung $g : N \to M$ gibt mit $g \circ f = \mathrm{id}_M$. Man bezeichnet g auch als **Linksinverse** von f.*

2) *f surjektiv genau dann, wenn es eine Abbildung $g : N \to M$ gibt mit $f \circ g = \mathrm{id}_N$. Man bezeichnet g auch als **Rechtsinverse** von f.*

3) *f bijektiv genau dann, wenn es eine Abbildung $g : N \to M$ gibt mit $g \circ f = \mathrm{id}_M$ und $f \circ g = \mathrm{id}_N$.*

   Weiter ist dann $g = f^{-1}$ die Umkehrabbildung von f.

Beweis. *Teil 1 und 2 zeigen wir in Übung 2.13. Einen Hinweis geben Abbildungen 2.10 und 2.11. Man beachte, dass wir bei der Konstruktion von g in beiden Beispielen eine Wahlfreiheit haben, also g im Allgemeinen nicht eindeutig bestimmt ist.*

Zu 3: Sei f bijektiv. Wir zeigen, dass die Umkehrabbildung $g = f^{-1}$ die gesuchten Eigenschaften besitzt: Ist $x \in M$ und $y = f(x)$, dann gilt für die Umkehrabbildung $f^{-1}(y) = x$, also

$$f^{-1} \circ f = \mathrm{id}_M .$$

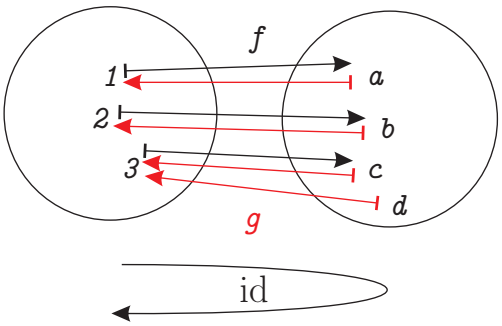


Abbildung 2.10: Konstruktion einer Linksinversen g für eine injektive Abbildung f.

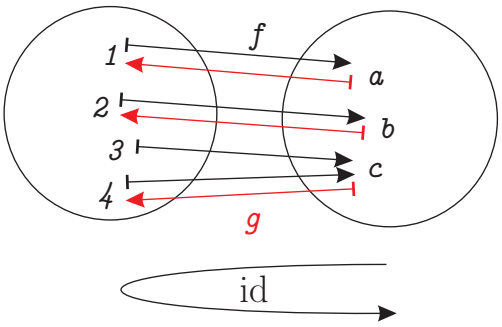


Abbildung 2.11: Konstruktion einer Rechtsinversen g für eine surjektive Abbildung f.

Durch Anwenden von f folgt, dass

$$(f \circ f^{-1})(f(x)) = f(x)$$

für alle $x \in M$. Da f surjektiv ist, erhalten wir jedes Element von N als $f(x)$, $x \in M$. Somit stimmen $f \circ f^{-1}$ und id_N auf ganz N überein, d.h. auch

$$f \circ f^{-1} = \mathrm{id}_N .$$

Existiert umgekehrt eine Abbildung $g : N \to M$ mit $g \circ f = \mathrm{id}_M$ und $f \circ g = \mathrm{id}_N$, dann ist f bijektiv mit Teil 1 und 2.

Es bleibt noch zu zeigen, dass g eindeutig durch $g \circ f = \mathrm{id}_M$ und $f \circ g = \mathrm{id}_N$ bestimmt und somit gleich f^{-1} ist: Sei $h : N \to M$

eine weitere Abbildung mit $h \circ f = \mathrm{id}_M$ *und* $f \circ h = \mathrm{id}_N$. *Dann folgt*

$$h = h \circ \mathrm{id}_N = h \circ f \circ g = \mathrm{id}_M \circ g = g.$$

■

2.4 Äquivalenzrelationen

Der Begriff der Äquivalenzrelation schwächt den Begriff der Gleichheit ab.

Definition 2.4.1 *Sei* M *eine Menge und* $R \subset M \times M$ *eine reflexive und transitive Relation. Ist* R *außerdem* ***symmetrisch****, das heißt*

$$(m, n) \in R \Rightarrow (n, m) \in R,$$

so heißt R *eine* ***Äquivalenzrelation****.*

Schreiben wir $m \sim n$ für $(m, n) \in R$, dann bedeutet

- reflexiv, dass $m \sim m$ für alle $m \in M$,
- transitiv, dass $m \sim l$ und $l \sim n \Rightarrow m \sim n$ für alle $m, l, n \in M$ und
- symmetrisch, dass $m \sim n \Rightarrow n \sim m$ für alle $m, n \in M$.

Beispiel 2.4.2 *Die Eigenschaft von zwei Menschen gleich groß zu sein, ist eine Äquivalenzrelation (dagegen ist die Eigenschaft gleich groß bis auf einen Unterschied von maximal* $1cm$ *zu sein nicht transitiv).*

Allgemeiner: Sei $f : M \to N$ *eine Abbildung. Dann wird durch*

$$m_1 \sim m_2 \Longleftrightarrow f(m_1) = f(m_2)$$

eine Äquivalenzrelation auf M *definiert.*

Definition 2.4.3 *Ist* M *eine Menge,* $\sim$ *eine Äquivalenzrelation und* $m \in M$*, dann heißt*

$$[m] = \{n \in M \mid n \sim m\} \subset M$$

die ***Äquivalenzklasse*** *von m. Jedes $n \in [m]$ heißt* ***Repräsentant*** *von $[m]$.*

Wir schreiben weiter

$$M/\sim = \{[m] \mid m \in M\} \subset 2^M$$

für die Menge der Äquivalenzklassen von $\sim$ und

$$\begin{array}{rccc} \pi: & M & \to & M/\sim \\ & m & \mapsto & [m] \end{array}$$

für die ***kanonische Abbildung****. Diese ist offenbar surjektiv.*

Satz 2.4.4 *Je zwei Äquivalenzklassen sind gleich oder disjunkt.*

Beweis. Sei $[m] \cap [n] \neq \varnothing$. Wir müssen $[m] = [n]$ zeigen. Ist $a \in [m] \cap [n]$, also $a \sim m$ und $a \sim n$, dann folgt mit Symmetrie und Transitivität, dass $m \sim n$, also $m \in [n]$. Sei nun $a \in [m]$ beliebig. Dann gilt $a \sim m$ und $m \sim n$, also $a \sim n$, das heißt $a \in [n]$. Wir haben also $[m] \subset [n]$ gezeigt. Die andere Inklusion folgt genauso. ■

Insbesondere gilt,

$$m \sim n \Leftrightarrow [m] = [n],$$

d.h. Äquivalenz von Elementen von M übersetzt sich in Gleichheit von Elementen von $M/\sim$.

Der Satz zeigt auch: Eine Äquivalenzrelation partitioniert die Menge M in die Äquivalenzklassen. **Partitionieren** bedeutet hier, eine Menge als disjunkte Vereinigung von nichtleeren Mengen zu schreiben.

Beispiel 2.4.5 *Zwei Atome einer Torte sollen äquivalent sein, wenn sie von derselben Person gegessen werden (dies ist eine Äquivalenzrelation, unter der naheliegenden Annahme, dass nichts von der Torte übrigbleibt). Die Einteilung in Äquivalenzklassen partitioniert die Torte in (nicht notwendig gleich grosse) Tortenstücke.*

Beispiel 2.4.6 *In Beispiel 2.4.2 sind zwei Menschen in derselben Äquivalenzklasse, genau dann, wenn sie gleich groß sind. Ist m ein Mensch, dann enthält $[m]$ alle Menschen, die dieselbe Größe wie m haben.*

Beispiel 2.4.7 *Betrachte die Äquivalenzrelation $\sim$ auf $\mathbb{R}^2$ gegeben durch*

$$(x_1, y_1) \sim (x_2, y_2) \Longleftrightarrow f(x_1, y_1) = f(x_2, y_2)$$

mit

$$f(x, y) = x^2 + y^2.$$

Die Äquivalenzklassen sind die konzentrischen Kreise (und $\{(0,0)\}$), also

$$M/\sim = \left\{ \left\{ (x, y) \mid x^2 + y^2 = r \right\} \mid r \in \mathbb{R}_{\geq 0} \right\}.$$

Siehe Abbildung 2.12. Siehe auch Übungsaufgabe 2.14.

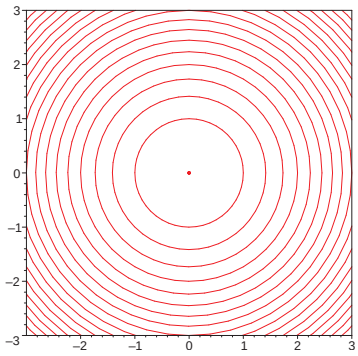


Abbildung 2.12: Äquivalenzklassen

2.5 Übungsaufgaben

Übung 2.1 *Bestimmen Sie die Wahrheitswerte folgender Aussagen:*

$\{3\} = \lvert\{1,2,3\}\rvert$	$\{1,3\} \in \mathcal{P}(\{1,2,3\})$
$0 \subset \{1,2,3\}$	$\{3\} \subset \{1,2,3\}$
$\{3\} \in \{1,2,3\}$	$\lvert\mathcal{P}(\{1,2,3\})\rvert = 8$
$\{\varnothing\} \subset \{1,2,3\}$	$\varnothing \subset \mathcal{P}(\{1,2,3\})$
$3 \in \{1,2,3\}$	$\{3\} \in \mathcal{P}(\{1,2,3\})$
$3 \subset \{1,2,3\}$	$\{1,3\} \subset \{1,2,3\}$
$\varnothing \subset \{1,2,3\}$	$3 \in \mathcal{P}(\{1,2,3\})$
$3 = \lvert\{1,2,3\}\rvert$	$\varnothing \in \mathcal{P}(\{1,2,3\})$

Übung 2.2 *Verwenden Sie den Induktionsbeweis der Formel*

$$\left|2^M\right| = 2^{|M|}$$

für endliche Mengen M, um alle Teilmengen von $M = \{1, 2, 3, 4\}$ aufzuzählen.

Übung 2.3 *Sei M eine Menge. Für das Komplement einer Teilmenge $X \subset M$ schreiben wir kurz $\overline{X} = M \backslash X$ Zeigen Sie, dass für Teilmengen $X, Y, Z \subset M$ die folgenden Gleichungen gelten:*

1) *Für $\cap$ gilt:*
   (a) *Assoziativität $X \cap (Y \cap Z) = (X \cap Y) \cap Z$.*
   (b) *Kommutativität $X \cap Y = Y \cap X$.*
   (c) *Identität $X \cap M = X$,*
2) *Für $\cup$ gilt:*
   (a) *Assoziativität $X \cup (Y \cup Z) = (X \cup Y) \cup Z$.*
   (b) *Kommutativität $X \cup Y = Y \cup X$.*
   (c) *Identität $X \cup \varnothing = X$,*
3) *Für $\cap$ und $\cup$ gelten die Distributivgesetze*

$$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$$
$$X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$$

4) *Idempotenz:*

$$X \cap X = X \qquad X \cup X = X$$

5) *Vergleichen Sie diese Formeln mit den Rechenregeln für ganze Zahlen.*
6) *Komplement:*

$$\overline{\overline{X}} = X \qquad X \cup \overline{X} = M \qquad X \cap \overline{X} = \varnothing$$

Dabei schreiben wir $\overline{X} = M \backslash X$ für das Komplement einer Teilmenge $X \subseteq M$.

7) De Morgansche Gesetze der Mengenlehre:

$$\overline{X} \cup \overline{Y} = \overline{X \cap Y}$$
$$\overline{X} \cap \overline{Y} = \overline{X \cup Y}$$

Hinweis: Verwenden Sie die entsprechenden Formeln in der Aussagenlogik. Illustrieren Sie die Behauptungen mit Venn-Diagrammen.

Übung 2.4 *1) Zeigen Sie für endliche Mengen M und N, dass*

$$|M \cup N| = |M| + |N| - |M \cap N|$$

und

$$|M \times N| = |M| \cdot |N|$$

2) Gegeben drei Mengen M, N und L, stellen Sie eine Formel für $|M \cup N \cup L|$ auf, und beweisen Sie diese.

Übung 2.5 *Geben Sie je ein Beispiel für eine Abbildung $\mathbb{N} \to \mathbb{N}$ an, die*

1) injektiv aber nicht surjektiv ist.

2) surjektiv aber nicht injektiv ist.

Übung 2.6 *Seien M, N endliche Mengen mit $|M| = |N|$ und $f : M \to N$ eine Abbildung. Zeigen Sie, dass folgende Aussagen äquivalent sind:*

1) f ist bijektiv,

2) f ist injektiv,

3) f ist surjektiv.

Übung 2.7 *Auf einem Fest treffen sich n Personen. Zeigen Sie, dass zwei von diesen mit derselben Anzahl von Anwesenden bekannt sind.*

Übung 2.8 *Seien die Zahlen $1, ..., 101$ in irgendeiner Reihenfolge gegeben. Zeigen Sie, dass 11 davon aufsteigend oder absteigend sortiert sind.*

Hinweis: Betrachten Sie eine geeignete Menge von Paaren und verwenden Sie das Schubfachprinzip.

Übung 2.9 *Sei $n \in \mathbb{N}$ und seien $n^2 + 1$ viele Punkte in dem Quadrat*

$$\{(x, y) \mid 0 \leq x < n,\ 0 \leq y < n\}$$

gegeben. Zeigen Sie, dass es unter diesen zwei Punkte gibt, die Abstand $\leq \sqrt{2}$ haben.

Übung 2.10 *Sei $n \in \mathbb{N}$ und $M \subset \{1, \ldots, 2n\}$ eine Menge von ganzen Zahlen mit $|M| = n + 1$ Elementen.*

1) *Zeigen Sie, dass es in M zwei verschiedene Zahlen gibt, sodass die eine Zahl die andere teilt.*

2) *Illustrieren Sie Ihren Beweis für $n = 4$ und alle Mengen M mit $1 \notin M$.*

Übung 2.11 *Zeigen Sie: Die Komposition von Abbildungen ist assoziativ, das heißt für Abbildungen*

$$M \xrightarrow{f} N \xrightarrow{g} L \xrightarrow{h} K$$

gilt

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

Übung 2.12 *Es seien M, N zwei Mengen und $f : M \to N$ eine Abbildung. Zeigen Sie:*

1) *Für jede Teilmenge $X \subseteq M$ gilt $X \subseteq f^{-1}(f(X))$.*

2) *Für jede Teilmenge $Y \subseteq N$ gilt $f(f^{-1}(Y)) \subseteq Y$.*

Gilt jeweils auch die Gleichheit?

Übung 2.13 *Seien $M, N, L \neq \varnothing$ Mengen und $f : M \to N$ und $h : N \to L$ Abbildungen. Zeigen Sie:*

1) *Sind f und h injektiv, dann ist auch $h \circ f$ injektiv.*

2) *Sind f und h surjektiv, dann ist auch $h \circ f$ surjektiv.*

3) *f ist injektiv genau dann, wenn es eine Abbildung $g : N \to M$ gibt mit $g \circ f = \mathrm{id}_M$.*

4) f ist surjektiv genau dann, wenn es eine Abbildung $g : N \to M$ gibt mit $f \circ g = \mathrm{id}_N$.

Implementieren Sie Ihren Algorithmus.

Übung 2.14 *Betrachten Sie die Menge $M = \mathbb{R}^2 \setminus \{(0,0)\}$ aller Punkte der reellen Ebene ohne den 0-Punkt.*

Wir definieren eine Äquivalenzrelation auf $M \times M$ durch $(x,y) \sim (x',y')$ genau dann, wenn es eine Gerade durch den Nullpunkt $(0,0) \in \mathbb{R}^2$ gibt, auf der sowohl der Punkt (x,y) als auch der Punkt (x',y') liegt, siehe Abbildung 2.13.

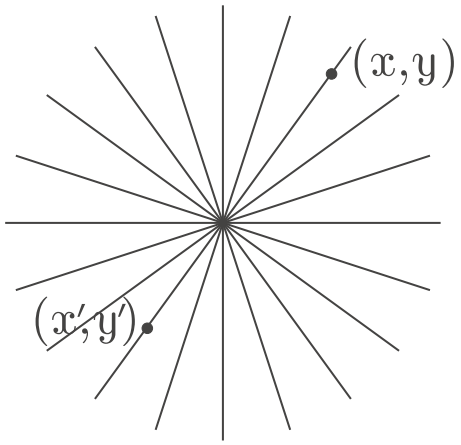


Abbildung 2.13: Geraden durch den Nullpunkt.

1) Zeigen Sie, dass durch $\sim$ eine Äquivalenzrelation gegeben ist.

2) Finden Sie eine geometrische Darstellung der Menge der Äquivalenzklassen $M/\sim$, indem Sie in jeder Äquivalenzklasse einen geeigneten Repräsentanten wählen.

3

Zahlen

In diesem Abschnitt beschäftigen wir uns mit wesentlichen Eigenschaften der ganzen Zahlen. Alle diese Eigenschaften werden wir in allgemeinerem Kontext später auch für andere Ringe kennenlernen.

3.1 Die ganzen Zahlen und Division mit Rest

Auf den natürlichen Zahlen $\mathbb{N}_0 = \{0, 1, 2, 3, ...\}$ gibt es Verknüpfungen + und $\cdot$, die dem Assoziativgesetz

$$a + (b + c) = (a + b) + c$$
$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

Kommutativgesetz

$$a + b = b + a$$
$$a \cdot b = b \cdot a$$

und Distributivgesetz

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

gehorchen für alle $a, b, c \in \mathbb{N}_0$. Auf die axiomatische Definition der natürlichen Zahlen wollen wir hier nicht weiter eingehen. Als Übungsaufgabe informiere man sich in Buch oder Suchmaschine der Wahl über die Peano-Axiome.

In $\mathbb{N}_0$ gibt es keine Zahl a mit

$$1 + a = 0.$$

Anschaulich heißt das: Wir können zwar Guthaben auf einem Konto darstellen aber keine Schulden.

Aus den natürlichen Zahlen konstruiert man deshalb die ganzen Zahlen $\mathbb{Z} = \{0, 1, -1, 2, -2, ...\}$ wie folgt:

Bemerkung 3.1.1 *Die Grundidee zur Konstruktion ist: Den Wert eines Kontos kann man als Differenz von Guthaben und Schulden schreiben. Verschiedene Tupel* (*Guthaben, Schulden*) *führen zu demselben Wert des Kontos, z.B.*

$$5 - 1 = 1000006 - 1000002$$

d.h. der Wert eines Kontos mit $5 €$ *Guthaben und* $1 €$ *Schulden entspricht einem Konto mit* $1000006 €$ *Guthaben und* $1000002 €$ *Schulden. Um den Wert zu repräsentieren, müssen wir also Äquivalenzklassen bezüglich einer geeigneten Äquivalenzrelation betrachten. Die beiden Konten in dem Beispiel haben denselben Wert, da*

$$5 + 1000002 = 1000006 + 1.$$

Man definiert also

$$\mathbb{Z} := (\mathbb{N}_0 \times \mathbb{N}_0) / \sim$$

mit der Äquivalenzrelation

$$(a, b) \sim (c, d) \Leftrightarrow a + d = b + c,$$

und die Äquivalenzklasse

$$[(a, b)] = \{(c, d) \mid (c, d) \sim (a, b)\}.$$

Wir stellen uns unter $[(a, b)]$ *die ganze Zahl* $a - b$ *vor. Dies motiviert die folgenden wohldefinierten Verknüpfungen* $+$ *und* $\cdot$ *auf* $\mathbb{Z}$

$$\begin{aligned} [(a, b)] + [(c, d)] &:= [(a + c, b + d)] \\ [(a, b)] \cdot [(c, d)] &:= [(a \cdot c + b \cdot d, a \cdot d + b \cdot c)], \end{aligned}$$

die dem Assoziativ-, Kommutativ- und Distributivgesetz gehorchen (siehe auch Übung 3.2). Es gilt dann

$$[(a,b)] + [(b,a)] = [(0,0)]$$

für alle $[(a,b)] \in \mathbb{Z}$*, insbesondere*

$$[(1,0)] + [(0,1)] = [(0,0)]\,.$$

Weiter ist

$$[(0,0)] + [(a,b)] = [(a,b)]$$
$$[(1,0)] \cdot [(a,b)] = [(a,b)]\,.$$

Eine Menge mit solchen Verknüpfungen nennt man kommutativen Ring mit 1*. Des Weiteren sind die ganzen Zahlen angeordnet durch die Totalordnung* $\leq$*.*

Jedes Konto $[(a,b)]$ *ist äquivalent zu einem eindeutig bestimmten Konto mit keinem Guthaben oder keinen Schulden: Für* $a \geq b$ *sei* $c \in \mathbb{N}_0$ *mit* $a = b + c$*. Dann gilt* $(a,b) \sim (c,0)$*. Für* $a < b$ *sei* $c \in \mathbb{N}$ *mit* $b = a + c$*. Dann gilt* $(a,b) \sim (0,c)$*. Wir schreiben kurz*

$$c := [(c,0)]$$

und

$$-c := [(0,c)]\,.$$

Es gilt dann

$$c + (-c) = 0$$

für alle $c \in \mathbb{Z}\backslash\{0\}$*, denn* $c + (-c) = [(c,c)] = [(0,0)] = 0$*.*

Auf ähnliche Weise lässt sich $\mathbb{Q}$ *aus* $\mathbb{Z}$ *konstruieren als*

$$\mathbb{Q} = (\mathbb{Z} \times \mathbb{Z}\backslash\{0\}) \,/\, \sim$$

mit der Äquivalenzrelation

$$(a,b) \sim (c,d) \Leftrightarrow ad = bc,$$

wobei wir die Äquivalenzklassen schreiben als

$$\frac{a}{b} := [(a,b)].$$

Die reellen Zahlen $\mathbb{R}$ *kann man wiederum aus* $\mathbb{Q}$ *mit Hilfe einer geeigneten Äquivalenzrelation konstruieren.*

In $\mathbb{Q}$ lässt sich jede Zahl a durch jede Zahl $b \neq 0$ teilen. In vielen Problemen des täglichen Lebens und der Mathematik macht dies allerdings keinen Sinn, da die kleinste sinnvolle Einheit 1 ist. Wollen wir etwa 1000 Passagiere gleichmäßig auf 3 Flugzeuge verteilen, so ist $\frac{1000}{3}$ keine sinnvolle Lösung, sondern vielmehr

$$1000 = 3 \cdot 333 + 1.$$

Dies bezeichnet man als Division mit Rest (1 Passagier bleibt übrig):

Lemma 3.1.2 (Division mit Rest) *Sind $a, b \in \mathbb{Z}$, $b \neq 0$, dann gibt es eindeutig bestimmte $q, r \in \mathbb{Z}$ mit*

$$a = b \cdot q + r$$

und $0 \leq r < |b|$.

Beispiel 3.1.3 *In obigem Beispiel ist $a = 1000$ und $b = 3$, und es gilt*

$$1000 = 3 \cdot 333 + 1$$

d.h. $q = 333$ und $r = 1$.

Zum Beweis von Lemma 3.1.2:
Beweis. Existenz: Ohne Einschränkung ist $b > 0$. Die Menge

$$\{w \in \mathbb{Z} \mid b \cdot w > a\} \neq \varnothing$$

hat ein kleinstes Element w. Setze dann

$$q := w - 1 \qquad r := a - qb.$$

Offenbar gilt dann $a = qb + r$, außerdem $qb + b > a$ also

$$r < b$$

und da w minimal gewählt war auch $bq \leq a$ also

$$r \geq 0.$$

Eindeutigkeit: Haben wir zwei solcher Darstellungen

$$b \cdot q_1 + r_1 = a = b \cdot q_2 + r_2$$

und ist OE $r_2 \leq r_1$, dann gilt

$$0 \leq \underbrace{r_1 - r_2}_{b\cdot(q_2-q_1)} < |b|\,,$$

also $q_1 = q_2$ und $r_1 = r_2$. ■

Der Beweis liefert einen expliziten (aber sehr ineffizienten) Algorithmus für die Division mit Rest. Praktisch geht man wie folgt vor:

Bemerkung 3.1.4 *Schulbuchdivision ohne Nachkommastellen bestimmt schrittweise die Dezimalstellen von q (beginnend mit der höchsten Dezimalstelle), gibt also einen Algorithmus zur Division mit Rest.*

Beispiel 3.1.5 *Für $a = 2225$ und $b = 7$ schreiben wir*

$$\begin{array}{rl} 2225 & = 7 \cdot 317 + 6 \\ -21 & \\ \hline 12 & \\ -7 & \\ \hline 55 & \\ -49 & \\ \hline 6 & \end{array}$$

also $q = 317$ und $r = 6$.

Mit Hilfe der Division mit Rest können wir Teilbarkeit algorithmisch entscheiden.

Definition 3.1.6 *Seien $a, b \in \mathbb{Z}$. Man sagt b **teilt** a*

$$b \mid a$$

wenn es ein $q \in \mathbb{Z}$ gibt mit $a = b{\cdot}q$. Dies bedeutet, dass die Division von a durch b Rest $r = 0$ liefert.

*Zwei Zahlen $a, b \in \mathbb{Z}$ heißen **teilerfremd**, wenn für $t \in \mathbb{N}$ mit $t \mid a$ und $t \mid b$ folgt $t = 1$.*

*Sei $m \in \mathbb{N}$ und $a, b \in \mathbb{Z}$. Dann heißt a **kongruent** zu b modulo m, geschrieben*

$$a \equiv b \bmod m,$$

wenn $m \mid (a - b)$.

Beispiel 3.1.7 $1 \equiv 7 \bmod 3$.

Kongruent modulo m zu sein ist eine Äquivalenzrelation, siehe dazu Übungsaufgabe 3.3. Dort implementieren wir auch eine Funktion, die Kongruenz modulo m mittels Division mit Rest entscheidet.

Für festgelegtes m schreiben wir die Äquivalenzklasse (genannt **Restklasse**) von a als

$$\begin{aligned}\overline{a} &= \{b \in \mathbb{Z} \mid a \equiv b \bmod m\} \\ &= \{a + k \cdot m \mid k \in \mathbb{Z}\}.\end{aligned}$$

Somit ist $a \equiv b \bmod m$ genau dann, wenn $\overline{a} = \overline{b}$.

Beispiel 3.1.8 *Kongruenz modulo* 3 *partitioniert* $\mathbb{Z}$ *in die* 3 *Restklassen*

$$\begin{aligned}\overline{0} &= \{..., -3, 0, 3, 6, ...\} \\ \overline{1} &= \{..., -2, 1, 4, 7, ...\} \\ \overline{2} &= \{..., -1, 2, 5, 8, ...\},\end{aligned}$$

denn bei der Division mit Rest von ganzen Zahlen nach 3 *treten genau die Reste* $0, 1, 2$ *auf.*

Restklassen spielen eine wichtige Rolle in vielen Publik-Key-Kryptosystemen. Darauf werden wir noch im Detail zurückkommen.

3.2 Fundamentalsatz der Arithmetik

Definition 3.2.1 *Ein Element* $p \in \mathbb{N}$, $p \geq 2$ *heißt* ***Primzahl****, wenn aus* $p = a \cdot b$, $a, b \in \mathbb{N}$ *folgt* $a = 1$ *oder* $b = 1$.

Beispiel 3.2.2 $2, 3, 5, 7, 11, 13, 17, 19, 23...$ *Die Bestimmung aller Primzahlen bis zu einer gegebenen Schranke werden wir im nächsten Abschnitt behandeln.*

Satz 3.2.3 (Fundamentalsatz der Arithmetik) *Jede Zahl* $n \in \mathbb{Z}\backslash\{0, -1, 1\}$ *hat eine eindeutige Darstellung*

$$n = \pm\, p_1^{r_1} \cdot ... \cdot p_s^{r_s}$$

mit Primzahlen $p_1 < ... < p_s$ *und* $r_i \in \mathbb{N}$. *Die* p_i *heißen* ***Primfaktoren*** *von* n.

Beweis. Existenz der Primfaktorzerlegung mit Induktion nach n:

$n = 2$ ist eine Primzahl. Ist $n > 2$ und keine Primzahl, dann ist $n = a \cdot b$ mit $a, b \neq 1$. Da $a, b < n$, haben a und b nach Induktionsvoraussetzung Zerlegungen, und durch sortieren der Primfaktoren erhalten wir eine Primfaktorzerlegung von $n = a \cdot b$.

Eindeutigkeit mit Induktion nach n:

$n = 2$ ist klar. Sei $n > 2$ und

$$n = p_1 \cdot \ldots \cdot p_s = q_1 \cdot \ldots \cdot q_t$$

mit $p_1 \leq \ldots \leq p_s$ und $q_1 \leq \ldots \leq q_t$. Ist $s = 1$ oder $t = 1$, dann ist n prim, und die Behauptung ist klar. Seien also $s, t \geq 2$.

Ist $p_1 = q_1$ dann hat

$$p_2 \cdot \ldots \cdot p_s = q_2 \cdot \ldots \cdot q_t < n$$

nach Induktionsvoraussetzung eine eindeutige Primfaktorzerlegung und die Behauptung folgt.

Angenommen es wäre $p_1 < q_1$. Dann gilt

$$n > \underbrace{p_1 \cdot (p_2 \cdot \ldots \cdot p_s - q_2 \cdot \ldots \cdot q_t)}_{=:N_1} = \underbrace{(q_1 - p_1) \cdot q_2 \cdot \ldots \cdot q_t}_{=:N_2} \geq 2,$$

also hat $N_1 = N_2$ nach Induktionsvoraussetzung eine eindeutige Primfaktorzerlegung. Wegen $p_1 < q_1 \leq \ldots \leq q_t$ ist $p_1 \neq q_i$, und p_1 ist kein Teiler von $q_1 - p_1$, denn sonst würde p_1 auch q_1 teilen. Somit ist p_1 ein Primfaktor von N_1, jedoch keiner von N_2, ein Widerspruch. ■

Beispiel 3.2.4 $24 = 2^3 \cdot 3$.

In MAPLE *können wir eine Primfaktorzerlegung berechnen mit:*

```
ifactor(24);
```

$(2)^3(3)$

Der Beweis des Fundamentalsatzes zeigt nur die Existenz einer eindeutigen Primfaktorzerlegung. Auf die algorithmische Berechnung einer solchen Zerlegung werden wir noch zurückkommen.

Aus dem Fundamentalsatz folgen sofort:

Corollar 3.2.5 (Euklids erster Satz) *Ist $p \in \mathbb{Z}$ prim und $a, b \in \mathbb{Z}$ mit $p \mid ab$, dann $p \mid a$ oder $p \mid b$.*

Beweis. Multiplikation der Primfaktorzerlegungen von a und b liefert die Primfaktorzerlegung von ab. ■

Corollar 3.2.6 (Euklids zweiter Satz) *Es gibt unendlich viele Primzahlen.*

Beweis. Sei $M = \{p_1, ..., p_r\}$ eine endliche Menge von Primzahlen. Wir zeigen, dass es eine Primzahl gibt, die nicht in M enthalten ist. Die Zahl $N = p_1 \cdot ... \cdot p_r + 1$ ist durch keine der Primzahlen p_i teilbar, denn sonst wäre auch 1 durch p_i teilbar. Ein Primfaktor p in einer Primfaktorzerlegung von N ist also eine Primzahl, die nicht in M liegt. ■

Ohne Beweis erwähnen wir folgenden Satz über die Dichte der Primzahlen:

Satz 3.2.7 (Primzahlsatz) *Sei für $x \in \mathbb{R}_{>0}$*

$$\pi(x) = |\{p \leq x \mid p \in \mathbb{N} \text{ prim}\}|$$

dann gilt

$$\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\ln(x)}} = 1.$$

Beispiel 3.2.8 *Das folgende Programm (in der Syntax von* MAPLE*) berechnet $\pi(x)$:*

```
pi:=proc(x)
local p,N;
p:=2;
N:=0:
while p<=x do
    p:=nextprime(p);
    N:=N+1;
od;
return(N);
end proc:
```

Damit erhalten wir z.B.

```
pi(100000);
```

9592

Siehe dazu auch Aufgabe 3.5.

3.3 Größter gemeinsamer Teiler und Euklidischer Algorithmus

Definition 3.3.1 *Sind $a_1, ..., a_t \in \mathbb{Z}$, dann heißt $d \in \mathbb{N}$ **größter gemeinsamer Teiler** von $a_1, ..., a_t$, geschrieben $d = \mathrm{ggT}(a_1, ..., a_t)$, wenn gilt*

1) *$d \mid a_j$ für alle $j = 1, ..., t$, d.h. d ist ein Teiler von allen a_j, und*

2) *ist $\tilde{d} \in \mathbb{Z}$ ein Teiler aller a_j, d.h. $\tilde{d} \mid a_j$ für alle $j = 1, ..., t$, dann gilt $\tilde{d} \mid d$.*

*Weiter heißt $m \in \mathbb{N}$ **kleinstes gemeinsames Vielfaches** von $a_1, ..., a_t$, geschrieben $m = \mathrm{kgV}(a_1, ..., a_t)$, wenn gilt*

1) *$a_j \mid m$ für alle $j = 1, ..., t$, d.h. m ist ein Vielfaches aller a_j, und*

2) *ist $\tilde{m} \in \mathbb{Z}$ ein Vielfaches aller a_j, d.h. $a_j \mid \tilde{m}$ für alle $j = 1, ..., t$, dann gilt $m \mid \tilde{m}$.*

Beispiel 3.3.2 *Die gemeinsamen Teiler von $18 = 2 \cdot 3^2$ und $66 = 2 \cdot 3 \cdot 11$ sind $1, 2, 3$ und 6, also gilt*

$$\mathrm{ggT}(18, 66) = 6.$$

Bemerkung 3.3.3 *Schreiben wir*

$$a_j = \pm 1 \cdot \prod_{i=1}^{s} p_i^{r_{ji}}$$

mit p_i prim und $r_{ji} \geq 0$, dann ist

$$\mathrm{ggT}(a_1, ..., a_t) = \prod_{i=1}^{s} p_i^{\min\{r_{ji} | j\}} \tag{3.1}$$

(und für kgV analog mit dem Maximum). Mit diesen Formeln sehen wir:

1) *Zwei Zahlen $a, b \in \mathbb{Z}$ sind teilerfremd genau dann, wenn*

$$\mathrm{ggT}(a, b) = 1.$$

2) Für $a, b \in \mathbb{N}$ ist

$$\mathrm{ggT}(a,b) \cdot \mathrm{kgV}(a,b) = a \cdot b.$$

Beispiel 3.3.4 *Für $18 = 2 \cdot 3^2$ und $66 = 2 \cdot 3 \cdot 11$ ist*

$$\mathrm{ggT}(18, 66) = 6.$$

Eine wesentlich effizientere Methode zur Bestimmung des größten gemeinsamen Teilers (und damit auch des kleinsten gemeinsamen Vielfachen) liefert der Euklidische Algorithmus:

Satz 3.3.5 (Euklidischer Algorithmus) *Seien $a_1, a_2 \in \mathbb{Z}\backslash\{0\}$. Dann terminiert die sukzessive Division mit Rest*

$$\begin{aligned} a_1 &= q_1 a_2 + a_3 \\ &\vdots \\ a_j &= q_j a_{j+1} + a_{j+2} \\ &\vdots \\ a_{n-2} &= q_{n-2} a_{n-1} + a_n \\ a_{n-1} &= q_{n-1} a_n + 0 \end{aligned}$$

und

$$\mathrm{ggT}(a_1, a_2) = a_n.$$

Rückwärtseinsetzen dieser Gleichungen

$$\begin{aligned} a_n &= a_{n-2} - q_{n-2} a_{n-1} \\ &\vdots \\ a_3 &= a_1 - q_1 a_2 \end{aligned}$$

liefert eine Darstellung

$$\mathrm{ggT}(a_1, a_2) = u \cdot a_1 + v \cdot a_2$$

mit $u, v \in \mathbb{Z}$. Die Berechnung dieser Darstellung bezeichnen wir auch als den ***erweiterten Euklidischen Algorithmus****.*

Beweis. Es ist $|a_{i+1}| < |a_i|$ für $i \geq 2$ und somit muss nach endlich vielen Schritten $a_i = 0$ sein. Es ist a_n ein Teiler von a_{n-1}, also auch von $a_{n-2} = q_{n-2} a_{n-1} + a_n$ und induktiv von $a_{n-1}, ..., a_1$. Ist t ein beliebiger Teiler von a_1 und a_2, dann auch von $a_3 = a_1 - q_1 a_2$ und induktiv von $a_1, ..., a_n$. ■

Beispiel 3.3.6 *Wir bestimmen den ggT von* 66 *und* 18 *mit Hilfe des Euklidischen Algorithmus, d.h. durch sukzessive Division mit Rest:*

$$66 = 3 \cdot 18 + 12$$
$$18 = 1 \cdot 12 + 6$$
$$12 = 2 \cdot 6 + 0$$

Somit ist $\mathrm{ggT}(66, 18) = 6$*, denn von unten gelesen gilt*

$$6 \mid 12 \text{ also } 6 \mid 18 \text{ also } 6 \mid 66$$

und von oben gelesen, ist t *ein Teiler von* 66 *und* 18*, dann*

$$t \mid 12 \text{ also } t \mid 6.$$

Weiter erhalten wir eine Darstellung von $\mathrm{ggT}(36, 15)$ *als* $\mathbb{Z}$*-Linearkombination von* 66 *und* 18

$$6 = 18 - 1 \cdot 12 = 18 - 1 \cdot (66 - 3 \cdot 18) = 4 \cdot 18 + (-1) \cdot 66.$$

In Maple *können wir den erweiterten Euklidischen Algorithmus durchführen mit:*

```
igcdex(66,18,'x','y');
6
```

Dabei werden in den Argumenten x *und* y *die Koeffizienten der Darstellung des ggT als Linearkombination gespeichert:*

```
x;
-1
y;
4
x*66+y*18;
6
```

Eine wesentliche Anwendung einer Darstellung der 1 als $\mathbb{Z}$-Linearkombination von zwei teilerfremden Zahlen ist das Lösen von simultanen Kongruenzen. Dies werden wir im nächsten Abschnitt über den Chinesischen Restsatz diskutieren.

3.4 Der chinesische Restsatz

Satz 3.4.1 (Chinesischer Restsatz in $\mathbb{Z}$) *Sind $n_1, ..., n_r \in \mathbb{N}$ paarweise teilerfremd und $a_1, ..., a_r \in \mathbb{Z}$, dann ist die* ***simultane Kongruenz***

$$\begin{aligned} x &\equiv a_1 \bmod n_1 \\ &\vdots \\ x &\equiv a_r \bmod n_r \end{aligned}$$

lösbar. Die Lösung ist eindeutig modulo $n = n_1 \cdot ... \cdot n_r$.

Beweis. Sei

$$\hat{n}_i = \frac{n}{n_i}$$

und finde mit dem erweiterten Euklidischen Algorithmus $x_i, y_i \in \mathbb{Z}$ mit

$$1 = \mathrm{ggT}\left(n_i, \hat{n}_i\right) = x_i n_i + y_i \hat{n}_i.$$

Dann ist

$$\begin{aligned} y_i \hat{n}_i &\equiv 0 \bmod n_j \ \ \forall j \neq i \\ y_i \hat{n}_i &\equiv 1 \bmod n_i. \end{aligned}$$

Somit erfüllt

$$z = \sum_{i=1}^{r} a_i y_i \hat{n}_i$$

die Kongruenzen und ebenso $z + k \cdot n$ für alle k. Sind x und x' Lösungen, dann $n_i \mid (x - x')$ für alle i. Somit gilt auch $\mathrm{kgV}(n_1, \dots, n_r) \mid (x - x')$. Da die n_i paarweise teilerfremd sind, ist $\mathrm{kgV}(n_1, \dots, n_r) = n_1 \cdot ... \cdot n_r$, d.h. es gilt

$$n \mid (x - x').$$

■

Der Chinesische Restsatz erlaubt uns also, eine beliebige Anzahl von Kongruenzen durch eine einzige äquivalente Kongruenz zu ersetzen. Praktisch fasst man iterativ jeweils zwei Kongruenzen zu einer zusammen. Deshalb formulieren wir das Lösungsverfahren in der folgenden Bemerkung nochmals für den Spezialfall $r = 2$:

Bemerkung 3.4.2 *Gegeben $n_1, n_2 \in \mathbb{N}$ teilerfremd und $a_1, a_2 \in \mathbb{Z}$, bestimmen wir eine Lösung der simultanen Kongruenzen*

$$x \equiv a_1 \bmod n_1$$
$$x \equiv a_2 \bmod n_2$$

Der erweiterte Euklidische Algorithmus liefert $u, v \in \mathbb{Z}$ mit

$$1 = \mathrm{ggT}(n_1, n_2) = u \cdot n_1 + v \cdot n_2$$

Wegen

$$un_1 \equiv 0 \bmod n_1$$
$$un_1 \equiv 1 \bmod n_2$$
$$vn_2 \equiv 1 \bmod n_1$$
$$vn_2 \equiv 0 \bmod n_2$$

gilt dann für

$$z := a_2 \cdot u \cdot n_1 + a_1 \cdot v \cdot n_2$$

dass

$$z \equiv a_1 \bmod n_1$$
$$z \equiv a_2 \bmod n_2$$

Ist x eine weitere Lösung, dann $n_i \mid (x - z)$ für $i = 1, 2$, und somit $n_1 n_2 \mid (x - z)$.

Insgesamt gilt

$$\left.\begin{array}{l} x \equiv a_1 \bmod n_1 \\ x \equiv a_2 \bmod n_2 \end{array}\right\} \Longleftrightarrow x \equiv z \bmod n_1 n_2$$

Iteratives Anwenden liefert einen weiteren Beweis von Satz 3.4.1.

Den Chinesischen Restsatz werden wir später wesentlich allgemeiner formulieren.

Beispiel 3.4.3 *Wir lösen die simultane Kongruenz*

$$x \equiv -28 \bmod 30$$
$$x \equiv 5 \bmod 7$$

Es ist $\mathrm{ggT}(30,7) = 1$*, also ist die Kongruenz lösbar. Mit dem erweiterten Euklidischen Algorithmus finden wir* u *und* v *mit*

$$u \cdot 30 + v \cdot 7 = 1$$

z.B. $u = -3$, $v = 13$*. Es gilt dann*

$$\begin{aligned}(-3) \cdot 30 &\equiv 0 \bmod 30\\ (-3) \cdot 30 &\equiv 1 \bmod 7\\ 13 \cdot 7 &\equiv 1 \bmod 30\\ 13 \cdot 7 &\equiv 0 \bmod 7\end{aligned}$$

und somit ist

$$z = (-28) \cdot (13 \cdot 7) + 5 \cdot (-3 \cdot 30) = -2998$$

eine Lösung (un diese ist eindeutig modulo 210*). Der Chinesische Restsatz erlaubt uns also zwei Kongruenzen durch eine einzelne Kongruenz zu ersetzen:*

$$\left.\begin{aligned}x &\equiv -28 \bmod 30\\ x &\equiv 5 \bmod 7\end{aligned}\right\} \Leftrightarrow x \equiv -2998 \equiv 152 \bmod 210.$$

Für letztere Kongruenz können wir die Lösungsmenge direkt angeben, sie ist

$$152 + 210 \cdot \mathbb{Z} = \{152 + k \cdot 210 \mid k \in \mathbb{Z}\},$$

also die Restklasse $\overline{152}$*.*

Sind die Moduli n_i nicht teilerfremd, so kann man eine sehr ähnliche Lösungsformel aufstellen, allerdings kann dann die Kongruenz auch unlösbar sein. Ein Kriterium gibt der folgende Satz:

Satz 3.4.4 *Seien* $a_1, a_2 \in \mathbb{Z}$ *und* $n_1, n_2 \in \mathbb{N}$*. Dann sind die simultanen Kongruenzen*

$$\begin{aligned}x &\equiv a_1 \bmod n_1\\ x &\equiv a_2 \bmod n_2\end{aligned}$$

genau dann lösbar, wenn

$$a_1 - a_2 \equiv 0 \bmod \mathrm{ggT}(n_1, n_2).$$

Die Lösung ist eindeutig modulo dem $\mathrm{kgV}(n_1, n_2)$*.*

Dies zeigen wir in Übungsaufgabe 3.12, indem wir die entsprechende Lösungsformel herleiten.

3.5 Primfaktorisierung

Zunächst behandeln wir folgendes offensichtliche Primfaktorisierungsverfahren:

Algorithmus 3.5.1 (Probedivision) *Sei $n \in \mathbb{N}$ zusammengesetzt (nicht prim). Für den kleinsten Primteiler p von n gilt*

$$p \leq m := \left\lfloor \sqrt{n} \right\rfloor.$$

Kennen wir alle Primzahlen $p \leq m$, dann testen wir $p \mid n$ mit Division mit Rest. Damit können wir eine gegebene Zahl n faktorisieren.

Beweis. Schreibe $n = p \cdot q$. Dann gilt $p^2 \leq p \cdot q = n$, also $p \leq \sqrt{n}$. Wegen $p \in \mathbb{N}$ ist also $p \leq \left\lfloor \sqrt{n} \right\rfloor$. ∎

Beispiel 3.5.2 *Zum Faktorisieren von 234 mittels Probedivision testen wir zunächst, ob n durch eine Primzahl $p \leq \left\lfloor \sqrt{234} \right\rfloor = 15$ teilbar ist. Wir finden*

$$234 = 2 \cdot 117.$$

Ist 117 nicht prim, so muss ein Primteiler $p \leq \left\lfloor \sqrt{117} \right\rfloor = 10$ vorkommen, wir finden

$$117 = 3 \cdot 39.$$

Ist 39 nicht prim, so muss ein Primteiler $p \leq \left\lfloor \sqrt{39} \right\rfloor = 6$ vorkommen, und wir finden

$$39 = 3 \cdot 13.$$

Schließlich ist 13 prim, denn 13 ist durch keine Primzahl $p \leq \left\lfloor \sqrt{13} \right\rfloor = 3$ teilbar.

Die Probedivision erlaubt uns auch, alle Primzahlen $\leq n$ induktiv aufzuzählen, denn kennen wir schon alle Primzahlen $p \leq \left\lfloor \sqrt{n} \right\rfloor < n$, so können wir durch Faktorisieren entscheiden, ob n prim ist.

Beispiel 3.5.3 *Wir bestimmen alle Primzahlen* ≤ 11. *Für den kleinsten Primteiler von* n *gilt* $p \leq m$, *wir erhalten also:*

n	m		
2	1		$\Rightarrow 2$ *prim*
3	1		$\Rightarrow 3$ *prim*
4	2	$4 = 2 \cdot 2$	$\Rightarrow 4$ *nicht prim*
5	2	$2 \nmid 5$	$\Rightarrow 5$ *prim*
6	2	$6 = 2 \cdot 3$	$\Rightarrow 6$ *nicht prim*
7	2	$2 \nmid 7$	$\Rightarrow 7$ *prim*
8	2	$8 = 2 \cdot 4$	$\Rightarrow 8$ *nicht prim*
9	3	$9 = 3 \cdot 3$	$\Rightarrow 9$ *nicht prim*
10	3	$10 = 2 \cdot 5$	$\Rightarrow 10$ *nicht prim*
11	3	$2 \nmid 11$ *und* $3 \nmid 11$	$\Rightarrow 11$ *prim*

Praktisch geht man aber umgekehrt vor, und streicht Vielfache von schon bekannten Primzahlen:

Algorithmus 3.5.4 (Sieb des Eratosthenes) *Wir erhalten eine Liste aller Primzahlen kleiner gleich* $N \in \mathbb{N}$, $N \geq 4$ *wie folgt:*

1) *Erstelle eine boolsche Liste* L *mit einem Eintrag zu jeder Zahl* $2, ..., N$. *Markiere alle Zahlen als prim* $(true)$. *Setze* $p = 2$.

2) *Markiere alle* $j \cdot p$ *mit* $j \geq p$ *als nicht prim* $(false)$.

3) *Finde das kleinste* $q > p$, *das als prim* $(true)$ *markiert ist. Falls* $q > \sqrt{N}$ *gebe* L *zurück. Setze* $p := q$, *gehe zu Schritt* (2).

Beweis. In Schritt (2) sind alle $j \cdot p$ mit $2 \leq j < p$ schon aus vorherigen Schritten als $false$ markiert, da sie einen Primteiler $< p$ besitzen. Somit sind alle echten Vielfachen von p als $false$ markiert.

Die Zahl q in Schritt (3) ist stets prim: Nach Wahl von q ist p die größte Primzahl $< q$, aus vorherigen Schritten sind alle Vielfachen $j \cdot x$ von allen Primzahlen $x \leq p$ als $false$ markiert. Wäre q nicht prim, müsste q aber ein solches p als Primteiler haben, wäre also als $false$ markiert.

Sobald der Algorithmus terminiert, sind also alle Zahlen als $false$ markiert, die eine Primzahl $p \leq \sqrt{N}$ als echten Teiler haben, d.h. nicht prim sind. ■

Beispiel 3.5.5 *Wir bestimmen alle Primzahlen* ≤ 15 *und geben in jedem Durchlauf die Liste aller* j *mit* $L_j = true$ *an:*

	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$p = 2$	2	3		5		7		9		11		13		15
$p = 3$	2	3		5		7				11		13		

Im ersten Schritt streichen wir alle Vielfachen von 2*, im zweiten Schritt alle Vielfachen von* 3*. Alle verbliebenen Zahlen sind prim, denn* $p = 5 > \sqrt{15}$*.*

Für große Zahlen gibt es wesentlich effizientere Methoden als Probedivision, um einen Primteiler zu finden. Darauf werden wir noch zurückkommen.

3.6 Übungsaufgaben

Übung 3.1 *Sei* $n \in \mathbb{N}$ *und* $M \subset \{1, \ldots, 2n\}$ *eine Menge von ganzen Zahlen mit* $|M| = n + 1$ *Elementen. Zeigen Sie, dass es in* M *zwei verschiedene Zahlen gibt, sodass die eine Zahl die andere teilt.*

Übung 3.2 *Zeigen Sie:*

1) *Auf* $M = \mathbb{N}_0 \times \mathbb{N}_0$ *ist durch*

$$(a, b) \sim (c, d) \Leftrightarrow a + d = b + c$$

eine Äquivalenzrelation gegeben.

2) *Die Verknüpfungen Addition und Multiplikation*

$$[(a, b)] + [(c, d)] = [(a + c, b + d)]$$
$$[(a, b)] \cdot [(c, d)] = [(a \cdot c + b \cdot d, a \cdot d + b \cdot c)]$$

auf

$$\mathbb{Z} = (\mathbb{N}_0 \times \mathbb{N}_0) \,/\, \sim$$

sind wohldefiniert, assoziativ, kommutativ und distributiv.

Auf diese Eigenschaften werden wir allgemeiner im Zusammenhang mit Gruppen und Ringen zurückkommen.

Übung 3.3 *1) Sei $m \in \mathbb{N}$ und $a, b \in \mathbb{Z}$. Dann heißt a kongruent zu b modulo m*

$$a \equiv b \bmod m$$

wenn $m \mid (a-b)$. Zeigen Sie, dass "modulo m kongruent sein" eine Äquivalenzrelation ist.

2) Schreiben Sie eine Funktion, die $a \equiv b \bmod m$ entscheidet.

3) Zeigen Sie, dass $11111111111 \equiv 67360232502 \bmod 123259$.

Übung 3.4 *Zeigen Sie:*

1) Ist $r \in \mathbb{N}$ und $p = 2^r - 1$ prim, dann ist r prim.

2) Ist $r \in \mathbb{N}$ und $p = 2^r + 1$ prim, dann ist $r = 2^k$ mit $k \in \mathbb{N}_0$.

Übung 3.5 *Überprüfen Sie den Primzahlsatz experimentell in* MAPLE*:*

1) Schreiben Sie eine Prozedur, die

$$\pi(x) = |\{p \leq x \mid p \in \mathbb{N} \text{ prim}\}|$$

für $x > 0$ berechnet.

2) Vergleichen Sie die Funktion $\frac{\pi(x)}{x}$ mit $\frac{1}{\ln(x)-a}$ für $a \in \mathbb{Z}_{\geq 0}$, insbesondere für große x. Für welches a erhalten Sie die beste Approximation?

3) Stellen Sie Ihre Beobachtungen graphisch dar.

Hinweis: Verwenden Sie die MAPLE*-Funktion* nextprime.

Übung 3.6 *Sei P_N die Wahrscheinlichkeit, dass zufällig gewählte natürliche Zahlen $n, m \leq N$ teilerfremd sind. Bestimmen Sie P_N für $N = 10^6, 10^{12}$ und 10^{18} approximativ durch Stichproben im Umfang von jeweils 10^2, 10^4 und 10^6 Versuchen mit Hilfe eines Computeralgebrasystems. Überprüfen Sie experimentell, dass P_N für grosse Werte von N den Wert*

$$\frac{6}{\pi^2} \approx 60.7\%$$

annimmt.

Übung 3.7 *Implementieren Sie den erweiterten Euklidischen Algorithmus. Testen Sie Ihre Implementierung an Beispielen.*

Übung 3.8 *Kürzen Sie*

$$\frac{90297278063}{18261358091}$$

Übung 3.9 *Auf ein urspünglich leeres Konto werden regelmäßig* $2809\,€$ *gutgeschrieben, und gelegentlich* $10403\,€$ *abgebucht. Ist es möglich, dass das Konto irgendwann einen Kontostand von genau* $1\,€$ *hat?*

Übung 3.10 *Implementieren Sie*

1) *das Sieb des Eratosthenes und*
2) *die Faktorisierung von ganzen Zahlen mittels Probedivision.*
3) *Bestimmen Sie die Primfaktorzerlegung von*

$$116338867864982351.$$

Übung 3.11 *Bestimmen Sie die Menge* $L \subset \mathbb{Z}$ *aller Lösungen* x *der simultanen Kongruenzen*

$$\begin{aligned} x &\equiv 2 \bmod 3 \\ x &\equiv 2 \bmod 7 \\ x &\equiv 3 \bmod 10 \end{aligned}$$

Übung 3.12 *Seien* $a_1, a_2 \in \mathbb{Z}$ *und* $n_1, n_2 \in \mathbb{Z}_{>0}$*. Zeigen Sie: Die simultanen Kongruenzen*

$$\begin{aligned} x &\equiv a_1 \bmod n_1 \\ x &\equiv a_2 \bmod n_2 \end{aligned}$$

sind genau dann lösbar, wenn

$$a_1 - a_2 \equiv 0 \bmod \mathrm{ggT}\,(n_1, n_2)$$

Die Lösung ist eindeutig modulo dem $\mathrm{kgV}\,(n_1, n_2)$*.*

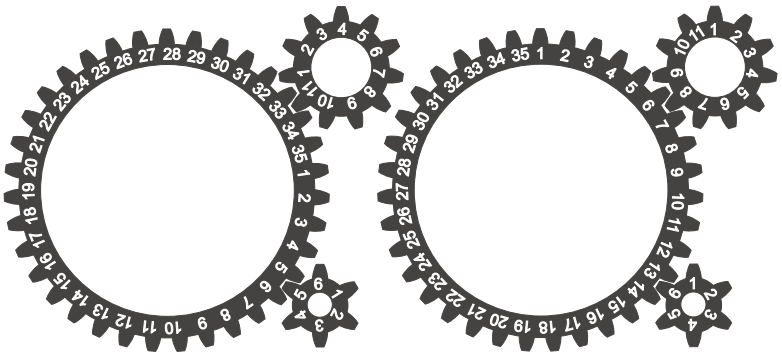


Abbildung 3.1: Zwei Konfigurationen von drei Zahnrädern

Übung 3.13 *Lassen sich die beiden Konfigurationen von Zahnrädern in Abbildung 3.1 durch Drehung ineinander überführen? Falls ja, um wieviele Schritte muss man dafür drehen?*

Übung 3.14 *Bestimmen Sie die Menge $L \subset \mathbb{Z}$ aller Lösungen x der simultanen Kongruenzen*

$$x \equiv 1 \bmod 108$$
$$x \equiv 25 \bmod 80$$

Übung 3.15 *Schreiben Sie mit Hilfe Ihrer Implementierung des erweiterten Euklidischen Algorithmus (oder der* MAPLE*-Funktion* igcdex*) eine Prozedur, die die Lösungsmenge der simultanen Kongruenzen*

$$x \equiv a_1 \bmod n_1$$
$$x \equiv a_2 \bmod n_2$$

für $a_1, a_2 \in \mathbb{Z}$ und $n_1, n_2 \in \mathbb{Z}_{>0}$ mit $\mathrm{ggT}(n_1, n_2) = 1$ bestimmt. Vergleichen Sie mit der MAPLE*-Funktion* chrem*.*

Erweitern Sie die Funktionalität Ihrer Implementierung so, dass sie auch im Fall nicht teilerfremder n_1, n_2 korrekt funktioniert.

4

Gruppen

4.1 Übersicht

In diesem Kapitel beschäftigen wir uns mit den Grundlagen der Gruppentheorie, die vielfältige Anwendungen in den weiteren Kapiteln über Ringe, Körper und lineare Algebra haben. Als Beispiele für Gruppen betrachten wir Symmetriegruppen von Teilmengen des $\mathbb{R}^n$, z.B. die Mengen der Drehungen und (Dreh-) Spiegelungen, die jeweils einen der Platonischen Körper Tetraeder, Würfel, Oktaeder, Dodekaeder und Ikosaeder (siehe Abbildung 4.1) wieder in sich selbst überführen. Die Gruppeneigenschaft sieht man hier (u.a.) dadurch, dass das Hintereinanderausführen von zwei Symmetrien wieder eine Symmetrie ist und wir jede Symmetrie durch eine andere wieder rückgängig machen können. Zum Beispiel ist in der Symmetriegruppe des Tetraeders die Drehsymmetrie um 120° gleich dem Produkt von zwei Spiegelungen, siehe Abbildung 4.2.

Allgemein gilt: Die Komposition von zwei Symmetrien ist wieder eine Symmetrie. Zu jeder Symmetrie gibt es eine inverse Symmetrie, sodass die Komposition die identische Abbildung gibt.

Für Symmetriegruppen spielt der Begriff der Operation einer Gruppe G auf einer Menge M eine wichtige Rolle. Zum Beispiel könnte G die Symmetriegruppe des Tetraeders sein und M der Tetraeder oder die Menge der Eckpunkte, der Kanten oder Seiten des Tetraeders. Eine Gruppenoperation ist eine Abbildung (mit

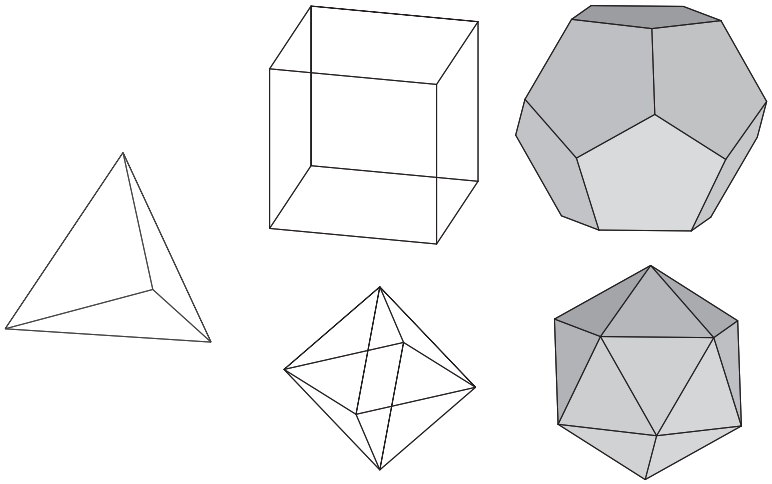


Abbildung 4.1: Die Platonischen Körper

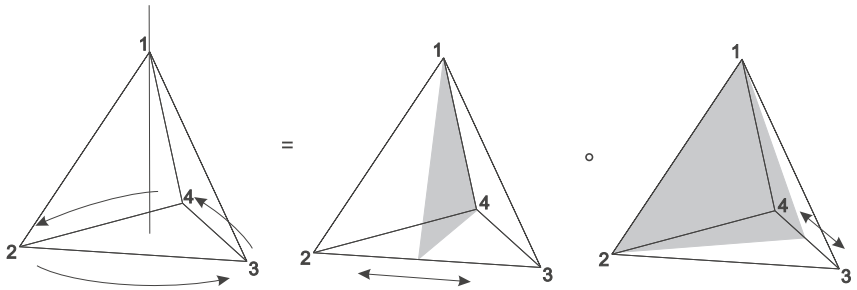


Abbildung 4.2: Komposition von zwei Symmetrien des Tetraeders

einigen offensichtlichen Zusatzbedingungen)

$$\begin{array}{ccc} G \times M & \longrightarrow & M \\ (g, m) & \longmapsto & g \cdot m \end{array}$$

d.h. ein Gruppenelement g bildet ein Element $m \in M$ auf ein anderes Element von M ab, das wir $g \cdot m$ nennen. Starten wir mit einem m und wenden alle Elemente von G an, erhalten wir die Bahn von m, zum Beispiel können wir jede Ecke des Tetraeders durch eine Symmetrie auf jede andere Ecke abbilden. Auf diese Weise zerlegt sich M in disjunkte Bahnen. Als zentralen Satz beweisen wir die Bahnengleichung.

Die beiden wichtigsten Beispiele von Operationen für die Konstruktion und Klassifikation von Gruppen sind jedoch die einer Untergruppe $H \subset G$ durch Translation

$$\begin{array}{ccc} H \times G & \longrightarrow & G \\ (h, g) & \longmapsto & hg \end{array}$$

und von G auf sich selbst durch Konjugation

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (a, b) & \longmapsto & aba^{-1} \end{array}$$

Die Translation werden wir im Detail diskutieren und auf die Konjugation in Übung 4.12 zurückkommen.

4.2 Gruppen und Operationen

4.2.1 Grundbegriffe

Definition 4.2.1 *Eine* ***Gruppe*** $(G, \circ)$ *ist eine Menge* G *zusammen mit einer* ***Verknüpfung***

$$\begin{array}{rccc} \circ : & G \times G & \longrightarrow & G \\ & (a, b) & \mapsto & a \circ b \end{array}$$

die folgende Axiome erfüllt:

(G1) Assoziativität

$$a \circ (b \circ c) = (a \circ b) \circ c \ \forall a, b, c \in G$$

(G2) Es existiert ein neutrales Element, d.h. ein

$$e \in G$$

mit

$$e \circ a = a \circ e = a \ \forall a \in G$$

(G3) Existenz des Inversen, d.h. $\forall a \in G \ \exists a^{-1} \in G$ *mit*

$$a^{-1} \circ a = a \circ a^{-1} = e$$

Gilt außerdem das Kommutativgesetz

$$a \circ b = b \circ a \ \forall a, b \in G$$

dann heißt G ***abelsch****.*

Eine Menge G zusammen mit einer Verknüpfung

$$\circ : \quad G \times G \quad \longrightarrow \quad G$$

die $(G1)$ erfüllt, nennt man ***Halbgruppe****, $(G, \circ)$ mit $(G1)$ und $(G2)$ heißt* ***Monoid****.*

Die Anzahl der Elemente $|G|$ bezeichnet man als die ***Ordnung*** *von G (kann ∞ sein).*

Bemerkung 4.2.2 *Setzt man für eine Gruppe G nur die Existenz eines linksneutralen Elements $e \in G$ mit $e \circ a = a \ \forall a \in G$ und von linksinversen Elementen a^{-1} für jedes $a \in G$ mit $a^{-1} \circ a = e$ voraus, dann ist e auch rechtsneutral und die a^{-1} sind rechtsinvers:*

1) Für $a, b \in G$ gilt: Ist $a \circ b = e$, dann ist auch $b \circ a = e$.

2) Es ist $a \circ e = a$ für alle $a \in G$.

Bemerkung 4.2.3 *Ist G eine Gruppe so gilt:*

1) Das neutrale Element von G ist eindeutig.

2) Die Inversen der Elemente von G sind eindeutig.

3) Für $a, b \in G$ ist $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$.

4) Für $a \in G$ ist $(a^{-1})^{-1} = a$.

Diese Aussagen zeigen wir in Übung 4.2.

Neben den in Abschnitt 4.1 angesprochenen Symmetriegruppen wollen wir noch die folgenden zentralen Beispiele von Gruppen diskutieren:

Beispiel 4.2.4 *1) Die Menge der ganzen Zahlen mit der Addition*

$$(\mathbb{Z}, +)$$

ist eine Gruppe. Das neutrale Element ist die 0.

2) *Die Menge der ganzen Zahlen zusammen mit der Multiplikation*

$$(\mathbb{Z}, \cdot)$$

bildet ein Monoid. Das neutrale Element ist die 1.

3) *Die Menge der rationalen Zahlen ungleich* 0 *zusammen mit der Multiplikation*

$$(\mathbb{Q}\backslash\{0\}, \cdot)$$

bildet eine Gruppe.

4) *Sei X eine beliebige Menge. Die Menge der Selbstabbildungen von X*

$$S(X) = \{f : X \longrightarrow X \mid f \text{ bijektiv}\}$$

zusammen mit der Komposition ist eine Gruppe.

Speziell für

$$X = \{1, ..., n\}$$

heißt die Menge der ***Permutationen*** *von n Elementen*

$$S_n := S(\{1, ..., n\})$$

die ***symmetrische Gruppe****. Offenbar gilt*

$$|S_n| = n \cdot (n-1) \cdot ... \cdot 2 \cdot 1 = n!$$

Für $\sigma \in S_n$ schreiben wir auch

$$\sigma = \begin{pmatrix} 1 & \cdots & n \\ \sigma(1) & \cdots & \sigma(n) \end{pmatrix}$$

Ein Element von S_n heißt ***Transposition****, wenn es genau zwei Elemente von X vertauscht.*

Durch Nummerieren der Ecken können wir die Drehung des Tetraeders in Abbildung 4.3 mit der Permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} \in S_4$$

und die Spiegelung in Abbildung 4.4 mit der Transposition

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} \in S_4$$

identifizieren.

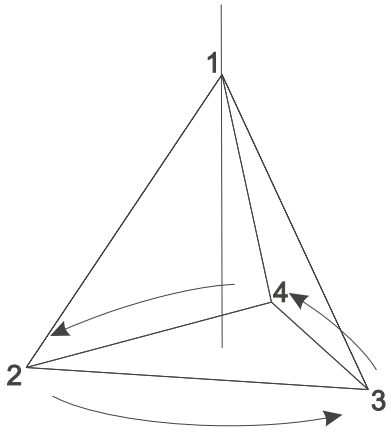


Abbildung 4.3: Eine Drehsymmetrie des Tetraeders

5) *Sei*

$$A = \{\alpha, \beta, \gamma, ...\}$$

eine endliche Menge. Ein ***Wort*** *über dem Alphabet A ist eine endliche Folge*

$$w = b_1 b_2 ... b_n$$

mit $b_i \in A$. *Gegeben ein weiteres Wort* $v = a_1 ... a_m$, *definiert man die Verknüpfung "Hintereinanderschreiben"durch*

$$w \circ v = b_1 ... b_n a_1 ... a_m$$

Die Menge

$$G = \{w \mid w \text{ ein Wort über } A\}$$

zusammen mit $\circ$ *bildet eine Halbgruppe.*

Erlauben wir in G auch das leere Wort e, dann wird $(G, \circ)$ *zu einem Monoid.*

6) *Fügen wir zusätzliche Buchstaben* $\alpha^{-1}, \beta^{-1}, ...$ *mit der Rechenregel*

$$\alpha\alpha^{-1} = \alpha^{-1}\alpha = e$$

hinzu, dann erhalten wir die ***freie Gruppe*** *erzeugt von A.*

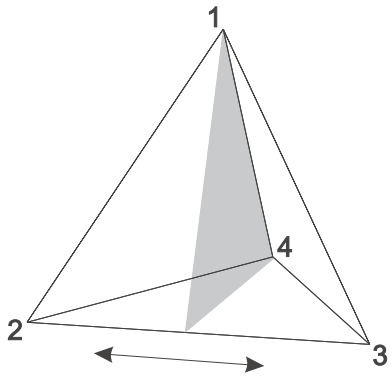


Abbildung 4.4: Eine Spiegelsymmetrie des Tetraeders

7) *Sind G_1, G_2 Gruppen, dann ist das* ***kartesische Produkt*** $G_1 \times G_2$ *von G_1 und G_2 mit der Verknüpfung*

$$(a_1, b_1) \circ (a_2, b_2) := (a_1 \circ a_2, b_1 \circ b_2)$$

ebenfalls eine Gruppe.

Definition und Satz 4.2.5 (Untergruppenkriterium) *Sei $(G, \circ)$ eine Gruppe. Eine Teilmenge $H \subset G$ heißt* ***Untergruppe****, wenn die beiden folgenden äquivalenten Bedingungen erfüllt sind*

1) *$(H, \circ)$ ist eine Gruppe (d.h. $e \in H$ und $a, b \in H \Longrightarrow a \circ b \in H$, $b^{-1} \in H$)*

2) *$H \neq \varnothing$, und $a, b \in H \Longrightarrow a \circ b^{-1} \in H$.*

Beweis. (1) $\Rightarrow$ (2) ist klar. Ist umgekehrt $H \neq \varnothing$, dann gibt es ein $a \in H$. Für dieses gilt $e = a \circ a^{-1} \in H$, und somit für alle $a \in H$, dass $a^{-1} = e \circ a^{-1} \in H$. Also für alle $a, b \in H$ ist $b^{-1} \in H$, und damit

$$a \circ b = a \circ \left(b^{-1}\right)^{-1} \in H.$$

■

Beispiel 4.2.6 *Sei G die Symmetriegruppe des Tetraeders, r_{120} die Drehung in Abbildung 4.3 und s_{23} die Spiegelung in Abbildung 4.4. Dann sind*

$$\{id, r_{120}, (r_{120})^2\} \subset G$$
$$\{id, s_{23}\} \subset G$$

jeweils Untergruppen.

Beispiel 4.2.7 *Die Untergruppen von* $(\mathbb{Z}, +)$ *haben die Gestalt*

$$n\mathbb{Z} := \{n \cdot k \mid k \in \mathbb{Z}\}$$

wobei $n \in \mathbb{Z}_{\geq 0}$.

Beweis. Mit dem Untergruppenkriterium sieht man sofort, dass $n\mathbb{Z} \subset \mathbb{Z}$ eine Untergruppe ist. Sei umgekehrt $H \subset \mathbb{Z}$ eine Untergruppe. Entweder gilt $H = \{0\}$ oder es gibt ein kleinstes Element $n > 0$ in H. Wir zeigen, dass dann $H = n\mathbb{Z}$ gilt: Sei $m \in H$. Division mit Rest liefert eine Darstellung

$$m = qn + r$$

mit $0 \leq r < n$ und $r \in H$. Nach der Definition von n folgt $r = 0$, also $m \in n\mathbb{Z}$. ■

Beispiel 4.2.8 *Sei* $n \in \mathbb{N}$ *und* $a \in \mathbb{Z}$. *Die Äquivalenzklasse (Restklasse) von* a *modulo* n *kann man mit Hilfe der Untergruppe* $n\mathbb{Z} \subset \mathbb{Z}$ *ausdrücken als*

$$\begin{aligned}\overline{a} &= \{b \in \mathbb{Z} \mid a \equiv b \bmod n\} \\ &= a + n\mathbb{Z} := \{a + b \mid b \in n\mathbb{Z}\} = \{a + k \cdot n \mid k \in \mathbb{Z}\} \subset \mathbb{Z}\end{aligned}$$

(siehe auch Übungsaufgabe 3.3).

Die Menge der Restklassen

$$\mathbb{Z}_n := \mathbb{Z}/n := \left\{\overline{0}, \overline{1}, \overline{2}, ..., \overline{n-1}\right\}$$

wird mit der Verknüpfung

$$\overline{a} + \overline{b} := \overline{a + b}$$

eine Gruppe, die ***Gruppe der Restklassen modulo n*** *(mit neutralem Element* $\overline{0}$ *und Inversem* $-\overline{a} = \overline{-a}$ *von* $\overline{a} \in \mathbb{Z}/n$*).*

Da $\overline{a} + \overline{b} := \overline{a + b}$ *nicht in Termen von* $\overline{a}$ *und* $\overline{b}$ *sondern den Repräsentanten* a *und* b *definiert ist, müssen wir noch zeigen, dass* $\overline{a} + \overline{b}$ *wohldefiniert ist, d.h. nicht von der Wahl der Repräsentanten* a *und* b *abhängt:*

Ist $\overline{a_1} = \overline{a_2}$ *und* $\overline{b_1} = \overline{b_2}$, *also* $a_1 - a_2 = n \cdot k_1$ *und* $b_1 - b_2 = n \cdot k_2$ *mit Zahlen* k_1, k_2, *so gilt*

$$\overline{a_1} + \overline{b_1} = \overline{a_1 + b_1} = \overline{a_2 + b_2 + n \cdot (k_1 + k_2)} = \overline{a_2 + b_2} = \overline{a_2} + \overline{b_2}.$$

Beispiel 4.2.9 *Für $n = 3$ ist $\mathbb{Z}/3 = \{\overline{0}, \overline{1}, \overline{2}\}$ mit*

$$\overline{0} = \{..., -3, 0, 3, 6, ...\} = 3\mathbb{Z}$$
$$\overline{1} = \{..., -2, 1, 4, 7, ...\} = 1 + 3\mathbb{Z}$$
$$\overline{2} = \{..., -1, 2, 5, 8, ...\} = 2 + 3\mathbb{Z}$$

siehe auch Abbildung 4.5.

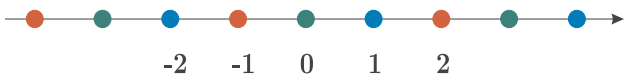


Abbildung 4.5: Restklassen modulo 3

Die Verknüpfung kann man durch eine Tabelle beschreiben werden

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

*die **Verknüpfungstafel** oder **Gruppentafel**, beispielsweise gilt* $\overline{2} + \overline{2} = \overline{2 + 2} = \overline{4} = \overline{1}$.

Beispiel 4.2.10 *Für jeden Teiler a von n und $d = \frac{n}{a}$ ist*

$$\left\{\overline{0}, \overline{a}, \overline{2a}, ..., \overline{(d-1)a}\right\} \subset \mathbb{Z}/n$$

eine Untergruppe (Übung).

Zum Beispiel für $n = 6$ und $a = 2$ erhalten wir die Untergruppe

$$\left\{\overline{0}, \overline{2}, \overline{4}\right\} \subset \mathbb{Z}/6.$$

Vergleichen wir die Gruppentafel

$+$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{0}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{2}$

dieser Gruppe mit der von $\mathbb{Z}/3$, so fällt auf, dass die Elemente der beiden Gruppen zwar verschiedene Namen haben, aber denselben Rechenregeln gehorchen.

Die Identifikation der Untergruppe $\left\{\overline{0},\overline{2},\overline{4}\right\} \subset \mathbb{Z}/6$ mit $\mathbb{Z}/3$ ist ein Beispiel eines Gruppenisomorphismus, d.h. einer bijektiven Abbildung, die die Gruppenstruktur erhält. Der Gruppenisomorphismus

$$\begin{array}{rccc} \varphi: & \mathbb{Z}/3 & \longrightarrow & \left\{\overline{0},\overline{2},\overline{4}\right\} \\ & 0+3\mathbb{Z} & \longmapsto & 0+6\mathbb{Z} \\ & 1+3\mathbb{Z} & \longmapsto & 2+6\mathbb{Z} \\ & 2+3\mathbb{Z} & \longmapsto & 4+6\mathbb{Z} \end{array}$$

erfüllt zum Beispiel

$$\varphi\left(\overline{1}+\overline{1}\right) = \varphi\left(\overline{2}\right) = \overline{4} = \overline{2}+\overline{2} = \varphi\left(\overline{1}\right)+\varphi\left(\overline{1}\right).$$

Wir scheiben dann

$$\mathbb{Z}/3 \cong \left\{\overline{0},\overline{2},\overline{4}\right\}$$

und allgemeiner gilt

$$\mathbb{Z}/d \cong \left\{\overline{0},\overline{a},\overline{2a},...,\overline{(d-1)a}\right\}.$$

Definition 4.2.11 *Ein **Gruppenhomomorphismus** φ zwischen zwei Gruppen G_1 und G_2 ist eine Abbildung*

$$\varphi: G_1 \longrightarrow G_2$$

die

$$\varphi(a \circ b) = \varphi(a) \circ \varphi(b) \quad \forall a,b \in G_1$$

erfüllt, also die Verknüpfungsstruktur erhält.

Man beachte, dass $\circ$ auf der linken Seite die Verknüpfung in G_1, auf der rechten Seite die in G_2 bezeichnet.

Bemerkung 4.2.12 *Ist $\varphi: G_1 \longrightarrow G_2$ ein Gruppenhomomorphismus, so gilt*

$$\varphi(e_1) = e_2$$

wobei $e_i \in G_i$ jeweils das neutrale Element bezeichnet.

*Der **Kern** von φ*

$$\operatorname{Ker}\varphi = \{a \in G_1 \mid \varphi(a) = e_2\}$$

*und das **Bild** von φ*

$$\operatorname{Bild}\varphi = \varphi(G_1)$$

sind Untergruppen von G_1 bzw. G_2.

Für den Beweis der Aussagen siehe Übung 4.4.

Zum Beispiel für den Gruppenhomomorphismus $\varphi : \mathbb{Z}/3 \to \mathbb{Z}/6$, gegeben durch $\overline{1} \mapsto \overline{2}$ wie oben, erhalten wir

$$\operatorname{Bild}\varphi = \left\{\overline{0}, \overline{2}, \overline{4}\right\}$$
$$\operatorname{Ker}\varphi = \left\{\overline{0}\right\}.$$

Lemma 4.2.13 *Ein Gruppenhomomorphismus $\varphi : G_1 \longrightarrow G_2$ ist injektiv genau dann, wenn*

$$\operatorname{Ker}\varphi = \{e_1\},$$

d.h. der Kern nur das neutrale Element e_1 von G_1 enthält.

Beweis. Wir bemerken zunächst, dass für $b \in G_1$

$$(\varphi(b))^{-1} = \varphi\left(b^{-1}\right)$$

da

$$\varphi(b) \circ \varphi\left(b^{-1}\right) = \varphi(b \circ b^{-1}) = \varphi(e_1) = e_2,$$

und das Inverse eindeutig bestimmt ist. Für $a, b \in G_1$ gilt damit

$$\varphi(a) = \varphi(b) \Longleftrightarrow \varphi\left(a \circ b^{-1}\right) = e_2 \Longleftrightarrow a \circ b^{-1} \in \operatorname{Ker}\varphi.$$

denn

$$\varphi(a) \circ (\varphi(b))^{-1} = \varphi(a) \circ \varphi\left(b^{-1}\right) = \varphi(a \circ b^{-1})$$

Ist also $\operatorname{Ker}\varphi = \{e_1\}$, dann folgt aus $\varphi(a) = \varphi(b)$, dass $a = b$.

Ist umgekehrt φ injektiv, dann folgt aus

$$\varphi(a) = e_2 = \varphi(e_1)$$

dass $a = e_1$. ■

Definition und Satz 4.2.14 *Injektive Gruppenhomomorphismen nennt man auch (Gruppen-)* ***Monomorphismen****, surjektive Gruppenhomomorphismen (Gruppen-)* ***Epimorphismen****.*

Ein (Gruppen-) ***Isomorphismus***

$$\varphi : G_1 \longrightarrow G_2$$

ist ein bijektiver Homomorphismus. Die Umkehrabbildung

$$\varphi^{-1} : G_2 \longrightarrow G_1$$

ist dann ebenfalls ein Homomorphismus. Wir schreiben auch $G_1 \cong G_2$.

Siehe auch Übung 4.4.

Beispiel 4.2.15 *1) Die Inklusion einer Untergruppe $H \hookrightarrow G$ ist ein Monomorphismus.*

2) Die Abbildung

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & n\mathbb{Z} \\ k & \longmapsto & n \cdot k \end{array}$$

ist für $n \geq 1$ ein Isomorphismus.

*3) Die **Exponentialfunktion***

$$\begin{array}{ccc} (\mathbb{R}, +) & \longrightarrow & (\mathbb{R}_{>0}, \cdot) \\ x & \longmapsto & \exp(x) = e^x \end{array}$$

in Abbildung 4.6 ist ein Homomorphismus, denn nach der Funktionalgleichung der Exponentialfunktion gilt $e^{x_1+x_2} = e^{x_1} \cdot e^{x_2}$ für alle $x_i \in \mathbb{R}$. Da die Exponentialfunktion stetig und streng monoton steigend ist mit $\lim_{x\mapsto\infty} e^x = \infty$ und $\lim_{x\mapsto-\infty} e^x = 0$, definiert sie sogar einen Isomorphismus.

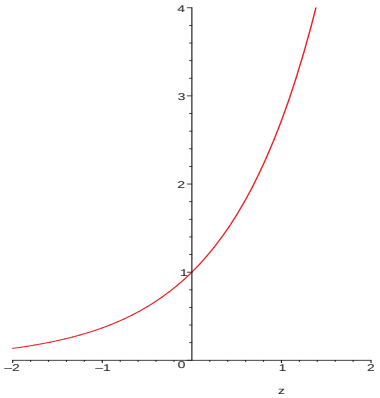


Abbildung 4.6: Exponentialfunktion

4) Im Gegensatz dazu ist mit $\mathbb{C}^* = \mathbb{C}\backslash\{0\}$ die Abbildung

$$\begin{array}{ccc} (\mathbb{C}, +) & \longrightarrow & (\mathbb{C}^*, \cdot) \\ z & \longmapsto & \exp(z) = e^z \end{array}$$

zwar ein Epimorphismus, aber kein Isomorphismus. Sie hat den Kern

$$\operatorname{Ker}(\exp : \mathbb{C} \longrightarrow \mathbb{C}^*) = 2\pi i\mathbb{Z} := \{2\pi i n \mid n \in \mathbb{Z}\}\,.$$

5) Sei $n \geq 2$. Die ***Signatur*** *oder das* ***Signum***

$$\begin{array}{rccl} \operatorname{sign}: & S_n & \longrightarrow & (\{\pm 1\}, \cdot) \\ & \sigma & \longmapsto & \operatorname{sign}(\sigma) = \prod\limits_{\substack{i,j=1 \\ i<j}}^{n} \frac{\sigma(i)-\sigma(j)}{i-j} \end{array}$$

ist ein Epimorphismus und

$$\operatorname{Ker}(\operatorname{sign}) = A_n$$

heißt die ***alternierende Gruppe****.*

Die Definition von sign *übersetzt sich in das folgende Programm (in der Syntax von* Maple*):*

```
sgn:=proc(sigma)
local s,j,i;
s:=1;
for j from 1 to nops(sigma) do
    for i from 1 to j-1 do
        s:=s*(sigma[i]-sigma[j])/(i-j);
    od;
od;
return(s);
end proc:
```

wobei wir die Permutation σ durch die Liste $(\sigma(1), \ldots, \sigma(n))$ repräsentieren.

Als Beispiel betrachten wir die Permutationen aus Abbildung 4.2. Für die Drehung

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

berechnet man mit obiger Formel, dass

$$\begin{aligned} \operatorname{sign}(\sigma) &= \frac{1-3}{1-2} \cdot \frac{1-4}{1-3} \cdot \frac{1-2}{1-4} \cdot \frac{3-4}{2-3} \cdot \frac{3-2}{2-4} \cdot \frac{4-2}{3-4} \\ &= \frac{3-2}{2-3} \cdot \frac{4-2}{2-4} = (-1)^2 = 1 \end{aligned}$$

und für die beiden Spiegelungen

$$\tau_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} \qquad \tau_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$$

dass $\operatorname{sign}(\tau_i) = -1$. *Tatsächlich gilt für jede Transposition* τ, *dass* $\operatorname{sign}(\tau) = -1$. *Dies beweisen wir in Kürze.*

Da sign *ein Gruppenhomomorphismus ist, folgt aus* $\sigma = \tau_1 \cdot \tau_2$ *direkt*

$$\operatorname{sign}(\sigma) = \operatorname{sign}(\tau_1) \cdot \operatorname{sign}(\tau_2) = 1.$$

Wie wir in Satz 4.2.34 sehen werden, lässt sich das Signum über die Homomorphismus-Eigenschaft leicht berechnen, indem man eine Permutation als ein geeignetes Produkt von Permutationen mit bekanntem Signum schreibt.

Siehe auch Übungsaufgabe 4.5.

6) Sind $a, b \in \mathbb{N}$ *und* $\operatorname{ggT}(a, b) = 1$. *Dann gilt*

$$\mathbb{Z}/ab \cong \mathbb{Z}/a \times \mathbb{Z}/b$$

Dies ist eine Umformulierung des Chinesischen Restsatzes. Zum Beweis siehe Übung 4.8.

Praktisch werden Gruppen oft durch Erzeuger gegeben:

Definition 4.2.16 *Sei* E *eine Teilmenge einer Gruppe* G. *Dann ist* $\langle E \rangle$ *die kleinste Untergruppe von* G, *die alle Elemente von* E *enthält. Äquivalent ist* $\langle E \rangle$ *der Durchschnitt aller Untergruppen* U *mit* $E \subset U \subset G$ *(denn der Durchschnitt von Untergruppen ist wiederum eine Untergruppe).*

Wir nennen $\langle E \rangle$ *die* ***von E erzeugte Untergruppe*** *von* G. *Eine Gruppe* G *heißt* ***zyklisch****, wenn es ein* $g \in G$ *gibt mit*

$$G = \langle g \rangle .$$

Für $g \in G$ ist offenbar

$$\langle g \rangle = \{ g^r \mid r \in \mathbb{Z} \}$$

mit

$$g^r = \underbrace{g \circ \ldots \circ g}_{r}$$

$g^r = (g^{-1})^{-r}$ für $r < 0$. Bei einer additiven Verknüpfung + schreiben wir intuitiver $r \cdot g$ statt g^r.

Beispiel 4.2.17 *1) Die Restklassengruppe $\mathbb{Z}/n$ wird zyklisch von $\overline{1}$ erzeugt.*

2) Die Gruppe $(\mathbb{Z}, +)$ ist zyklisch von 1 erzeugt.

3) Die Untergruppe $n\mathbb{Z} \subset (\mathbb{Z}, +)$ wird zyklisch erzeugt von n, also $n\mathbb{Z} = \langle n \rangle$. Für $n \neq 0$ gilt nach Beispiel 4.2.15, dass $n\mathbb{Z} \cong \mathbb{Z}$.

Wir werden später zeigen, dass alle zyklischen Gruppen bis auf Isomorphie von der Form $\mathbb{Z}$ oder $\mathbb{Z}/n$ sind (siehe Beispiel 4.3.14).

Definition 4.2.18 *Sei $g \in G$ ein Element einer Gruppe. Dann heißt*

$$\operatorname{ord}(g) = |\langle g \rangle|$$

*die **Ordnung** von g.*

Siehe auch Übungsaufgabe 4.9.

Beispiel 4.2.19 *Für die Drehung des Tetraeders um 120°*

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

erhalten wir

$$\langle \sigma \rangle = \left\{ \mathrm{id} = \sigma^0, \sigma^1, \sigma^2 \right\} \cong \mathbb{Z}/3$$

und somit $\operatorname{ord}(\sigma) = 3$.

4.2.2 Gruppenoperationen

Gruppen werden in der Mathematik betrachtet, da sie als Mengen von Symmetrien von Objekten auftauchen. Um Symmetriegruppen einzuführen, verwenden wir die Notation einer Operation.

Definition 4.2.20 *Sei $(G, \circ)$ eine Gruppe und M eine Menge. Eine **Operation** von G auf M (von links) ist eine Abbildung*

$$\begin{array}{rccc} \cdot : & G \times M & \longrightarrow & M \\ & (g, m) & \longmapsto & g \cdot m \end{array}$$

die folgende Bedingungen erfüllt:

1)

$$e \cdot m = m$$

für alle $m \in M$.

2)

$$(a \circ b) \cdot m = a \cdot (b \cdot m)$$

für alle $a, b \in G$ und $m \in M$.

Bemerkung 4.2.21 *Analog kann man auch Operationen von rechts*

$$\begin{array}{rccc} \cdot : & M \times G & \longrightarrow & M \\ & (m, g) & \longmapsto & m \cdot g \end{array}$$

betrachten mit $m \cdot e = m$ und $(m \cdot a) \cdot b = m \cdot (a \circ b)$.

Es scheint erst einmal überflüssig beide Notationen zu haben, jedoch gibt es Situationen, bei der es zwei unterschiedliche kanonische Definition für eine Operation gibt. Ein Beispiel ist die Operation einer Untergruppe $H \subset G$ von auf G durch $H \times G \to G$, $(h, g) \mapsto h \circ g$ von links und $G \times H \to G$, $(g, h) \mapsto g \circ h$ von rechts, auf die wir später noch ausführlich zurückkommen.

Bemerkung 4.2.22 *Anders formuliert ist eine Operation von G auf M ein Gruppenhomomorphismus*

$$\begin{array}{rccc} \varphi : & G & \longrightarrow & S(M) \\ & g & \mapsto & \varphi(g) := \left(\begin{array}{ccc} M & \longrightarrow & M \\ m & \mapsto & g \cdot m \end{array} \right) \end{array}$$

von G in die Gruppe der Selbstabbildung von M.

Beweis. Wir überprüfen, ob $\varphi(g)$ für alle $g \in G$ bijektiv und φ ein Homomorphismus ist: Sei $g \cdot m_1 = g \cdot m_2$ für $m_1, m_2 \in M$, dann folgt

$$\begin{aligned} m_1 &= e \cdot m_1 = \left(g^{-1} \circ g\right) \cdot m_1 = g^{-1} \cdot (g \cdot m_1) \\ &= g^{-1} \cdot (g \cdot m_2) = \left(g^{-1} \circ g\right) \cdot m_2 = e \cdot m_2 = m_2. \end{aligned}$$

Jedes $m \in M$ liegt im Bild von $\varphi(g)$, denn $m = e \cdot m = g \cdot (g^{-1} \cdot m)$. Weiter gilt

$$\begin{aligned} \varphi(g \circ h) &= (m \mapsto (g \circ h) \cdot m) = (m \mapsto g \cdot (h \cdot m)) \\ &= (m \mapsto g \cdot m) \circ (m \mapsto h \cdot m) = \varphi(g) \circ \varphi(h). \end{aligned}$$

■

Beispiel 4.2.23 *S_n operiert auf $\{1, ..., n\}$ durch*

$$\begin{array}{ccc} S_n \times \{1, ..., n\} & \longrightarrow & \{1, ..., n\} \\ (\sigma,\ j) & \longmapsto & \sigma(j) \end{array}$$

Ein anderes zentrales Beispiel ist die Operation der Gruppe der Bewegungen auf dem $\mathbb{R}^n$:

Definition 4.2.24 *Eine Euklidische **Bewegung** $f : \mathbb{R}^n \to \mathbb{R}^n$ ist eine Abbildung, die den Euklidischen Abstand*

$$\|x\| := \sqrt{\textstyle\sum_{i=1}^{n} x_i^2}$$

erhält, d.h. mit

$$\|x - y\| = \|f(x) - f(y)\|$$

*für alle $x, y \in \mathbb{R}^n$. Abbildung 4.7 zeigt eine Bewegung, die sich aus einer Translation und einer Drehspiegelung zusammensetzt. Die Menge $\mathrm{E}(n)$ der Euklidischen Bewegungen des $\mathbb{R}^n$ ist mit der Komposition eine Gruppe, die **Bewegungsgruppe**.*

Sei $M \subset \mathbb{R}^n$ eine Teilmenge. Die Gruppe

$$\mathrm{Sym}(M) = \{A \in \mathrm{E}(n) \mid A(M) = M\}$$

*heißt **Symmetriegruppe** von M.*

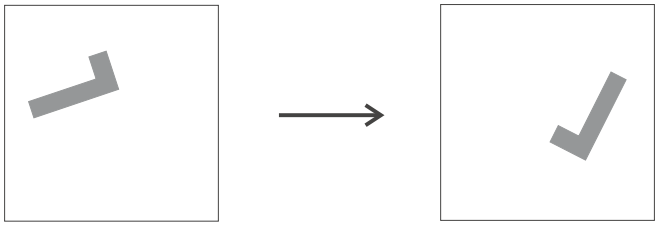
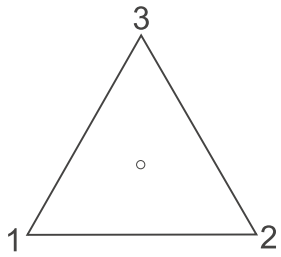
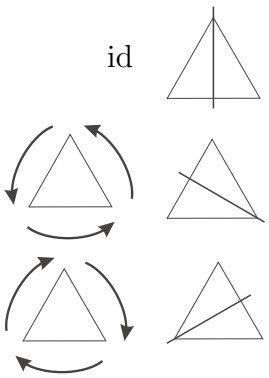


Abbildung 4.7: Beispiel einer Bewegung des $\mathbb{R}^2$.

Beispiel 4.2.25 (Symmetriegruppe) *Wir beschreiben die Symmetriegruppe* $\mathrm{Sym}\,(D)$ *des gleichseitigen Dreiecks* D*.*

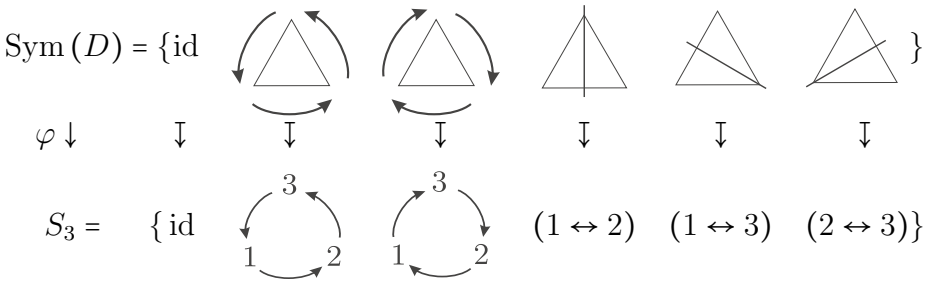


Jede Symmetrie ist eine Drehung oder Spiegelung



Jede Symmetrie ist eindeutig durch ihre Wirkung auf den Ecken festgelegt. Durch Nummerieren der Ecken können wir also jedes Element als eine bijektive Abbildung $\{1,2,3\} \to \{1,2,3\}$ *auffas-*

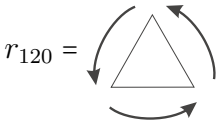
sen. Genauer haben wir einen Gruppenisomorphismus φ



Dieser wird induziert durch die Operation von $\mathrm{Sym}\,(D)$ *auf den Ecken des Dreiecks*

$$\mathrm{Sym}\,(D) \times \{1,2,3\} \longrightarrow \{1,2,3\}\,.$$

Bezeichnet etwa



die Drehung um $120°$*, dann gibt die Operation die Zuordnung*

$$(r_{120}, 1) \mapsto 2,\ (r_{120}, 2) \mapsto 3,\ (r_{120}, 3) \mapsto 1$$

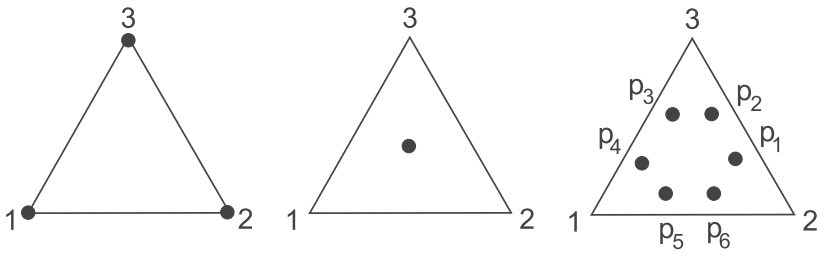
also

$$\varphi(r_{120}) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Beispiel 4.2.26 (Bahn und Stabilisator) *Gegeben ein Punkt des gleichseitigen Dreiecks* D*, wollen wir untersuchen, auf welche anderen Punkte dieser unter der Operation*

$$\mathrm{Sym}\,(D) \times D \longrightarrow D$$

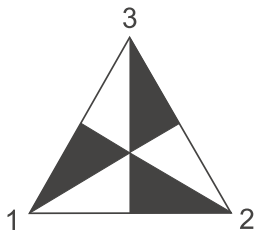
abgebildet werden kann. Diese Menge nennt man die Bahn, die Anzahl der Elemente die Länge der Bahn. Beispiele von Bahnen sind



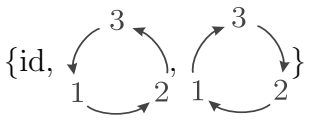
Die Operation auf D induziert eine Operation

$$\mathrm{Sym}\,(D) \times 2^D \longrightarrow 2^D$$

auf der Menge aller Teilmengen von D. In der Bahn der schwarzen Teilmenge liegt außerdem noch die weisse Teilmenge:



Andererseits kann man die Menge aller Elemente von $\mathrm{Sym}\,(D)$ *betrachten, die einen gegebenen Punkt (oder eine Teilmenge) festhalten. Die Ecke* 1 *wird festgehalten von* $\{\mathrm{id}, (2 \leftrightarrow 3)\}$*, der Mittelpunkt m von* $\mathrm{Sym}\,(D)$ *und der Punkt p_1 nur von der Identität. Die schwarze Teilmenge wird festgehalten von*



Wir beobachten, dass diese Mengen stets Untergruppen von $\mathrm{Sym}\,(D)$ *sind, und das Produkt der Gruppenordnung mit der Länge der jeweiligen Bahn stets* $|\mathrm{Sym}\,(D)| = 6$ *ergibt*

	Bahn	*festgehalten von*	
1	$\{1,2,3\}$	$\{\mathrm{id}, (2 \leftrightarrow 3)\}$	$3 \cdot 2 = 6$
m	$\{m\}$	$\mathrm{Sym}\,(D)$	$1 \cdot 6 = 6$
p_1	$\{p_1, \ldots, p_6\}$	$\{\mathrm{id}\}$	$6 \cdot 1 = 6$

Dies werden wir in Abschnitt 4.2.4 zeigen.

Zunächst formalisieren wir aber diese Ideen:

Definition 4.2.27 *Sei $G \times M \to M$ eine Operation. Für $m \in M$ nennt man*

$$Gm = \{g \cdot m \mid g \in G\} \subset M$$

die ***Bahn*** *(oder den* ***Orbit****) von m. Ist $N \subset M$ eine Teilmenge, dann heißt*

$$\mathrm{Stab}\,(N) = \{g \in G \mid gN = N\}\,,$$

wobei $gN = \{g \cdot n \mid n \in N\}$*, der* ***Stabilisator*** *der Menge* N*.*

Der wichtigste Spezialfall ist der Stabilisator einer einelementigen Menge: Für ein Elements $m \in M$ *sei*

$$\mathrm{Stab}(m) = \{g \in G \mid g \cdot m = m\} = \mathrm{Stab}(\{m\}).$$

Eines unserer zentralen Ziele ist der Beweis der Bahnformel: Für jede Gruppenoperation $G \times M \to M$ und jedes $m \in M$ gilt

$$|G| = |Gm| \cdot |\mathrm{Stab}(m)|.$$

Darauf kommen wir in Abschnitt 4.2.4 zurück.

Zunächst untersuchen wir die Struktur von Bahnen genauer:

Bemerkung 4.2.28 *Zwei Bahnen* Gm_1 *und* Gm_2 *sind entweder gleich oder disjunkt. In der gleichen Bahn zu sein ist also eine Äquivalenzrelation.*

Beweis. Existiert ein

$$m_3 \in Gm_1 \cap Gm_2$$

dann gibt es $g_1, g_2 \in G$ mit

$$m_3 = g_1 \cdot m_1 = g_2 \cdot m_2$$

also

$$m_2 = g_2^{-1} \cdot (g_1 \cdot m_1).$$

Für jedes $g \in G$ ist damit

$$g \cdot m_2 = g \cdot (g_2^{-1} \cdot (g_1 \cdot m_1)) = (g \circ g_2^{-1} \circ g_1) \cdot m_1 \in Gm_1$$

d.h.

$$Gm_2 \subset Gm_1.$$

Ebenso gilt die andere Inklusion, also ist $Gm_2 = Gm_1$.

Die zweite Aussage folgt, da jede Partition einer Menge (d.h. eine Zerlegung der Menge in eine Vereinigung von paarweise disjunkten, nichtleeren Teilmenge) eine Äquivalenzrelation definiert (indem wir zwei Elemente als äquivalent betrachten, wenn sie in der selben Partitionsteilmenge liegen). Alternativ kann man die zweite Aussage auch leicht anhand der Definition einer Äquivalenzrelation überprüfen (Übung). ■

Wollen wir die Bahnen einer Operation aufzählen, dann geben wir in jeder Bahn ein Element an, um diese Bahn zu repräsentieren:

Definition 4.2.29 *Die Menge der Bahnen bezeichnen wir mit M/G (**Quotient** von M nach G). Jedes Element $m \in Gm_1$ nennen wir einen **Repräsentanten** der Bahn, denn $Gm = Gm_1$. Weiter heißt*

$$\begin{array}{rccc} \pi: & M & \longrightarrow & M/G \\ & m & \longmapsto & Gm \end{array}$$

***Quotientenabbildung**.*

Mit obigen Bemerkungen sieht man:

Definition und Satz 4.2.30 *Sei $G \times M \to M$ eine Operation. Ein **vollständiges Repräsentantensystem** der Bahnen ist eine Teilmenge $R \subset M$, sodass jede Bahn Gm genau ein Element von R enthält.*

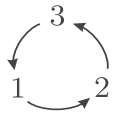
Dann ist M die disjunkte Vereinigung

$$M = \dot{\bigcup_{r \in R}} G \cdot r$$

Die Darstellung von Permutation in Abbildungsschreibweise nicht nicht effizient: Für die Permutation

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

müssen wir uns die Bilder von $4, \ldots, 7$ nicht merken. Die Bilder von $1, 2, 3$ können wir in dem Diagramm



codieren. Dies ist die Idee eines Zykels:

Definition 4.2.31 *Ist $\sigma \in S_n$, dann zerlegt die Operation von $\langle \sigma \rangle$ die Menge $\{1, \ldots, n\}$ in Bahnen der Form*

$$\langle \sigma \rangle x = \left\{ x, \sigma(x), \sigma^2(x), \ldots, \sigma^{t-1}(x) \right\}$$

*und t minimal mit $\sigma^t(x) = x$. Gibt es nur eine Bahn der Länge $t > 1$ (d.h. alle anderen haben Länge 1), dann heißt σ **Zykel** der Ordnung t, und wir schreiben*

$$\sigma = \left(x, \sigma(x), \sigma^2(x), \ldots, \sigma^{t-1}(x) \right),$$

d.h. wir codieren zusätzlich zu der Bahn als Menge noch die Reihenfolge in der die Bahn durchlaufen wird. Transpositionen sind Zykel der Länge 2. *Für das neutrale Element schreiben wir* ().

Man könnte für Zykel auch eine Kreisnotation wie oben verwenden, die würde aber zu viel Platz verbrauchen und ist auch in einer Computerkonsole schwer einzugeben.

Bemerkung 4.2.32 *Der Zykel*

$$\sigma = (a_1, \dots, a_t) \in S_n$$

ist also die Abbildung

$$\begin{aligned} \{1, \dots, n\} &\longrightarrow \{1, \dots, n\} \\ a_1 &\longmapsto a_2 \\ a_2 &\longmapsto a_3 \\ &\vdots \\ a_{t-1} &\longmapsto a_t \\ a_t &\longmapsto a_1 \\ a &\longmapsto a \quad \textit{sonst.} \end{aligned}$$

Es gilt $\operatorname{ord}(\sigma) = t$.

Beispiel 4.2.33 *Für die Drehung*

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

des Tetraeders um 120° *(siehe auch Beispiel 4.2.19) erhalten wir die Zerlegung in Bahnen*

$$\{1, 2, 3, 4\} = \{1\} \dot\cup \{2, 3, 4\}.$$

Somit ist σ *ein Zykel und unter Beachtung der Reihenfolge der Bahnelemente erhalten wir*

$$\sigma = (2, 3, 4),$$

d.h. $2 \mapsto 3$, $3 \mapsto 4$, $4 \mapsto 2$. *Zur Notation kann man den Zykel natürlich an jeder Stelle auftrennen, es ist also*

$$\sigma = (2, 3, 4) = (3, 4, 2) = (4, 2, 3).$$

Die Drehung

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$$

des Tetraeders um $240°$ *gibt dieselbe Zerlegung in Bahnen* $\{1,2,3,4\} = \{1\} \dot{\cup} \{2,3,4\}$*, allerdings ist*

$$\sigma^2 = (2,4,3).$$

Man beachte, dass sich Quadrate von σ *in der Zykelschreibweise leicht ausrechnen lassen: Man muss in der Liste nur jeweils* 2 *Schritte weitergehen, um das Bild eines Elements zu erhalten (analog für höhere Potenzen).*

Zykel sind aber nicht ausreichend, um alle Permutation darzustellen: Unter der Operation von

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 1 & 6 & 7 & 8 & 5 \end{pmatrix}$$

gibt es zwei Bahnen der Länge 4 also ist

$$\sigma = (1,2,3,4) \circ (5,6,7,8)$$

das Produkt von zwei Zykeln. Da Bahnen disjunkt sind, können wir immer in ein Produkt von elementfremden (d.h. disjunkten) Zyklen zerlegen:

Satz 4.2.34 *Es gilt:*

1) Jedes Element der S_n *ist ein Produkt elementfremder Zykel.*

2) Jedes Element der S_n *ist ein Produkt von Transpositionen.*

Beweis. Sei $\sigma \in S_n$.

1) Sei $\{x_1, ..., x_r\}$ ein vollständiges Repräsentantensystem der Bahnen der Operation von $\langle\sigma\rangle$ auf $\{1, ..., n\}$. Schränken wir σ als Abbildung auf die Bahn $\langle\sigma\rangle\, x_i$ ein, erhalten wir einen Zykel σ_i und

$$\sigma = \sigma_1 \circ ... \circ \sigma_r$$

2) Mit 1) können wir annehmen, dass σ ein Zykel $(y_0, ..., y_{t-1})$ ist. Dann gilt

$$(y_0, ..., y_{t-1}) = (y_0, y_1) \circ ... \circ (y_{t-2}, y_{t-1}) .$$

■

Das Kompositionszeichen $\circ$ lässt man in der Zykleschreibweise oft auch weg.

Beispiel 4.2.35 *Sei*

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

Die Operation von $\langle\sigma\rangle$ *zerlegt*

$$\{1, ..., 9\} = \{1, 2, 3, 4\} \dot\cup \{5, 9\} \dot\cup \{6, 8\} \dot\cup \{7\}$$

in disjunkte Bahnen und

$$\begin{aligned} \sigma &= (1, 4, 3, 2)\,(5, 9)\,(6, 8) \\ &= (1, 4)\,(4, 3)\,(3, 2)\,(5, 9)\,(6, 8) . \end{aligned}$$

Siehe auch Übungsaufgabe 4.7.

Bemerkung 4.2.36 *Ist* $\sigma = \tau_1 \circ ... \circ \tau_r$ *mit Transpositionen* τ_i, *dann können wir das Signum von* σ *sofort berechnen als*

$$\operatorname{sign}(\sigma) = (-1)^r,$$

denn sign *ist ein Gruppenhomomorphismus und* $\operatorname{sign}\tau = -1$ *für jede Transposition* τ.

Beweis. Wir berechnen

$$\operatorname{sign}(\tau) = \prod_{i<j} \frac{\tau(i) - \tau(j)}{i - j}.$$

Angenommen $\tau = (k, l)$ und $k < l$. Dann ist

$$\frac{\tau(i) - \tau(j)}{i - j} = \begin{cases} -1 & \text{für } i = k \text{ und } j = l \\ 1 & \text{für } i, j \notin \{k, l\} \\ \frac{\tau(i) - j}{i - j} & \text{für } i \in \{k, l\} \text{ und } j \neq l \\ \frac{i - \tau(j)}{i - j} & \text{für } i \neq k \text{ und } j \in \{k, l\}. \end{cases}$$

Wenn wir von den letzten beiden Fällen noch die Fälle $i = k < j < l$ bzw. $k < i < j = l$ abspalten, erhalten wir

$$\operatorname{sign}(\tau) = -\underbrace{\prod_{\substack{i=k,l \\ j \text{ mit} \\ l<j}} \frac{\tau(i)-j}{i-j}}_{>0} \cdot \underbrace{\prod_{\substack{j \text{ mit} \\ k<j<l}} \frac{l-j}{k-j} \cdot \prod_{\substack{i \text{ mit} \\ k<i<l}} \frac{i-k}{i-l}}_{1} \cdot \underbrace{\prod_{\substack{j=k,l \\ i \text{ mit} \\ i<k}} \frac{i-\tau(j)}{i-j}}_{>0}.$$

Die beiden mittleren Produkte kürzen sich weg, und alle Zähler und Nenner des ersten und letzten Produktes sind negativ. Somit ist $\operatorname{sign}\tau < 0$ also $\operatorname{sign}\tau = -1$. ■

Beispiel 4.2.37 *Für*

$$\begin{aligned}\sigma &= (1,4,3,2)\,(5,9)\,(6,8)\\ &= (1,4)\,(4,3)\,(3,2)\,(5,9)\,(6,8)\end{aligned}$$

erhalten wir

$$\operatorname{sign}(\sigma) = (-1)^5 = -1.$$

Bemerkung 4.2.38 *Aus der Darstellung einer Permutation $\sigma = c_1 \circ \ldots \circ c_r$ als Produkt disjunkter Zykel c_i der Länge m_i lässt sich die Ordnung von σ bestimmen als*

$$\operatorname{ord}(\sigma) = \operatorname{kgV}(m_1, \ldots, m_r).$$

Für den Beweis siehe Übungsaufgabe 4.9.

Beispiel 4.2.39 *Für $\sigma = (1,4,3,2)\,(5,9)\,(6,8)$ erhalten wir*

$$\operatorname{ord}(\sigma) = \operatorname{kgV}(4,2,2) = 4.$$

Wir können dies auch direkt nachrechnen

$$\begin{aligned}\sigma^2 &= (1,4,3,2)^2(5,9)^2(6,8)^2 = (1,3)(2,4)\\ \sigma^3 &= (1,2,3,4)(5,9)(6,8)\\ \sigma^4 &= \mathrm{id}\,.\end{aligned}$$

Für Untergruppen der S_n implementiert das Computeralgebrasystem GAP, siehe [13], Algorithmen zur Berechnung im Wesentlichen aller in diesem Kapitel eingeführten Objekte.

Beispiel 4.2.40 *Wir bestimmen* $\mathrm{ord}(\sigma)$ *für*

$$\sigma = (1,4,3,2)\,(5,9)\,(6,8)$$

mit Hilfe von GAP*:*

```
sigma:=(1,4,3,2)(5,9)(6,8);
(1,4,3,2)(5,9)(6,8)
sigma^2;
(1,3)(2,4)
sigma^3;
(1,2,3,4)(5,9)(6,8)
sigma^4;
()
```

Somit gilt $\mathrm{ord}(\sigma) = 4$*. Dies berechnet* GAP *auch (mittels Bemerkung 4.2.38) durch:*

```
Order(sigma);
4
```

Man beachte, dass man, abweichend von der üblichen Konvention, zur Berechnung von $\sigma \circ \tau$ *für* $\sigma, \tau \in S_n$ *in* GAP $\tau * \sigma$ *eingeben muss (d.h. Abbildungen nehmen ihr Argument auf der linken Seite). Wir überprüfen in* GAP*, dass mit* $\tau = (2,5)$ *gilt*

$$\begin{aligned}\sigma \circ \tau &= (1,4,3,2)\,(5,9)\,(6,8) \circ (2,5)\\ &= (1,4,3,2,9,5)(6,8).\end{aligned}$$

```
tau:=(2,5);;
tau*sigma;
(1,4,3,2,9,5)(6,8)
```

Bemerkung 4.2.41 *Die symmetrische Gruppe* S_3 *wird von* $(1,2)$ *und* $(2,3)$ *erzeugt*

$$S_3 = \langle (1,2), (2,3) \rangle$$

denn $(1,2)\,(2,3) = (1,2,3)$ *und* $(1,2)\,(2,3)\,(1,2) = (1,3)$*. Allgemein gilt*

$$S_n = \langle (1,2), (2,3), ..., (n-1,n) \rangle,$$

siehe auch die Übungsaufgaben 4.21 und 4.22.

Beispiel 4.2.42 *In* GAP *können wir eine Gruppe ein Erzeugnis wie folgt definieren:*

```
G:=Group((1,2),(2,3));
```
$Group([(1,2),(2,3)])$
```
Elements(G);
```
$[(),(2,3),(1,2),(1,2,3),(1,3,2),(1,3)]$

4.2.3 Operation durch Translation

Bisher haben wir als Gruppenoperationen die Operation von $\mathrm{Sym}(M)$ auf einer Menge M und von S_n auf $\{1,...,n\}$ betrachtet. Ein weiteres wichtiges Beispiel ist die Operation einer Gruppe $(G,\circ)$ auf sich selbst

$$\begin{aligned} G \times G &\longrightarrow G \\ (g,h) &\mapsto g \circ h \end{aligned}$$

gegeben durch die Verknüpfung (dies ist eine Operation sowohl von links als auch von rechts). Sie spielt die entscheidende Rolle im Beweis des folgenden Satzes, der eine zentrale Bedeutung für das praktische Rechnen mit Gruppen hat: Er erlaubt es, jede endliche Gruppe als Untergruppe einer S_n aufzufassen. In dieser Darstellung können wir die Gruppe dann im Computer handhaben.

Satz 4.2.43 (Cayley) *Jede Gruppe G ist isomorph zu einer Untergruppe der Gruppe der Selbstabbildungen $S(G)$.*

Insbesondere für $n := |G| < \infty$ können wir G als Untergruppe von $S_n \cong S(G)$ auffassen.

Beweis. Die Abbildung

$$\begin{array}{rccc} \varphi: & G & \to & S(G) \\ & g & \mapsto & \begin{pmatrix} G & \to & G \\ h & \mapsto & g \circ h \end{pmatrix} \end{array}$$

ist ein Gruppenhomomorphismus und

$$\mathrm{Ker}\,\varphi = \{g \in G \mid g \circ h = h \ \forall h \in G\} = \{e\}$$

(mit der Eindeutigkeit des neutralen Elements) also φ injektiv. Somit gilt

$$G \cong \mathrm{Bild}(\varphi) \subset S(G).$$

■

Für endliche Gruppen kann man die Verknüpfung

$$\begin{aligned} G \times G &\longrightarrow G \\ (g,h) &\mapsto g \circ h \end{aligned}$$

mittels einer Tabelle angeben

	g_1	g_2	...
g_1	$g_1 \circ g_1$	$g_1 \circ g_2$	...
g_2	$g_2 \circ g_1$	$g_2 \circ g_2$	...
$\vdots$	$\vdots$	$\vdots$	

der **Verknüpfungstafel** oder **Gruppentafel**, wie wir sie schon in Beispiel 4.2.9 kennengerlernt haben.

Beispiel 4.2.44 *Die Gruppe*

$$G = \mathbb{Z}/4 = \left\{\overline{0}, \overline{1}, \overline{2}, \overline{3}\right\}$$

hat die Verknüpfungstafel

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

In jeder Zeile und Spalte steht jedes Element genau einmal.

Die Zeilen der Verknüpfungstafel spezifizieren $\varphi(g)$, in dem Beispiel ist also

$$\varphi(\overline{0}) = \begin{pmatrix} \overline{0} & \overline{1} & \overline{2} & \overline{3} \\ \overline{0} & \overline{1} & \overline{2} & \overline{3} \end{pmatrix}$$

$$\varphi(\overline{1}) = \begin{pmatrix} \overline{0} & \overline{1} & \overline{2} & \overline{3} \\ \overline{1} & \overline{2} & \overline{3} & \overline{0} \end{pmatrix}$$

$$\varphi(\overline{2}) = \begin{pmatrix} \overline{0} & \overline{1} & \overline{2} & \overline{3} \\ \overline{2} & \overline{3} & \overline{0} & \overline{1} \end{pmatrix}$$

$$\varphi(\overline{3}) = \begin{pmatrix} \overline{0} & \overline{1} & \overline{2} & \overline{3} \\ \overline{3} & \overline{0} & \overline{1} & \overline{2} \end{pmatrix}$$

wobei wir die Abbildungschreibweise analog zu Elementen der S_n auch für Elemente der $S(G)$ verwenden.

Wir können dann noch durch Durchnummerieren der Elemente von G die Identifikation $S(G) \cong S_4$ vornehmen.

Eine Gruppe ist abelsch genau dann, wenn ihre Verknüpfungstafel bezüglich der Diagonalen symmetrisch ist. Das Assoziativgesetz lässt sich der Tabelle nicht unmittelbar ansehen.

Analog zur Operation einer Gruppe auf sich selbst kann man auch die Operation einer Untergruppe betrachten:

Beispiel 4.2.45 *Wie in Beispiel 4.2.7 gezeigt, sind die Untergruppen von $(\mathbb{Z}, +)$ von der Form*

$$n\mathbb{Z} = \{n \cdot k \mid k \in \mathbb{Z}\} .$$

Eine Gruppenoperation von $n\mathbb{Z}$ auf $\mathbb{Z}$ (von rechts) ist gegeben durch

$$\begin{aligned} \mathbb{Z} \times n\mathbb{Z} &\to \mathbb{Z} \\ (a, n \cdot k) &\mapsto a + n \cdot k \end{aligned}$$

Die Bahnen sind genau die Restklassen modulo n

$$\overline{a} = a + n\mathbb{Z} = \{a + n \cdot k \mid k \in \mathbb{Z}\} .$$

Analog könnten wir von links durch Addition operieren und erhalten dieselben Bahnen, da $+$ kommutativ ist. Aufgrund der üblichen Notation $a + n\mathbb{Z}$ für Restklassen bevorzugt man aber die Schreibweise von rechts.

Für $n = 4$ erhalten wir z.B. durch die Operation von $4\mathbb{Z}$ auf $\mathbb{Z}$ die Bahnen

$4\mathbb{Z}$	$1 + 4\mathbb{Z}$	$2 + 4\mathbb{Z}$	$3 + 4\mathbb{Z}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
-4	-3	-2	-1
0	1	2	3
4	5	6	7
$\vdots$	$\vdots$	$\vdots$	$\vdots$

Wir haben in Beispiel 4.2.8 schon gesehen, dass die Menge dieser Bahnen mit der Addition

$$\overline{a} + \overline{b} = (a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a + b) + n\mathbb{Z} = \overline{a + b}$$

wieder eine Gruppe $\mathbb{Z}/n$ ist.

Später werden wir allgemein untersuchen, wann eine Menge von Bahnen einer Untergruppe wieder eine Gruppe bildet.

Zunächst formulieren wir dieses Konzept allgemein:

Definition 4.2.46 (Nebenklassen) *Sei $H \subset G$ eine Untergruppe. Dann definiert die Verknüpfung in G eine Operation von H auf G*

$$H \times G \longrightarrow G,\ (h, g) \longmapsto h \circ g$$

von links, und ebenso eine von rechts

$$G \times H \longrightarrow G,\ (g, h) \longmapsto g \circ h.$$

Für $g \in G$ heißen die Bahnen dieser Operation

$$Hg := H \circ g := \{h \circ g \mid h \in H\}$$

bzw.

$$gH := g \circ H := \{g \circ h \mid h \in H\}$$

*rechte bzw. linke **Nebenklassen** von g.*

Eines unserer wesentlichen Ziele wird (in Abschnitt 4.3) sein, der Menge der Nebenklassen G/H eine Gruppenstruktur zu geben. Soll man hier rechte oder linke Nebenklassen nehmen? Analog zu der Definition von $\mathbb{Z}/n$ ist die repräsentantenweise Verknüpfung

$$g_1H \circ g_2H = (g_1 \circ g_2)H$$

die einzig sinnvolle Art die Verknüfpung zu definieren. Wie wir sehen werden, ist dies aber genau dann wohldefiniert, wenn

$$gH = Hg \text{ für alle } g \in G$$

gilt, also die rechten mit den linken Nebenklassen übereinstimmen. Die Frage nach der Wahl von rechten oder linken Nebenklassen stellt sich also nicht. Eine Untergruppe mit $gH = Hg$ für alle $g \in G$ nennen wir einen Normalteiler von G.

Satz 4.2.47 *Sei $H \subset G$ eine Untergruppe. Je zwei Nebenklassen von H haben gleich viele Elemente.*

Beweis. Seien $a, b \in G$. Dann stehen aH und bH in Bijektion zueinander durch Multiplikation mit ba^{-1} von links

$$\begin{array}{ccc} g & \longmapsto & b \circ a^{-1} \circ g \\ G & \overset{1:1}{\longrightarrow} & G \\ \cup & & \cup \\ aH & \longrightarrow & bH \\ a \circ h & \longmapsto & b \circ a^{-1} \circ a \circ h = b \circ h \end{array}$$

(was ist die Umkehrabbildung?). Die rechten und linken Nebenklassen aH und Ha stehen in Bijektion vermöge **Konjugation** mit a

$$\begin{array}{ccc} g & \longmapsto & a^{-1} \circ g \circ a \\ G & \overset{1:1}{\longrightarrow} & G \\ \cup & & \cup \\ aH & \longrightarrow & Ha \\ a \circ h & \longmapsto & a^{-1} \circ a \circ h \circ a = h \circ a \end{array}$$

(was ist die Umkehrabbildung?). Die Operation durch Konjugation diskutieren wir auch in Aufgabe 4.12. ■

Corollar 4.2.48 (Indexformel) *Sei $H \subset G$ eine Untergruppe. Es gilt*

$$|G| = |G/H| \cdot |H|$$

insbesondere in einer endlichen Gruppe teilt $|H|$ die Gruppenordnung $|G|$.

Definition 4.2.49 *Ist $H \subset G$ eine Untergruppe, so heißt*

$$[G : H] := |G/H|$$

***Index** von H in G.*

Wir bemerken zunächst, dass

$$\begin{aligned} H &\to aH \\ h &\mapsto a \circ h \end{aligned}$$

eine Bijektion ist (siehe den Beweis von Satz 4.2.47), also

$$|aH| = |H| .$$

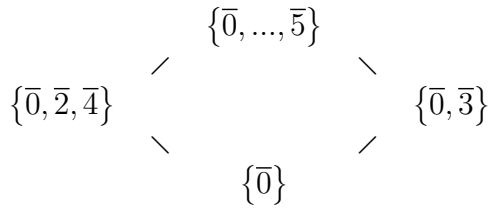
Wir beweisen nun die Indexformel:

Beweis. Nach Definition und Satz 4.2.30 ist G die disjunkte Vereinigung aller aH mit a aus einem vollständigen Repräsentantensystem R, also falls $|G| < \infty$ gilt

$$|G| = \sum_{a \in R} |aH| = |R| \cdot |H|$$

(mit Satz 4.2.47). Ist $|G| = \infty$, dann auch $|G/H| = \infty$ oder $|H| = \infty$. ■

Beispiel 4.2.50 *Die Gruppe* $G = \mathbb{Z}/6$ *der Ordnung* 6 *hat die Untergruppen*



mit den Ordnungen $1, 2, 3$ *und* 6.

Bemerkung 4.2.51 *Man beachte, dass es in einer Gruppe nicht zu jedem Teiler eine Untergruppe geben muss, z.B. hat die* $A_4 = \{\sigma \in S_4 \mid \text{sign}(\sigma) = 1\}$ *keine Untergruppe der Ordnung* 6. *Der folgende* GAP*-Code berechnet alle möglichen Ordnungen von Untergruppen der* A_4*:*

```
G:=AlternatingGroup(4);;
Order(G);
12
L:=ConjugacyClassesSubgroups(G);;
List(List(L,Representative),Size);
[ 1, 2, 3, 4, 12 ]
```

Im Kontext der sogenannten Sylowsätze kann man zeigen, dass es zu jedem Primpotenzteiler von $|G|$ *eine Untergruppe gibt.*

Aus der Indexformel (Satz 4.2.48) erhalten wir mit $H = \langle g \rangle$:

Corollar 4.2.52 *In einer endlichen Gruppe* G *ist die Ordnung eines Elements* $g \in G$ *ein Teiler der Gruppenordnung* $|G|$*, d.h.* $\text{ord}(g) \mid |G|$.

Beispiel 4.2.53 *In* $G = \mathbb{Z}/6$ *habe* $\overline{1}$ *und* $\overline{5} = \overline{-1}$ *die Ordnung* 6, *die Elemente* $\overline{2}$ *und* $\overline{4}$ *haben Ordnung* 3, *und das Element* $\overline{3}$ *hat Ordnung* 2. *Das Neutrale Element* $\overline{0}$ *hat Ordnung* 1.

Corollar 4.2.54 *Jede Gruppe* G *mit* $|G|$ *prim ist zyklisch.*

Beweis. Aus der Indexformel erhalten wir, dass G nur die Untergruppen $\{e\}$ und G besitzt. Somit ist für jedes $e \neq g \in G$ schon

$$\{e\} \neq \langle g \rangle = G$$

■

4.2.4 Bahnengleichung

Wir betrachten nun wieder die Operation einer Gruppe G auf einer Menge M und fragen nach der Beziehung zwischen der Bahn eines Elements $m \in M$ und dem Stabilisator von m.

Satz 4.2.55 *Sei*

$$G \times M \longrightarrow M$$

eine Operation, $m \in M$ *und*

$$H := \mathrm{Stab}\,(m)\,.$$

Dann gibt es eine natürliche Bijektion

$$\begin{array}{ccc} G/H & \longrightarrow & Gm \\ gH & \longmapsto & g \cdot m \end{array}$$

Beweis. Die Abbildung ist wohldefiniert: Ist $gH = g'H$, dann $g' \in gH$, also $g' = g \circ h$ mit $h \in H$. Es folgt

$$g' \cdot m = g \cdot (h \cdot m) = g \cdot m,$$

da m von h stabilisiert wird. Die Abbildung ist offenbar surjektiv. Sie ist auch injektiv, denn

$$g_1 \cdot m = g_2 \cdot m \Rightarrow (g_1^{-1} \circ g_2) \cdot m = m \Rightarrow g_1^{-1} \circ g_2 \in H \Rightarrow$$
$$g_2 = g_1 \circ (g_1^{-1} \circ g_2) \in g_1 H \Rightarrow g_1 H = g_2 H.$$

■

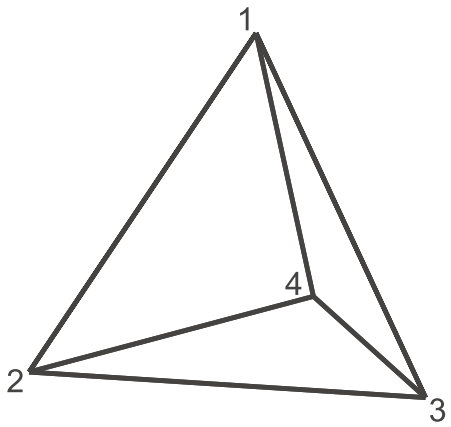


Abbildung 4.8: Tetraeder

Corollar 4.2.56 (Bahnformel) *Sei $G \times M \longrightarrow M$ eine Operation und $m \in M$. Dann gilt*

$$|Gm| \cdot |\mathrm{Stab}\,(m)| = |G|\,.$$

Beweis. Es ist

$$|Gm| = |G/H|$$

mit Satz 4.2.55 und

$$|G/H| \cdot |H| = |G|$$

nach der Indexformel 4.2.48. ■

Beispiel 4.2.57 (Symmetriegruppe des Tetraeders) *Sei T ein regulärer Tetraeder mit den Ecken $1, ..., 4$ wie in Abbildung 4.8. Die Symmetrien von T sind durch ihre Wirkung auf den Ecken eindeutig bestimmt. Wir können also die Symmetriegruppe* $\mathrm{Sym}\,(T)$ *von T als Untergruppe von S_4 auffassen.*

Die Spiegelung an der Ebene, aufgespannt durch eine Kante und den Mittelpunkt der gegenüberliegenden Seite, entspricht einer Transposition, z.B. die Spiegelung an der in Abbildung 4.9 eingezeichneten Ebene entspricht $(2, 3)$. Da die S_4 von den Transpositionen erzeugt wird, folgt:

$$\mathrm{Sym}\,(T) \cong S_4.$$

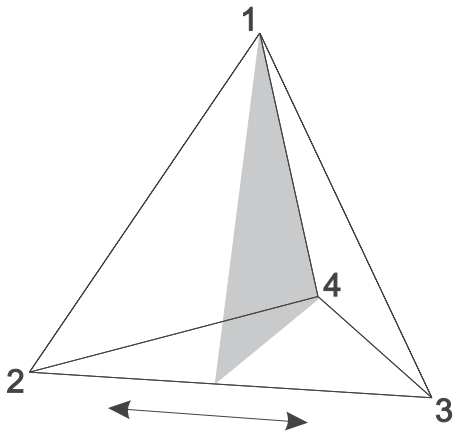


Abbildung 4.9: Spiegelsymmetrie $(2,3)$ des Tetraeders

Beispiel 4.2.58 (Bahnen und Stabilisatoren) *Für die Operation von $G = S_4$ auf dem Tetraeder T mit Mittelpunkt 0 durch Permutation der Vertices von T betrachten wir die Bahnen Gm für die Punkte $m \in T$, die in Abbildung 4.10 markiert sind:*

Bahnen Gm	$\lvert Gm\rvert$	*Stabilisatoren* $\mathrm{Stab}(m)$	$\lvert\mathrm{Stab}(m)\rvert$
$G1 = \{1,2,3,4\}$	4	S_3	6
Gm_{12} $= \{m_{12},\dots,m_{34}\}$	6	$\mathrm{Stab}(m_{12})$ $= \{e,(12),(34),(12)(34)\}$ $\cong \mathbb{Z}_2 \times \mathbb{Z}_2$	4
Gp	24	$\mathrm{Stab}(p) = \{e\}$	1
$G0 = \{0\}$	1	$\mathrm{Stab}(0) = S_4$	24

Wir bemerken, dass stets $\lvert Gm\rvert \cdot \lvert\mathrm{Stab}(m)\rvert = \lvert G\rvert$.

Bemerkung 4.2.59 *Umgekehrt kann man die Ordnung der Symmetriegruppe bestimmen mittels der Formel*

$$\lvert G\rvert = \lvert Gm\rvert \cdot \lvert\mathrm{Stab}(m)\rvert$$

bestimmen, falls für einen Punkt m sowohl Länge der Bahn als auch Ordnung des Stabilisators bekannt ist. Dazu wählen wir den Punkt m so, dass er auf keiner Drehachse oder Spiegelebene liegt.

Für den Tetraeder können wir etwa $m = p$ wie in Abbildung 4.10 wählen.

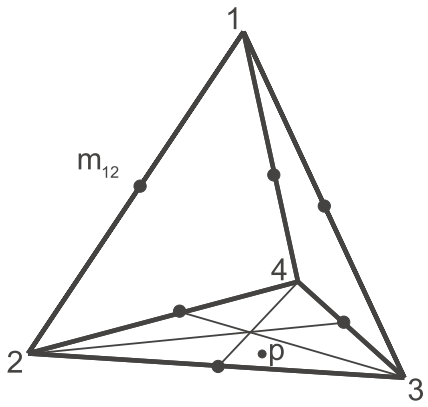


Abbildung 4.10: Bahnen von Punkten des Tetraeders

Satz 4.2.60 (Bahnengleichung) *Sei $R \subset M$ ein vollständiges Repräsentantensystem der Bahnen einer Operation $G \times M \to M$. Dann gilt*

$$|M| = \sum_{r \in R} \frac{|G|}{|\mathrm{Stab}\,(r)|}$$

Beweis. M ist nach Definition und Satz 4.2.30 die disjunkte Vereinigung

$$M = \bigcup_{r \in R} G \cdot r$$

also

$$|M| = \sum_{r \in R} |G \cdot r| = \sum_{r \in R} \frac{|G|}{|\mathrm{Stab}\,(r)|}.$$

■

Beispiel 4.2.61 *Die Permutation*

$$\begin{aligned} \sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 1 & 2 & 3 & 9 & 7 & 6 & 5 & 8 & 10 \end{pmatrix} \\ &= (1,4,3,2)\,(5,9,8)\,(6,7) \end{aligned}$$

erzeugt eine zyklische Gruppe

$$G = \langle \sigma \rangle = \left\{ \mathrm{id}, \sigma, \sigma^2, ..., , \sigma^{11} \right\}$$

der Ordnung $12 = \mathrm{kgV}(4,3,2)$ *(siehe Aufgabe 4.9 zur Berechnung der Ordnung). Die Operation von* $\langle\sigma\rangle$ *zerlegt*

$$\{1,...,10\} = \{1,2,3,4\} \dot\cup \{5,8,9\} \dot\cup \{6,7\} \dot\cup \{10\}$$

in Bahnen. Also gilt die Bahnengleichung

$$\begin{aligned} 10 &= 4+3+2+1 \\ &= \frac{12}{3}+\frac{12}{4}+\frac{12}{6}+\frac{12}{12} \end{aligned}$$

mit

$$\begin{aligned} \mathrm{Stab}(1) &= \left\{\mathrm{id}, \sigma^4, \sigma^8\right\} \\ \mathrm{Stab}(5) &= \left\{\mathrm{id}, \sigma^3, \sigma^6, \sigma^9\right\} \\ \mathrm{Stab}(6) &= \left\{\mathrm{id}, \sigma^2, \sigma^4, \sigma^6, \sigma^8, \sigma^{10}\right\} \\ \mathrm{Stab}(10) &= \left\{\mathrm{id}, \sigma^1, \sigma^2, ..., \sigma^{11}\right\} = G, \end{aligned}$$

wobei wir das vollständige Repräsentantensystem $R = \{1,5,6,10\}$ *gewählt haben.*

Eine weitere Anwendung ist die Klassifikation von Graphen bis auf Isomorphie:

4.2.5 Anwendung: Aufzählen von Graphen

Definition 4.2.62 *Ein* ***Graph*** *(ungerichtet und ohne Mehrfachkanten) ist ein Tupel* (V,E) *aus einer Menge* V *und einer Teilmenge* $E \subset \binom{V}{2}$*. Dabei bezeichnet* $\binom{V}{2}$ *die Menge der zweielementigen Teilmengen von* V*, und* V *heißt Menge der* ***Vertices*** *(oder Knoten oder Ecken) und* E *Menge der* ***Kanten*** *(oder Edges) des Graphen.*

Beispiel 4.2.63 *Durch* $V = \{1,2,3\}$ *und* $E = \{\{1,2\},\{2,3\}\}$ *ist der Graph* $\Gamma = (V,E)$ *in Abbildung 4.11 gegeben.*

Bemerkung 4.2.64 *Es gibt offenbar genau* $2^{\binom{n}{2}}$ *Graphen auf* n *Vertices (Übung).*

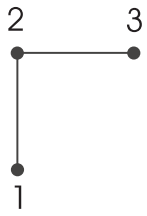


Abbildung 4.11: Graph

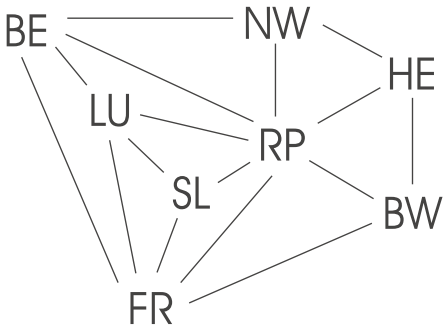


Abbildung 4.12: Nachbarschaftsverhältnisse

Beispiel 4.2.65 *Graphen haben Anwendungen z.B. in der Routenplanung (kürzester Weg/Rundweg), Erstellung von Fahrplänen, Analyse von Netzwerken (Leitungsnetz, Internet) und bei der Planung von Arbeitsschritten (out-of-order execution). Der Graph in Abbildung 4.12 zeigt die Nachbarschaftsverhältnisse von Rheinland-Pfalz und seinen Nachbarn.*

Oft will man Graphen, die durch Umnummerieren der Vertices auseinander hervorgehen, gleich behandeln:

Definition 4.2.66 *Zwei Graphen (V_1, E_1) und (V_2, E_2) heißen* ***isomorph****, wenn eine bijektive Abbildung $\varphi : V_1 \to V_2$ existiert, sodass*

$$\{v, w\} \in E_1 \iff \{\varphi(v), \varphi(w)\} \in E_2$$

für alle $v, w \in V_1$.

Bemerkung 4.2.67 *Isomorphie von Graphen ist eine Äquivalenzrelation (Übung). Die S_n operiert auf der Menge aller Graphen durch Anwenden von $\sigma \in S_n$ auf die Vertices der Kanten.*

Beispiel 4.2.68 *Die beiden Graphen in Abbildung 4.13 sind isomorph durch* $\varphi = (2,3) \in S_3$*, denn* φ *bildet die Kante* $\{2,3\}$ *auf sich selbst ab, und die Kante* $\{1,2\}$ *auf* $\{1,3\}$*.*

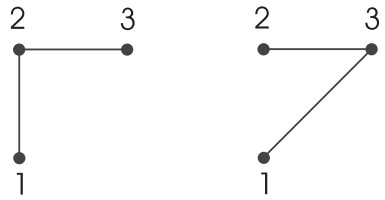
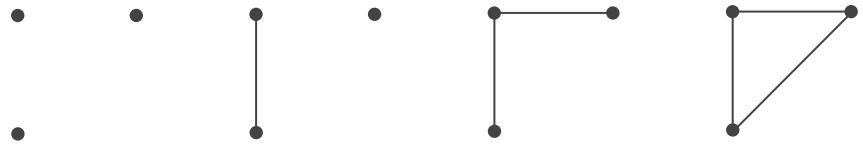


Abbildung 4.13: Isomorphe Graphen

Satz 4.2.69 *Es gibt genau* 4 *Isomorphieklassen von Graphen mit* 3 *Ecken.*

Beweis. Die Graphen



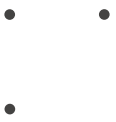
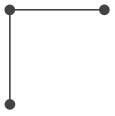
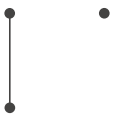
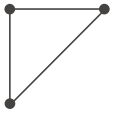
sind offenbar paarweise nicht isomorph. Wir zeigen, dass sie ein vollständiges Repräsentantensystem der Graphen mit 3 Vertices bilden: Sei

$$V = \{1,2,3\}$$

und sei M die Menge der Graphen mit Vertexmenge V, also

$$|M| = 2^{\binom{3}{2}} = 2^3 = 8.$$

Die Gruppe $G = S_3$ operiert auf M durch Permutation der Vertices. Wir geben für jeden der obigen Graphen m den Isomorphietyp des Stabilisators und mit Hilfe der Bahnenformel die Länge der Bahn an:

	m	Stab(m)	$\lvert Gm\rvert$		r	Stab(m)	$\lvert Gm\rvert$
1		S_3	1	3		$\mathbb{Z}/2$	3
2		$\mathbb{Z}/2$	3	4		S_3	1

Alle Bahnen zusammen haben also tatsächlich

$$8 = 1 + 3 + 3 + 1$$

Elemente. Somit bilden die vier angegebenen Graphen ein vollständiges Repräsentantensystem der Bahnen der Operation von G auf M. Weiter sind die Bahnen genau die Isomorphieklassen. ■

Siehe auch Übungsaufgabe 4.15.

4.3 Normalteiler

4.3.1 Normalteiler und Quotientengruppe

Sei H eine Untergruppe von $(G, \circ)$ und

$$G/H = \{gH \mid g \in G\}$$

die Menge der linken Nebenklassen

$$gH = \{g \circ h \mid h \in H\}$$

von H, d.h. die Menge der Bahnen der Translationsoperation $G \times H \to G$, $(g, h) \mapsto g \circ h$ von H auf G.

Beispiel 4.3.1 *Für $H = n\mathbb{Z} \subset \mathbb{Z} = G$ haben wir schon gesehen, dass die Menge*

$$G/H = \mathbb{Z}/n = \{\overline{0}, \ldots, \overline{n-1}\}$$

der Nebenklassen

$$\overline{a} = a + n\mathbb{Z}$$

mit der von der Addition in $\mathbb{Z}$ induzierten Verknüpfung

$$\overline{a} + \overline{b} := \overline{a + b}$$

zu einer Gruppe wird.

Ist es allgemein der Fall, dass G/H mit der von G induzierten Verknüpfung

$$aH \cdot bH := (a \circ b)H$$

zu einer Gruppe wird? Wie im Fall von $\mathbb{Z}/n$ liegt das Problem in der Wohldefiniertheit der Verknüpfung, d.h. der Unabhängigkeit von der Wahl der Repräsentanten a, b der Nebenklassen aH und bH.

Beispiel 4.3.2 *Wir betrachten nochmals die entspechende Rechnung für $\mathbb{Z}/n$: Sei $\overline{a_1} = \overline{a_2}$ und $\overline{b_1} = \overline{b_2}$, also $a_1 = a_2 + k \cdot n$ und $b_1 = b_2 + l \cdot n$, so gilt*

$$a_1 + b_1 = a_2 + k \cdot n + b_2 + l \cdot n = a_2 + b_2 + (k + l) \cdot n,$$

also $\overline{a_1 + b_1} = \overline{a_2 + b_2}$. Wir haben hier $k \cdot n$ und b_2 vertauscht. Dies war nur möglich, da $G = \mathbb{Z}$ abelsch ist.

Nun zum allgemeinen Fall. Ist G/H mit $aH \cdot bH = (a \circ b)H$ eine Gruppe, dann ist die Quotientenabbildung

$$\pi : G \longrightarrow G/H,\ g \longmapsto gH$$

ein Gruppenhomomorphismus, denn für alle $a, b \in G$ gilt

$$\pi(a) \cdot \pi(b) = aH \cdot bH = (a \circ b)H = \pi(a \circ b).$$

Dann ist

$$\pi(e) = eH = H \in G/H$$

das neutrale Element und somit $H = \mathrm{Ker}(\pi)$. Für den Kern eines Gruppenhomomorphismus beobachten wir allgemein:

Bemerkung 4.3.3 *Sei*

$$\varphi : G \longrightarrow F$$

ein Gruppenhomomorphismus und

$$H = \mathrm{Ker}(\varphi) \subset G.$$

Dann gilt für $g \in G$ und

$$gHg^{-1} := \left\{ g \circ h \circ g^{-1} \mid h \in H \right\},$$

dass

$$gHg^{-1} = H.$$

Beweis. Ist $h \in \operatorname{Ker}\varphi$, dann gilt für jedes $g \in G$

$$\varphi\left(g \circ h \circ g^{-1}\right) = \varphi(g) \circ \varphi(h) \circ \varphi(g)^{-1} = \varphi(g) \circ \varphi(g)^{-1} = e,$$

also $g \circ h \circ g^{-1} \in H$ und somit

$$gHg^{-1} \subset H.$$

Ersetzen wir g durch g^{-1}, so erhalten wir die andere Inklusion. ■

Untergruppen, die diese Eigenschaft des Kerns haben, nennt man Normalteiler:

Definition 4.3.4 *Sei $H \subset G$ eine Untergruppe. H heißt **Normalteiler** von G (in Zeichen $H \lhd G$), wenn*

$$gHg^{-1} = H \text{ für alle } g \in G$$

(äquivalent ist $gH = Hg$ für alle $g \in G$ oder $gHg^{-1} \subset H$ für alle $g \in G$).

Allgemeiner als das obige Beispiel gilt:

Bemerkung 4.3.5 *Ist $\varphi : G \longrightarrow F$ ein Gruppenhomomorphismus und $M \subset F$ ein Normalteiler, dann ist $\varphi^{-1}(M) \subset G$ ein Normalteiler. Ist φ surjektiv und $N \subset G$ ein Normalteiler, dann ist $\varphi(N) \subset F$ ein Normalteiler.*

Dies zeigen wir in Übungsaufgabe 4.17.

Satz 4.3.6 *Sei $H \subset G$ eine Untergruppe. Die Menge G/H ist genau dann mit der von G induzierten Verknüpfung*

$$aH \cdot bH = (a \circ b)H$$

*eine Gruppe, wenn H ein Normalteiler ist. Wir bezeichnen dann G/H als die **Quotientengruppe**.*

Beweis. Die Notwendigkeit, dass H Normalteiler ist, haben wir schon gezeigt. Die Bedingung ist auch hinreichend: Sei $H \subset G$ Normalteiler. Wir zeigen, dass

$$aH \cdot bH = (a \circ b)H$$

eine wohldefinierte Verknüpfung definiert, d.h. gegeben andere Repräsentanten

$$a_2 \in a_1 H \qquad b_2 \in b_1 H$$

müssen wir zeigen, dass

$$(a_2 \circ b_2)H = (a_1 \circ b_1)H.$$

Schreibe

$$a_2 = a_1 \circ h \qquad b_2 = b_1 \circ h'$$

mit $h, h' \in H$. Da H ein Normalteiler ist, gilt

$$Hb_1 = b_1 H,$$

also existiert ein $h'' \in H$ mit

$$h \circ b_1 = b_1 \circ h''$$

und damit

$$(a_2 \circ b_2)H = (a_1 \circ h \circ b_1 \circ h')H = (a_1 \circ b_1 \circ h'' \circ h')H = (a_1 \circ b_1)H.$$

Man beachte, dass $hH = H$ für alle $h \in H$, da Multiplikation mit h eine bijektive Abbildung $H \to H$ gibt (warum?).

Wir überprüfen noch, dass diese wohldefinierte Verknüpfung auf G/H tatsächlich eine Gruppenstruktur definiert: Assoziativität

$$(aH \cdot bH) \cdot cH = aH \cdot (bH \cdot cH)$$

folgt aus $(a \circ b) \circ c = a \circ (b \circ c)$. Weiter ist

$$eH = H$$

das neutrale Element und

$$(aH)^{-1} = a^{-1}H$$

das Inverse von aH. ■

Beispiel 4.3.7 *Jede Untergruppe einer abelschen Gruppe ist ein Normalteiler. Zum Beispiel sind die Untergruppen* $n\mathbb{Z} \subset (\mathbb{Z}, +)$

Normalteiler. Wir überprüfen dies nochmals anhand der Definition: Für alle $g \in \mathbb{Z}$ gilt

$$\begin{aligned} g + n\mathbb{Z} &= \{g + nk \mid k \in \mathbb{Z}\} \\ &= \{nk + g \mid k \in \mathbb{Z}\} = n\mathbb{Z} + g. \end{aligned}$$

Die Quotientengruppen sind die Restklassengruppen

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/n = \left\{\overline{0}, ..., \overline{n-1}\right\}.$$

Das neutrale Element ist $\overline{0} = 0 + n\mathbb{Z} = n\mathbb{Z}$ und das Inverse $-\overline{a} = \overline{-a} = \overline{n-a}$.

Beispiel 4.3.8 *$A_n = \ker(\text{sign}) \subset S_n$ ist nach Bemerkung 4.3.3 ein Normalteiler. Wir überprüfen dies nochmals anhand der Definition: Für alle $\tau \in S_n$ und $\sigma \in A_n$ gilt*

$$\text{sign}(\tau \circ \sigma \circ \tau^{-1}) = \text{sign}(\tau)\,\text{sign}(\sigma)\,\text{sign}(\tau)^{-1} = \text{sign}(\sigma) = 1.$$

Bemerkung 4.3.9 *Jede Untergruppe $U \subset G$ vom Index $[G : U] = 2$ ist ein Normalteiler von G.*

Den kurzen Beweis geben wir in Übungsaufgabe 4.16. Siehe auch Übungsaufgabe 4.13.

Beispiel 4.3.10 *Die Untergruppe $U = \langle(1,2,3)\rangle$ der Drehsymmetrien des gleichseitigen Dreiecks D ist ein Normalteiler der Symmetriegruppe $S_3 = \text{Sym}(D)$. Die Nebenklassen sind*

$$()U = U() = U = \{(), (1,2,3), (1,3,2)\}$$

und

$$\begin{aligned} &(1,2)U = (1,3)U = (2,3)U \\ &= U(1,2) = U(1,3) = U(2,3) \\ &= \{(1,2), (2,3), (1,3)\} \end{aligned}$$

4.3.2 Homomorphiesatz

Ist $\varphi : G \longrightarrow F$ ein Monomorphismus, dann können wir $G \cong \text{Bild}(\varphi) \subset F$ als Untergruppe von F auffassen. Anderenfalls kann man φ mittels der Quotientengruppenkonstruktion injektiv machen:

Satz 4.3.11 (Homomorphiesatz) *Sei $\varphi : G \longrightarrow F$ ein Gruppenhomomorphismus. Dann gilt*

$$G/\operatorname{Ker}\varphi \cong \text{Bild}(\varphi).$$

Beweis. Wir definieren

$$\begin{aligned}\widetilde{\varphi} : G/\operatorname{Ker}\varphi &\longrightarrow \text{Bild}\,\varphi \\ \widetilde{\varphi}(a\operatorname{Ker}\varphi) &:= \varphi(a)\end{aligned}$$

Dies ist wohldefiniert, da für

$$a' = a \circ h \in a\operatorname{Ker}\varphi \text{ mit } h \in \operatorname{Ker}\varphi$$

gilt

$$\varphi(a') = \varphi(a)\cdot\varphi(h) = \varphi(a)\cdot e = \varphi(a).$$

Mit φ ist auch $\widetilde{\varphi}$ ein Homomorphismus, surjektiv auf das Bild von φ, und injektiv, denn

$$\begin{aligned}&\widetilde{\varphi}(a\operatorname{Ker}\varphi) = e \\ \Rightarrow\ &\varphi(a) = e \Rightarrow a \in \operatorname{Ker}\varphi \\ \Rightarrow\ &a\operatorname{Ker}\varphi = \operatorname{Ker}\varphi = e_{G/\operatorname{Ker}\varphi}.\end{aligned}$$

■

Also faktorisiert $\varphi : G \longrightarrow F$ in

$$\begin{array}{ccccc} & G & \xrightarrow{\varphi} & F & \\ \text{Projektion} & \downarrow & & \uparrow & \text{Inklusion} \\ & G/\operatorname{Ker}\varphi & \cong & \text{Bild}\,\varphi & \end{array}$$

Beispiel 4.3.12 *Sei $n \geq 2$. Angewendet auf* $\text{sign} : S_n \to (\{-1,1\},\cdot)$ *mit Kern A_n und* $\text{Bild}(\text{sign}) = \{-1,1\} \cong \mathbb{Z}/2$ *gibt Satz 4.3.11, dass*

$$S_n/A_n \cong \mathbb{Z}/2.$$

Beispiel 4.3.13 *Die* ***Kleinsche Vierergruppe***

$$V_4 = \{(), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$$

ist ein Normalteiler von S_4 *und für die Quotientengruppe gilt*

$$S_4/V_4 \cong S_3.$$

Dies zeigen wir in Übungsaufgabe 4.18, wo wir den Isomorphismus geometrisch interpretieren, indem wir die S_4 *als Symmetriegruppe des Tetraeders auffassen.*

Man kann $S_4/V_4 \cong S_3$ *auch mit Hilfe von GAP beweisen:*

```
S4:=SymmetricGroup(4);;
NormalSubgroups(S4);
[ Group(()),
Group([ (1,4)(2,3), (1,3)(2,4) ]),
Group([ (2,4,3), (1,4)(2,3), (1,3)(2,4) ]),
Sym( [ 1 .. 4 ] ) ]
V4:=Group((1,2)(3,4),(1,3)(2,4));;
Elements(V4);
[ (), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3) ]
Q:=S4/V4;;
Order(Q);
6
IsomorphismGroups(Q,CyclicGroup(6));
fail
IsomorphismGroups(Q,SymmetricGroup(3));
[ f1, f2 ] -> [ (2,3), (1,2,3) ]
```

Beispiel 4.3.14 (Klassifikation zyklischer Gruppen) *Eine zyklische Gruppe* G *ist eine Gruppe die von einem einzigen Element* $g \in G$ *erzeugt wird, also* $G = \langle g \rangle$*. Dann ist*

$$\begin{array}{rcl} \varphi : (\mathbb{Z}, +) & \longrightarrow & \langle g \rangle = G \\ k & \longmapsto & g^k \end{array}$$

ein Epimorphismus. Die Ordnung $\operatorname{ord}(g) = |G|$ *kann endlich oder unendlich sein. Im Fall* $\operatorname{ord}(g)$ *unendlich ist* φ *ein Isomorphismus, denn nur* $g^0 = e$*. Anderenfalls ist* $\operatorname{Ker}\varphi = \langle n \rangle = n\mathbb{Z}$ *(da jede*

Untergruppe von $\mathbb{Z}$ von der Form $n\mathbb{Z}$ ist) und der Homomorphiesatz gibt

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} &\cong \langle g \rangle \\ \overline{k} &\mapsto g^k \end{aligned}$$

Somit haben wir gezeigt: Jede zyklische Gruppe G endlicher Ordnung ist isomorph zu $\mathbb{Z}/n\mathbb{Z}$ mit $n = |G|$, jede zyklische Gruppe unendlicher Ordnung ist isomorph zu $\mathbb{Z}$.

4.4 Übungsaufgaben

Übung 4.1 *Basteln Sie Papiermodelle der Platonischen Körper Tetraeder, Würfel, Oktaeder, Dodekaeder und Ikosaeder (siehe Abbildung 4.1).*

Übung 4.2 *Sei G eine Menge zusammen mit einer Verknüpfung*

$$\begin{array}{rccc} \circ : & G \times G & \longrightarrow & G \\ & (a,b) & \mapsto & a \circ b \end{array}$$

die folgende Axiome erfüllt:

(G1) Assoziativität

$$a \circ (b \circ c) = (a \circ b) \circ c \ \forall a, b, c \in G.$$

(G2') Es existiert ein linksneutrales Element, d.h. ein

$$e \in G$$

mit

$$e \circ a = a \ \forall a \in G.$$

(G3') Existenz des Linksinversen, d.h. $\forall a \in G \ \exists a^{-1} \in G$ mit

$$a^{-1} \circ a = e.$$

Zeigen Sie:

1) Für $a, b \in G$ gilt: Ist $a \circ b = e$, dann ist auch $b \circ a = e$.

2) *Es ist* $a \circ e = a$ *für alle* $g \in G$.

3) *Das neutrale Element von* G *ist eindeutig.*

4) *Die Inversen der Elemente von* G *sind eindeutig.*

5) *Für* $a, b \in G$ *ist* $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$.

6) *Für* $a \in G$ *ist* $(a^{-1})^{-1} = a$.

Übung 4.3 *Untersuchen Sie, ob durch die folgenden Definitionen eine Halbgruppe, ein Monoid oder eine Gruppe gegeben ist:*

1) $\mathbb{R} \cup \{-\infty\}$ *zusammen mit der Verknüpfung*

$$a \heartsuit b = \max\{a, b\},$$

2) $3 + 6\mathbb{Z} = \{3 + 6 \cdot k \mid k \in \mathbb{Z}\}$ *mit der Addition,*

3) $\mathbb{R}^n$ *mit der Verknüpfung*

$$(a_1, ..., a_n) + (b_1, ..., b_n) = (a_1 + b_1, ..., a_n + b_n).$$

Übung 4.4 *Sei* $\varphi : G_1 \longrightarrow G_2$ *ein Gruppenhomomorphismus. Zeigen Sie:*

1) $\mathrm{Ker}(\varphi) \subset G_1$ *und* $\mathrm{Bild}(\varphi) \subset G_2$ *von* φ *sind Untergruppen.*

2) *Ist* φ *ein Isomorphismus, dann ist auch die Umkehrabbildung*

$$\varphi^{-1} : G_2 \longrightarrow G_1$$

ein Gruppenisomorphismus.

Übung 4.5 *Zeigen Sie, dass*

$$\begin{array}{rccl} \mathrm{sign}: & S_n & \longrightarrow & (\{1, -1\}, \cdot) \\ & \sigma & \longmapsto & \mathrm{sign}(\sigma) = \prod\limits_{\substack{i,j=1 \\ i<j}}^{n} \frac{\sigma(i) - \sigma(j)}{i - j} \end{array}$$

ein Gruppenepimorphismus ist.

Übung 4.6 *Lässt sich bei dem bekannten Schiebespiel folgende Konfiguration*

2	1	3	4
5	6	7	8
9	10	11	12
13	14	15	

in die Ausgangsstellung

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

überführen?

Übung 4.7 *Schreiben Sie*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 5 & 6 & 4 & 3 & 7 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 4 & 2 & 5 & 7 & 6 \end{pmatrix},$$

$\sigma \circ \tau$ und $\tau \circ \sigma$ sowohl als Produkt disjunkter Zykel als auch als Produkt von Transpositionen. Bestimmen Sie jeweils Ordnung und sign*.*

Übung 4.8 *1) Zeigen Sie: Sind $a, b \in \mathbb{Z}$ mit $a, b \geq 1$ und $\mathrm{ggT}(a, b) = 1$. Dann gilt*

$$\mathbb{Z}/(a \cdot b) \cong \mathbb{Z}/a \times \mathbb{Z}/b.$$

2) Bestimmen Sie das Urbild von $(8 + 10\mathbb{Z}, -11 + 21\mathbb{Z})$ unter dem Gruppenisomorphismus

$$\mathbb{Z}/210 \cong \mathbb{Z}/10 \times \mathbb{Z}/21.$$

Übung 4.9 *1) Sei G eine Gruppe und seien $x, y \in G$ mit $x \cdot y = y \cdot x$ und $\langle x \rangle \cap \langle y \rangle = \{e\}$. Zeigen Sie:*

$$\mathrm{ord}(x \cdot y) = \mathrm{kgV}(\mathrm{ord}(x), \mathrm{ord}(y)).$$

2) Sei

$$\sigma = c_1 \cdot \ldots \cdot c_r \in S_n$$

Produkt disjunkter Zykel c_i der Längen m_i. Bestimmen Sie $\operatorname{ord}(\sigma)$.

Übung 4.10 *Welche Ordnungen treten bei den Elementen von S_6 auf?*

Übung 4.11 *1) Schreiben Sie jedes Element der S_4 als Produkt disjunkter Zykel.*

2) Ordnen Sie jedem $\sigma \in S_4$ eine Partition von 4 zu (d.h. eine Summe $4 = p_1 + \ldots + p_r$ mit $p_i \geq 1$). Diese Partition nennt man Zykeltyp von σ.

3) Interpretieren Sie jeden Zykeltyp geometrisch, indem Sie die S_4 als Symmetriegruppe des Tetraeders (Abbildung 4.14) auffassen.

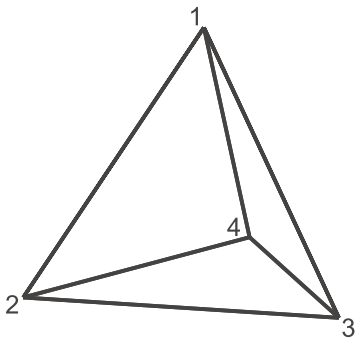


Abbildung 4.14: Tetraeder

Übung 4.12 *1) Zeigen Sie: Die Abbildung*

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (a, b) & \longmapsto & a \circ b \circ a^{-1} \end{array}$$

definiert eine Operation von G auf G von links, die ***Konjugation****.*

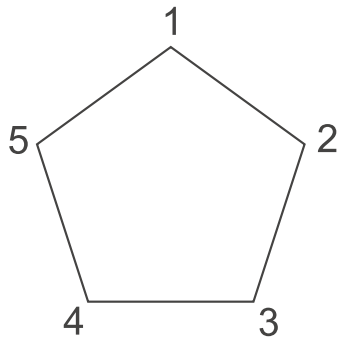


Abbildung 4.15: Regelmäßiges 5-Eck

2) *Die Bahn von* $b \in G$

$$b^G := \left\{ a \circ b \circ a^{-1} \mid a \in G \right\}$$

heißt ***Konjugationsklasse*** *von* b*. Bestimmen Sie alle Konjugationsklassen der* S_3*.*

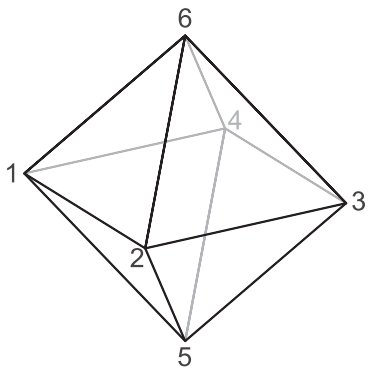
Übung 4.13 *Sei* G *die Symmetriegruppe des regelmäßigen* 5*-Ecks (Abbildung 4.15). Bestimmen Sie*

1) *die Gruppenordnung von* G *(beweisen Sie Ihre Behauptung),*

2) *alle Elemente von* G *als Permutationen der Ecken,*

3) *alle Untergruppen von* G *und welche davon Normalteiler sind.*

Übung 4.14 *Sei* $G = \mathrm{Sym}(O)$ *die Symmetriegruppe des Oktaeders* O*. Durch Nummerieren der Ecken*



können wir G als Untergruppe der S_6 auffassen.

1) *Bestimmen Sie die Gruppenordnung von G mit Hilfe der Bahnformel.*

2) *Finden Sie Erzeuger von G und beweisen Sie Ihre Behauptung mit Hilfe von GAP.*

3) *Bestimmen Sie die Konjugationsklassen von G mit Hilfe von GAP.*

4) *Interpretieren Sie die Elemente von G geometrisch.*

Hinweis: Verwenden Sie die GAP-Befehle `Group`, `Order` *und* `ConjugacyClasses`.

Übung 4.15 *Zeigen Sie, dass es genau 11 Isomorphieklassen von (ungerichteten) Graphen mit 4 Vertices gibt.*

Übung 4.16 *Sei H eine Untergruppe von G. Zeigen Sie: Ist $[G:H]=2$, dann ist H ein Normalteiler in G.*

Übung 4.17 *Sei $\varphi : G \longrightarrow F$ ein Gruppenhomomorphismus. Zeigen Sie:*

1) *Ist $M \subset F$ ein Normalteiler, dann ist $\varphi^{-1}(M) \subset G$ ein Normalteiler.*

2) *Ist φ surjektiv und $N \subset G$ ein Normalteiler, dann ist $\varphi(N) \subset F$ ein Normalteiler.*

3) *Geben Sie ein Beispiel eines Gruppenhomomorphismus an, dessen Bild kein Normalteiler ist.*

Übung 4.18 *Zeigen Sie, dass die Kleinsche Vierergruppe*

$$V_4 = \{(), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$$

ein Normalteiler in S_4 ist und für die Quotientengruppe gilt

$$S_4/V_4 \cong S_3.$$

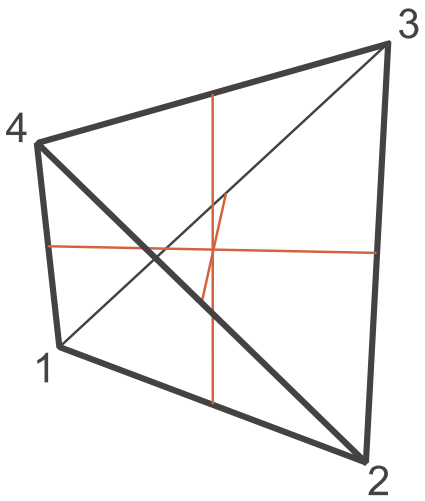


Abbildung 4.16: Tetraeder mit Kantenmittendiagonalen

Geben Sie eine geometrische Interpretation, indem Sie die S_4 als Symmetriegruppe des Tetraeders auffassen.

Hinweis: Jede Symmetrie des Tetraeders $T \subset \mathbb{R}^3$ mit den Ecken

$$e_1 = (1,-1,-1) \quad e_2 = (-1,1,-1) \quad e_3 = (-1,-1,1) \quad e_4 = (1,1,1)$$

permutiert die Koordinatenachsen von $\mathbb{R}^3$, siehe Abbildung 4.16. Dies induziert einen Gruppenhomomorphismus

$$\varphi : S_4 \to S_3.$$

Übung 4.19 *Zeigen Sie, dass die Kleinsche Vierergruppe*

$$V_4 = \{(), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$$

ein Normalteiler in S_4 ist und für die Quotientengruppe gilt

$$S_4/V_4 \cong S_3$$

Geben Sie eine geometrische Interpretation, indem Sie die S_4 als Symmetriegruppe des Tetraeders auffassen.

Übung 4.20 *Sei G die Symmetriegruppe des Ikosaeders.*

1) Bestimmen Sie die Gruppenordnung von G.

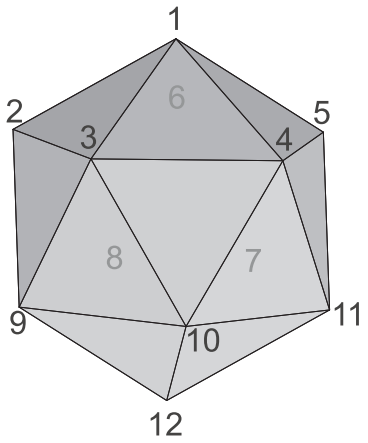


Abbildung 4.17: Ikosaeder mit Nummerierung der Ecken

2) Finden Sie Erzeuger der Symmetriegruppe G des Ikosaeders (Abbildung 4.17) als Untergruppe der S_{12}. Beweisen Sie Ihre Behauptung mit Hilfe von GAP.

Übung 4.21 *Zeigen Sie:*

1) Ist

$$\sigma = \begin{pmatrix} 1 & \cdots & n-1 & n \\ \sigma(1) & & \sigma(n-1) & k \end{pmatrix} \in S_n,$$

dann ist

$$(n-1,n) \cdot \ldots \cdot (k,k+1) \cdot \sigma \in S_{n-1}.$$

2) Die symmetrische Gruppe S_n wird erzeugt von den Transpositionen $(1,2),(2,3),\ldots,(n-1,n)$, d.h.

$$S_n = \langle (1,2),(2,3),\ldots,(n-1,n) \rangle .$$

Übung 4.22 *Sei $G \subset S_n$ eine Untergruppe mit $(1,2) \in G$ und $(1,2,\ldots,n) \in G$. Zeigen Sie*

$$G = S_n.$$

5

Ringe

5.1 Übersicht

Im ersten Kapitel hatten wir uns mit dem Ring der ganzen Zahlen $\mathbb{Z}$ und dessen grundlegenden Eigenschaften beschäftigt, insbesondere mit der Existenz einer eindeutigen Primfaktorisierung, dem Euklidischen Algorithmus zur Bestimmung des größten gemeinsamen Teilers und dem Chinesischen Restsatz. Hier wollen wir untersuchen, inwieweit sich diese Eigenschaften auch bei anderen Ringen wiederfinden lassen. Außerdem werden wir einem Ring die sogenannte Einheitengruppe zuordnen und diese dann mit Hilfe der Methoden der Gruppentheorie aus Kapitel 2 untersuchen.

In Verallgemeinerung der ganzen Zahlen ist ein **kommutativer Ring mit 1** eine Menge R mit Verknüpfungen + (Addition) und $\cdot$ (Multiplikation), sodass

1) $(R, +)$ eine abelsche Gruppe (mit neutralem Element 0) ist,

2) $(R, \cdot)$ ein kommutatives Monoid (mit neutralem Element 1) ist,

3) das von $\mathbb{Z}$ bekannte Distributivgesetz

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

für alle $a, b, c \in R$ gilt.

Neben $\mathbb{Z}$ ist zum Beispiel auch die Restklassengruppe

$$\mathbb{Z}/n = \left\{\overline{0}, ..., \overline{n-1}\right\}$$

ein Ring durch Multiplikation der Repräsentanten

$$\overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

Dies ist wohldefiniert, denn

$$(a + k_1 \cdot n) \cdot (b + k_2 \cdot n) = a \cdot b + n \cdot (k_1 \cdot b + k_2 \cdot a + k_1 \cdot k_2 \cdot n).$$

Das folgende Beispiel zeigt eine Anwendung der Multiplikation:

Beispiel 5.1.1 *Heute ist Freitag und Vollmond. Vollmond tritt alle* 30 *Tage auf. Nach wieviel Tagen ist zum nächsten Mal Vollmond an einem Montag? Dazu bestimmen wir alle* $k \in \mathbb{Z}$ *mit*

$$5 + 30 \cdot k \equiv 1 \bmod 7,$$

d.h. $\overline{k} \in \mathbb{Z}/7$ *mit*

$$\overline{2} \cdot \overline{k} = \overline{3} \in \mathbb{Z}/7.$$

Können wir durch $\overline{2}$ *teilen, dann lässt sich* $\overline{k}$ *berechnen. Tatsächlich besitzt* $\overline{2} \in \mathbb{Z}/7$ *ein multiplikativ Inverses, denn*

$$\overline{4} \cdot \overline{2} = \overline{1}.$$

Somit ist

$$\overline{k} = \overline{2}^{-1} \cdot \overline{3} = \overline{4} \cdot \overline{3} = \overline{12} = \overline{5}.$$

Nach $5 \cdot 30 = 150$ *Tagen ist also zum nächsten Mal Vollmond an einem Montag.*

Sind alle Elemente von $\mathbb{Z}/n$ invertierbar? Offenbar ist $\overline{1}$ immer invertierbar und $\overline{0}$ nie invertierbar. Betrachten wir als Beispiel $\mathbb{Z}/4$. Die Verknüpfungen sind gegeben durch

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Wir sehen, dass $\overline{3}$ bezüglich $\cdot$ ein Inverses besitzt, denn

$$\overline{3} \cdot \overline{3} = \overline{1}.$$

Dagegen ist $\overline{2}$ nicht invertierbar, da in der Gruppentafel der Multiplikation in der entsprechenden Zeile (oder Spalte) keine $\overline{1}$ steht. Allgemein bezeichnet man ein Element $a \in R$ als **Einheit**, wenn a die 1 teilt, d.h. ein $b \in R$ existiert mit

$$a \cdot b = 1.$$

Die Menge der Einheiten $R^\times$ bildet bezüglich $\cdot$ eine Gruppe, die **Einheitengruppe**, zum Beispiel hat $(\mathbb{Z}/4)^\times$ die Gruppentafel

$\cdot$	$\overline{1}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{3}$	$\overline{1}$

Viele praktische Anwendungen von Gruppen verwenden $(\mathbb{Z}/n)^\times$, etwa die RSA Public-Key-Kryptographie.

Das Element $\overline{2}$ ist nicht nur keine Einheit, es gilt sogar

$$\overline{2} \cdot \overline{2} = \overline{0}.$$

Allgemein heißt $a \in R$ **Nullteiler** von R, wenn a die Null teilt, d.h. ein $0 \neq b \in R$ existiert mit

$$a \cdot b = 0.$$

Ein Element kann nicht sowohl Einheit als auch Nullteiler sein, denn ist a eine Einheit und $a \cdot b = 0$, dann ist $b = a^{-1}ab = 0$. In den Übungen werden wir zeigen, dass, falls R nur endlich viele Elemente hat, jedes Element entweder Einheit oder Nullteiler ist (siehe Aufgabe 5.11). Im Allgemeinen gilt dies nicht: In $\mathbb{Z}$ gibt es (außer dem trivialen Nullteiler 0) keine Nullteiler, und die Einheiten sind 1 und -1.

Ein Ring (kommutativ mit $1 \neq 0$) ohne nicht-triviale Nullteiler heißt auch **Integritätsring**. Man kann dann durch Einführen von Brüchen jedes Element außer 0 zu einer Einheit machen. Die Verknüpfungen sind

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + cb}{bd} \quad \text{und} \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd},$$

wir brauchen also $b, d \neq 0 \Rightarrow bd \neq 0$. Zum Beispiel bilden wir so $\mathbb{Q}$ aus $\mathbb{Z}$. Ein Ring (kommutativ mit $1 \neq 0$), in dem jedes Element ungleich 0 eine Einheit ist, heißt **Körper**. Durch Bruchrechnung mit Elementen eines Integritätsrings erhält man den sogenannten Quotientenkörper. Körper spielen eine wichtige Rolle in der linearen Algebra.

Insgesamt werden wir die folgenden Klassen von Ringen einführen, die die wesentlichen Eigenschaften der ganzen Zahlen verallgemeinern: die Konstruktion des Quotientenkörpers, die Existenz einer Primfaktorisierung und die Durchführbarkeit des Euklidischen Algorithmus.

	Eigenschaften	Beispiel für $R = \mathbb{Z}$
$\left\{ \begin{array}{c} \text{Integritäts-} \\ \text{ringe} \end{array} \right\}$	Quotientenkörper-konstruktion	$\mathbb{Q}$
$\cup$		
$\left\{ \begin{array}{c} \text{Faktorielle} \\ \text{Ringe} \end{array} \right\}$	Eindeutige Primfaktorisierung, Existenz des ggT	$120 = 2^3 \cdot 3 \cdot 5$ $84 = 2^2 \cdot 3 \cdot 7$ $\text{ggT}\,(120, 84) = 2^2 \cdot 3$
$\cup$		
$\left\{ \begin{array}{c} \text{Euklidische} \\ \text{Ringe} \end{array} \right\}$	Euklidischer Algorithmus zur Bestimmung des ggT	$120 = 1 \cdot 84 + 36$ $84 = 2 \cdot 36 + 12$ $36 = 3 \cdot 12 + 0$

Aufgrund der Durchführbarkeit des Euklidischen Algorithmus spielen Euklidische Ringe eine besonders wichtige Rolle in der Informatik, es gibt aber auch andere Ringe, die algorithmisch zugänglich sind.

5.2 Grundbegriffe

Definition 5.2.1 *Ein* ***Ring*** $(R, +, \cdot)$ *ist eine Menge R zusammen mit zwei Verknüpfungen*

$$+ : R \times R \longrightarrow R,\ (a, b) \longmapsto a + b$$
$$\cdot : R \times R \longrightarrow R,\ (a, b) \longmapsto a \cdot b$$

für die gilt

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

(R2) die Multiplikation $\cdot$ *ist assoziativ,*

(R3) die Verknüpfungen sind distributiv, d.h.

$$a\cdot(b+c)=a\cdot b+a\cdot c$$
$$(a+b)\cdot c=a\cdot c+b\cdot c$$

für alle $a,b,c\in R$.

Existiert darüber hinaus ein ***Einselement****, d.h.*

(R4) es gibt ein Element $1\in R$ *mit*

$$a\cdot 1=1\cdot a=a$$

für alle $a\in R$*, so spricht man von einem* ***Ring mit 1*** *(als neutrales Element des Monoids* $(R,\cdot)$ *ist die* 1 *eindeutig), und ist*

(R5) die Multiplikation $\cdot$ ***kommutativ****, d.h.*

$$a\cdot b=b\cdot a$$

für alle $a,b\in R$*, so nennt man* R *einen* ***kommutativen Ring****.*

Ist $\varnothing\neq U\subset R$ *mit* $+$ *und* $\cdot$ *ein Ring, dann bezeichnen wir* U *als* ***Unterring*** *von* R*. Ist* R *ein Ring mit* 1*, so verlangen wir (in der Regel) außerdem* $1\in U$*.*

Wir schreiben für das Null- und Einselement auch 0_R und 1_R, falls im Kontext verschiedene Ringe vorkommen.

Beispiel 5.2.2 *1)* $R=\{0\}$ *ist ein Ring mit* $0=1$*, der sogenannte* ***Nullring****.*

2) $\mathbb{Z}\,,\mathbb{Q}\,,\mathbb{R}\,,\mathbb{C}$ *sind kommutative Ringe mit* 1*.*

3) Die geraden Zahlen $2\mathbb{Z}\subset\mathbb{Z}$ *bilden einen kommutativen Ring ohne* 1*.*

4) Sind R_1, R_2 Ringe, dann ist das kartesische Produkt $R_1 \times R_2$ ein Ring mit komponentenweiser Addition

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2)$$

und Multiplikation

$$(a_1, a_2) \cdot (b_1, b_2) = (a_1 \cdot b_1, a_2 \cdot b_2)\,.$$

Definition 5.2.3 *Seien R und S Ringe. Ein* ***Ringhomomorphismus***

$$\varphi : R \longrightarrow S$$

ist eine Abbildung, die

$$\varphi(a + b) = \varphi(a) + \varphi(b)$$

und

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$$

für alle $a, b \in R$ erfüllt (insbesondere ist $\varphi : (R, +) \longrightarrow (S, +)$ ein Gruppenhomomorphismus). Sind R und S Ringe mit 1, so verlangen wir in der Regel außerdem

$$\varphi(1_R) = 1_S.$$

Die Begriffe Mono-, Epi- und Isomorphismus werden analog wie bei Gruppen verwendet.

Bemerkung 5.2.4 *Das Bild von $\varphi(R) \subset S$ ist ein Unterring, ebenso der Kern*

$$\operatorname{Ker}\varphi = \{r \in R \mid \varphi(r) = 0\} \subset R.$$

Bemerkung 5.2.5 *Für einen Ring R mit 1 ist $\operatorname{Ker}\varphi$ ein Ring mit 1 nur in dem Spezialfall der Nullabbildung, denn*

$$1_R \in \operatorname{Ker}\varphi \Leftrightarrow \varphi(r) = \varphi(r \cdot 1_R) = \varphi(r) \cdot \varphi(1_R) = 0 \ \forall r \in R \Leftrightarrow \operatorname{Ker}\varphi = R.$$

Dies liegt daran, dass $\operatorname{Ker}\varphi$ ein Ideal ist. Darauf werden wir im nächsten Abschnitt über Ideale zurückkommen. Die Forderung $\varphi(1_R) = 1_S$ schließt also nur die Nullabbildung aus (warum?).

5.3 Die Einheitengruppe von $\mathbb{Z}/n$

Definition 5.3.1 *Sei R ein kommutativer Ring mit 1. Ein Element $u \in R$ heißt **Einheit** von R, wenn ein $w \in R$ existiert mit*

$$w \cdot u = 1.$$

*Die Menge der Einheiten wird mit $R^\times$ bezeichnet. Mit u ist offenbar auch w eine Einheit und $(R^\times, \cdot)$ ist eine Gruppe, die **Einheitengruppe** von R.*

Gilt $1 \neq 0$ und ist

$$R^\times = R \backslash \{0\},$$

*so heißt R **Körper**.*

Bemerkung: Das Inverse $w = u^{-1}$ ist in $R^\times$ eindeutig (Übung 4.2).

Ein Element $\overline{a} \in \mathbb{Z}/n$ ist also invertierbar genau dann, wenn es ein $b \in \mathbb{Z}$ gibt mit $\overline{a} \cdot \overline{b} = \overline{1}$, das heißt, wenn es $b, k \in \mathbb{Z}$ gibt mit

$$a \cdot b + n \cdot k = 1$$

Solche b und k erhalten wir mit dem erweiterten Euklidischen Algorithmus, falls

$$\mathrm{ggT}\,(a, n) = 1.$$

Haben wir umgekehrt eine solche Darstellung der 1, dann müssen natürlich a und n teilerfremd sein (denn jeder gemeinsame Teiler teilt auch 1). Somit können wir die Elemente der Einheitengruppe beschreiben:

Satz 5.3.2 *Für $n \in \mathbb{N}$ ist*

$$(\mathbb{Z}/n)^\times = \{\overline{a} \in \mathbb{Z}/n \mid \mathrm{ggT}\,(a, n) = 1\}$$

*Die Elemente heißen **prime Restklassen**. Die Gruppe $(\mathbb{Z}/n)^\times$ bezeichnen wir auch als die **prime Restklassengruppe**.*

Als direkte Folgerung erhalten wir:

Corollar 5.3.3 *Der Ring $\mathbb{Z}/n$ ist ein Körper genau dann, wenn n eine Primzahl ist.*

Beispiel 5.3.4 *Die Restklasse* $\overline{8} \in \mathbb{Z}/15$ *hat ein multiplikativ Inverses, d.h.* $\overline{8} \in (\mathbb{Z}/15)^\times$*, denn*

$$\mathrm{ggT}\,(8, 3 \cdot 5) = 1$$

Mit dem erweiterten Euklidischen Algorithmus erhalten wir eine Darstellung des größten gemeinsamen Teilers

$$1 = (2) \cdot 8 + (-1) \cdot 15$$

also ist

$$\overline{8}^{-1} = \overline{2}$$

Definition 5.3.5 *Die* ***Eulersche φ-Funktion*** $\varphi : \mathbb{N} \to \mathbb{Z}$ *ist definiert durch*

$$\varphi(n) := \left|(\mathbb{Z}/n)^\times\right| = |\{r \in \mathbb{Z} \mid 1 \le r \le n,\ \mathrm{ggT}\,(r, n) = 1\}|$$

gibt also für n *die Ordnung der Einheitengruppe* $(\mathbb{Z}/n)^\times$ *an.*

Satz 5.3.6 (Satz von Fermat-Euler) *Für alle* $a, n \in \mathbb{Z}$*,* $n \ge 1$ *mit* $\mathrm{ggT}\,(a, n) = 1$ *gilt*

$$a^{\varphi(n)} \equiv 1 \bmod n.$$

Beweis. Nach Corollar 4.2.52 teilt die Ordnung jedes Elements g einer Gruppe G die Gruppenordnung, also

$$g^{|G|} = e.$$

Angewendet auf $\overline{a} \in (\mathbb{Z}/n)^\times$ erhalten wir

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

■

Für Primzahlen p ist

$$\varphi(p) = p - 1,$$

also

$$a^{p-1} \equiv 1 \bmod p \quad \text{falls } p \nmid a$$

und somit (denn für $p \mid a$ ist $a^p \equiv 0 \equiv a \bmod p$):

Corollar 5.3.7 (Kleiner Satz von Fermat) *Ist p eine Primzahl und $a \in \mathbb{Z}$, dann gilt*

$$a^p \equiv a \bmod p.$$

Zur Berechnung der Eulerschen φ-Funktion verwendet man, dass sie multiplikativ über teilerfremde Produkte ist. Dazu bemerken wir zunächst: Der durch den Chinesischen Restsatz gegebene Gruppenisomorphismus (siehe Übung 4.8) ist tatsächlich ein Ringisomorphismus:

Satz 5.3.8 *Sind $m_1, m_2 \in \mathbb{N}$ teilerfremd, dann gilt*

$$\mathbb{Z}/m_1m_2 \cong \mathbb{Z}/m_1 \times \mathbb{Z}/m_2.$$

Beweis. Wie in Übung 4.8 gezeigt ist durch

$$\begin{array}{rccc} \pi: & \mathbb{Z}/m_1m_2 & \longrightarrow & \mathbb{Z}/m_1 \times \mathbb{Z}/m_2 \\ & a + m_1m_2\mathbb{Z} & \longmapsto & (a + m_1\mathbb{Z},\ a + m_2\mathbb{Z}) \end{array}$$

ein wohldefinierter Isomorphismus abelsche Gruppen bezüglich + gegeben. Weiter ist

$$\begin{aligned} \pi(ab + m_1m_2\mathbb{Z}) &= (ab + m_1\mathbb{Z},\ ab + m_2\mathbb{Z}) \\ &= ((a + m_1\mathbb{Z}) \cdot (b + m_1\mathbb{Z}),\ (a + m_2\mathbb{Z}) \cdot (b + m_2\mathbb{Z})) \\ &= (a + m_1\mathbb{Z},\ a + m_2\mathbb{Z}) \cdot (b + m_1\mathbb{Z},\ b + m_2\mathbb{Z}) \\ &= \pi(a + m_1m_2\mathbb{Z}) \cdot \pi(b + m_1m_2\mathbb{Z}), \end{aligned}$$

also π ein Ringisomorphismus. ■

Beispiel 5.3.9 *Mit Satz 3.4.1 erhalten wir durch Bestimmung der Lösungsmenge der simultanen Kongruenzen*

$$x \equiv 7 \bmod 15 \Longleftrightarrow \begin{cases} x \equiv 1 \bmod 3 \\ x \equiv 2 \bmod 5 \end{cases}$$

Entsprechend Satz 5.3.8 läßt sich diese Aussage umformulieren als

$$\begin{array}{ccccccc} \mathbb{Z}/15 & \cong & \mathbb{Z}/3 & \times & \mathbb{Z}/5 & \text{und} & \\ \overline{7} & \mapsto & (\overline{1} & , & \overline{2}) & & \end{array}$$

Die Bestimmung des Urbilds von $(\overline{1},\overline{2})$ *unter diesem Isomorphismus ist also das Lösen der simultanen Kongruenz*

$$x \equiv 1 \bmod 3$$
$$x \equiv 2 \bmod 5$$

Umgekehrt ist die Berechnung des Bildes von $\overline{7}$ *einfach die Reduktion modulo* 3 *und* 5.

Bezüglich der Multiplikation gilt z.B.

$$\pi(\overline{7}) \cdot \pi(\overline{4}) = (\overline{1},\overline{2}) \cdot (\overline{1},\overline{4}) = (\overline{1},\overline{8}) = (\overline{1},\overline{3})$$
$$= \pi(\overline{13}) = \pi(\overline{7} \cdot \overline{4}).$$

Mit Satz 5.3.8 ist die φ-Funktion multiplikativ:

Corollar 5.3.10 *Sind* $m_1, m_2 \in \mathbb{N}$ *teilerfremd, dann gilt*

$$\varphi(m_1 m_2) = \varphi(m_1)\,\varphi(m_2).$$

Beweis. Es ist $a + m_1 m_2\mathbb{Z} \in (\mathbb{Z}/m_1 m_2)^\times$ genau dann, wenn

$$(a + m_1\mathbb{Z}, a + m_2\mathbb{Z}) \in (\mathbb{Z}/m_1 \times \mathbb{Z}/m_2)^\times,$$

äquivalent, wenn $a + m_i\mathbb{Z} \in (\mathbb{Z}/m_i)^\times$ für alle i, da die Multiplikation komponentenweise definiert ist. Somit

$$(\mathbb{Z}/m_1 m_2)^\times = (\mathbb{Z}/m_1)^\times \times (\mathbb{Z}/m_2)^\times$$

■

Insbesondere erhalten wir:

Bemerkung 5.3.11 *Ist* $n = p \cdot q$ *das Produkt von zwei Primzahlen, so gilt*

$$\varphi(n) = (p-1)(q-1).$$

5.4 Anwendung: RSA Kryptosystem

5.4.1 Übersicht

Als Anwendung der Gruppentheorie wollen wir das Kryptosystem RSA behandeln. Hier verwendet der Sender den öffentlichen Schlüssel des Empfängers zum Chiffrieren einer Nachricht

und der Empfänger seinen privaten Schlüssel zum Dechiffrieren, d.h. es handelt sich um ein sogenanntes **Public-Key Kryptosystem**. Das Verfahren wurde von James Ellis, Clifford Cocks und Malcolm Williamson im britischen Nachrichtendienst entwickelt (und geheim gehalten) und ist nach Ronald Rivest, Adi Shamir und Leonard Adleman benannt, die es später erneut entdeckt haben. Es basiert auf einer Trapdoor (Geheimtür) - Einwegfunktion

$$\{\text{Klartextnachrichten}\} \to \{\text{verschlüsselte Nachrichten}\},$$

deren Wert leicht berechnet werden kann, das Urbild dagegen nur unter hohem Rechenaufwand, sofern man nicht die Geheimtür-Information (d.h. den privaten Schlüssel) besitzt.

Im Fall von RSA beruht diese Eigenschaft im Wesentlichen darauf, dass die Primfaktorzerlegung (und damit die Geheimtür) heute nur schwer zu berechnen ist. Allerdings ist nicht klar, ob nicht in Zukunft schnellere Verfahren zur Verfügung stehen. Auch muss man bei der Verwendung von RSA abschätzen, wie lange die Verschlüsselung unter dem typischen exponentiellen Anstieg der Rechenleistung von Computern (Moores Gesetz) sicher ist.

Typischerweise wird aus Gründen der Geschwindigkeit RSA nur zum Austausch eines Schlüssels für ein konventionelles symmetrisches Kryptosystem (z.B. 3DES, AES, Twofish, Serpent) eingesetzt.

RSA beruht auf Potenzieren in der Einheitengruppe $(\mathbb{Z}/n)^\times$ mit $n = p \cdot q$ und p, q sehr groß und prim. Die Idee ist es, Zahlen e und d zu konstruieren, sodass

$$(m^e)^d = m^{ed} \equiv m \bmod n$$

ist für jede Nachricht $m \in (\mathbb{Z}/n)^\times$. Dann verschlüsseln wir durch Potenzieren mit der Zahl e (die wir öffentlich machen) und Entschlüsseln durch Potenzieren mit der d (die wir geheim halten). Um geeignete d und e zu konstruieren, verwenden wir, dass die Ordnung jedes Elements die Gruppenordnung $\varphi(n)$ teilt (Corollar 4.2.52).

5.4.2 Setup

Für RSA wählt man eine große Zahl $N \in \mathbb{N}$ und codiert Nachrichteneinheiten in eine Zahl $0 \leq m < N$ (zum Beispiel $N = 26^k$ und repräsentiert Buchstaben durch Ziffern). In der Praxis verwendet man ein N mit etwa 200 bis 600 Dezimalziffern.

Jeder Benutzer führt nun die folgenden Schritte aus:

1) Wähle 2 Primzahlen p, q mit $p \cdot q > N$. Man beachte, dass es nach dem Primzahlsatz 3.2.7 genügend Primzahlen gibt. Siehe auch Übung 5.6, in der wir einen ersten Blick auf einen sogenannten Primzahltests werfen, mit denen man ohne Faktorisierung sehr schnell herausfinden kann, ob eine Zahl mit hoher Wahrscheinlichkeit prim ist. Siehe auch Übung 5.7 für ein Zertifikat, dass eine Zahl p prim ist (dies ist aber deutlich langsamer, da man eine Faktorisierung von $p-1$ bestimmen muss).

2) Berechne
$$n := p \cdot q$$
und mit Bemerkung 5.3.11 den Wert der Eulerfunktion
$$\varphi(n) = (p-1)(q-1).$$
Die Zahlen p und q können nun gelöscht werden. Es ist keine effiziente Methode bekannt, um $\varphi(n)$ zu berechnen, ohne die Faktorisierung $n = p \cdot q$ zu bestimmen.

3) Wähle eine Zahl $e \in \mathbb{N}$ mit
$$\mathrm{ggT}(e, \varphi(n)) = 1.$$

4) Berechne das Inverse $0 < d < \varphi(n)$ von e modulo $\varphi(n)$, also mit
$$ed \equiv 1 \bmod \varphi(n).$$
Nun kann $\varphi(n)$ gelöscht werden.

Der öffentliche Schlüssel ist das Tupel (n, e) und der private Schlüssel d.

5.4.3 Nachrichtenübertragung

Betrachten wir nun zwei Personen Alice und Bob mit Schlüsseln

	privat	öffentlich
Alice	d_A	(n_A, e_A)
Bob	d_B	(n_B, e_B)

Will Bob an Alice eine Nachricht m senden, berechnet er mit Hilfe des öffentlichen Schlüssels von Alice

$$c := m^{e_A} \bmod n_A$$

und überträgt c an Alice. Wir nehmen an, dass $\mathrm{ggT}(m, n_A) = 1$, was mit sehr hoher Wahrscheinlichkeit der Fall ist (anderenfalls hat B einen Teiler von n_A gefunden und kann damit den privaten Schlussel von A berechnen). Somit repräsentiert m ein Element in $(\mathbb{Z}/n_A)^\times$.

Alice berechnet nun zum Entschlüsseln mit Hilfe von ihrem privaten Schlüssel

$$\tilde{m} := c^{d_A} \bmod n_A$$

Dann gilt modulo n_A, dass

$$\tilde{m} \equiv c^{d_A} \equiv \left(m^{e_A}\right)^{d_A} = m^{e_A d_A} = m^{1+k\cdot\varphi(n_A)} = m\cdot\left(m^{\varphi(n_A)}\right)^k \equiv m \bmod n_A$$

mit dem Satz von Fermat-Euler 5.3.6.

Beispiel 5.4.1 *Alice wählt*

$$n_A = 7 \cdot 11 = 77$$

also

$$\varphi(n_A) = 6 \cdot 10 = 60$$

und

$$e_A = 13$$

Der öffentliche Schlüssel von Alice ist dann

$$(n_A, e_A) = (77, 13)$$

Mit dem erweiterten Euklidischen Algorithmus erhalten wir

$$1 = \mathrm{ggT}(e_A, \varphi(n_A)) = (-23) \cdot 13 + (5) \cdot 60$$

und somit das Inverse d_A *von* e_A *modulo* $\varphi(n_A)$

$$d_A = 37$$

den privaten Schlüssel von Alice.

Bob möchte die Nachricht $m = 31$ *verschlüsselt an Alice senden, berechnet also*

$$m^{e_A} \bmod n_A = 31^{13} \bmod 77 = 3 \bmod 77$$

und überträgt

$$c = 3$$

Zum Entschlüsseln berechnet Alice dann

$$c^{d_A} \bmod n_A = 3^{37} = 31 \bmod 77$$

Siehe auch Übungsaufgabe 5.3.

Bemerkung 5.4.2 *Zum Berechnen von* a^b *modulo* n *verwendet man ein Verfahren zum modularen Potenzieren. Das heißt man berechnet nicht erst* a^b *und reduziert dann modulo* n *sondern reduziert auch alle Zwischenergebnisse des Algorithmus modulo* n*. Die einfachste derartige Methode ist, sukzessive mit* a *zu multiplizieren und in jedem Schritt modulo* n *zu reduzieren. Geschickter ist es, zunächst sukzessive zu quadrieren.*

Wir berechnen so etwa $2^{16} \bmod 11 = 9$ *durch*

$$2^2 \bmod 11 = 4$$
$$4^2 \bmod 11 = 5$$
$$5^2 \bmod 11 = 3$$
$$3^2 \bmod 11 = 9.$$

Ist b *keine Potenz von* 2*, dann bestimmt man zunächst die Binärdarstellung*

$$b = b_0 2^0 + b_1 2^1 + b_2 2^2 + \dots .$$

Siehe dazu Übungsaufgabe 5.5. In MAPLE *ist ein solches Verfahren in dem Kommando*

```
Power(a,b) mod n
```

implementiert:

```
Power(201, 20 000 000) mod 113
```

49

5.5 Anwendung: Primfaktorisierung mit dem Verfahren von Pollard

Gelingt es uns die Faktorisierung $n = p \cdot q$ zu bestimmen, so erhalten wir $\varphi(n) = (p-1)(q-1)$. Damit können wir aus dem öffentlichen Schlüssel e den privaten Schlüssel d bestimmen und somit jede mit (n, e) verschlüsselte Nachricht mitlesen. Für große Zahlen n ist Probedivision nicht praktikabel. Es gibt wesentlich effizientere Methoden, um einen Primteiler zu finden. Als Beispiel behandeln wir ein Verfahren von John Pollard, das unter folgender Voraussetzung gut funktioniert (die wir bei der RSA-Schlüsselerzeugung also besser vermeiden sollten):

Algorithmus 5.5.1 (Pollard Faktorisierung) *Angenommen ein Primfaktor p von n hat die Eigenschaft, dass $p-1$ nur kleine Primpotenzfaktoren $\leq B$ besitzt. Dann lässt sich ein Vielfaches k von $p-1 = \varphi(p)$ bestimmen, ohne p zu kennen:*

$$k := \prod_{\substack{q \text{ Primzahl} \\ l \text{ maximal mit } q^l \leq B}} q^l$$

Sei nun $1 < a < n$ beliebig gewählt. Teste zunächst, ob $\operatorname{ggT}(a, n) = 1$ (wenn nicht, haben wir einen echten Teiler gefunden). Sind a und n teilerfremd, erhalten wir einen Faktor von n als

$$\operatorname{ggT}\left(a^k - 1, n\right) > 1$$

denn k ist nach Voraussetzung ein Vielfaches von $\varphi(p)$, also $k = k' \cdot \varphi(p)$. Damit gibt der kleine Fermatsche Satz

$$a^k = \left(a^{\varphi(p)}\right)^{k'} \equiv 1 \bmod p$$

also $p \mid \operatorname{ggT}(a^k - 1, n)$. Falls wir aufgrund der Wahl von a und B keinen echten Teiler finden, ändern wir unsere Wahl.

In dem Algorithmus kann a^k modulo n berechnet werden, denn ist p ein Teiler von $a^k - 1$ und n, dann auch von $a^k - 1 + s \cdot n$ für jedes s.

Beispiel 5.5.2 *Sei* $n = 21733$ *und* $B = 10$*, also*

$$k = 2^3 \cdot 3^2 \cdot 5 \cdot 7.$$

Sei weiter $a = 2$*. Dann ist*

$$2^k - 1 \equiv 16036 \bmod n$$

und

$$\mathrm{ggT}\,(16036, n) = 211.$$

Das Verfahren hat funktioniert, da

$$210 = 2 \cdot 3 \cdot 5 \cdot 7$$

ein Teiler von k *ist.*

Sowohl 211 *also auch* $\frac{n}{211} = 103$ *sind prim, was man z.B. mit Probedivision sieht. Damit haben wir* n *vollständig faktorisiert. Man beachte, dass die gefundenen Teiler im Allgemeinen nicht prim sein müssen.*

Siehe dazu auch Übungsaufgabe 5.4.

5.6 Anwendung: Diffie-Hellman Schlüsselaustausch

Eine wesentliche Schwachstelle von RSA liegt darin, dass ein Angreifer, wenn er den privaten Schlüssel einer Person in Besitz bringt, alle an diese Person gerichteten Nachrichten lesen kann. Dies gilt auch für verschlüsselte Nachrichten der Vergangenheit, die von dem Angreifer aufgezeichnet wurden. Der Diffie-Hellman Schlüsselaustausch hat dieses Problem nicht (dies bezeichnet man als **perfect forward secrecy**), da kein privater Schlüssel verwendet wird. Man geht folgendermaßen vor:

1) Alice und Bob einigen sich auf eine zyklische Gruppe $G = \langle g \rangle$ und einen Erzeuger g.

2) Alice wählt eine zufällige ganze Zahl $0 \leq a < |G|$, berechnet

$$g^a$$

und sendet dies an Bob.

3) Bob wählt eine zufällige Zahl $0 \leq b < |G|$, berechnet

$$g^b$$

und sendet dies an Alice.

4) Alice berechnet $(g^b)^a$ und Bob berechnet $(g^a)^b$. Bob und Alice teilen dann das Geheimnis

$$\left(g^b\right)^a = (g^a)^b$$

5) Alice und Bob löschen a bzw. b.

Bemerkung 5.6.1 *Zum Entschlüsseln muss ein Angreifer aus g^b die Zahl b bestimmen. Dies nennt man auch die Berechnung eines* ***diskreten Logarithmus****.*

Das Diffie-Hellman-Verfahren basiert darauf, dass typischerweise Potenzieren schnell durchführbar ist, aber umgekehrt die Berechnung eines Logarithmus aufwändig ist. Natürlich muss $|G|$ groß genug sein, für kleine Gruppen kann man alle Möglichkeiten durchprobieren.

Bemerkung 5.6.2 *Man kann zeigen: Ist K ein endlicher Körper so ist $K^\times$ eine zyklische Gruppe. In der Praxis verwendet man unter anderem $K = \mathbb{F}_p = \mathbb{Z}/p$ für eine Primzahl p (mit etwa 1000 Dezimalstellen).*

Beispiel 5.6.3 *Sei $p = 11$ und $g = \overline{2}$. Tatsächlich ist g ein Erzeuger:*

$$(\mathbb{Z}/11)^\times = \left\langle \overline{2} \right\rangle = \{\overline{2}, \overline{4}, \overline{8}, \overline{5}, \overline{10}, \overline{9}, \overline{7}, \overline{3}, \overline{6}, \overline{1}\}.$$

Alice wählt $a = 3$ und sendet

$$\overline{2}^3 = \overline{8},$$

Bob wählt $b = 9$ und sendet

$$\overline{2}^9 = \overline{512} = \overline{6}.$$

Beide teilen nun das Geheimnis

$$\overline{8}^9 = \overline{6}^3 = \overline{7}.$$

5.7 Polynome

5.7.1 Der Polynomring

Definition 5.7.1 *Sei R ein kommutativer Ring mit 1. Der **Polynomring** $R[x]$ über R in der Unbestimmten x ist die Menge aller Ausdrücke*

$$f = a_0x^0 + a_1x^1 + ... + a_nx^n$$

mit $n \in \mathbb{N}_0$, $a_i \in R$, $a_n \neq 0$.

*Wir nennen $\deg(f) := n$ den **Grad** von f und setzen $\deg(0) = -\infty$.*

Für $i > \deg(f)$ setzen wir $a_i = 0$.
Addition und Multiplikation von Polynomen sind wie folgt definiert:

$$\begin{aligned}&\left(a_0x^0 + a_1x^1 + ... + a_nx^n\right) + \left(b_0x^0 + b_1x^1 + ... + b_mx^m\right)\\ &= \left(a_0 + b_0\right)x^0 + \left(a_1 + b_1\right)x^1 + ... + \left(a_{\max(n,m)} + b_{\max(n,m)}\right)x^{\max(n,m)}\end{aligned}$$

und

$$\begin{aligned}&\left(a_0x^0 + a_1x^1 + ... + a_nx^n\right) \cdot \left(b_0x^0 + b_1x^1 + ... + b_mx^m\right)\\ &= c_0x^0 + c_1x^1 + ... + c_{n+m}x^{n+m}\end{aligned}$$

wobei

$$c_k = \sum_{j=0}^{k} a_jb_{k-j}$$

(sind also so gemacht, dass das Distributivgesetz gilt). Polynomringe in mehr als einer Variablen definieren wir induktiv als

$$R[x_1, ..., x_r] = R[x_1, ..., x_{r-1}][x_r].$$

Als Datenstruktur ist ein Polynom vom Grad n nichts anderes als eine Liste

$$a_0x^0 + a_1x^1 + ... + a_nx^n = (a_0, ..., a_n) \in R^{n+1}.$$

Definition 5.7.2 *Ein Term ist ein Polynom der Form $a_nx^n = (0, ..., 0, a_n)$. Jeder Polynom ist offenbar eine Summe von Termen.*

Nützlich werden Polynome dadurch, dass die Rechenoperationen kompatibel mit dem Einsetzen von Werten für die Variable x sind. Es spielt dann keine Rolle ob man erst mit Polynomen rechnet und dann Werte einsetzt oder erst einsetzt und mit diesen Werten die entsprechende Rechenoperation durchführt. Auf diese Weise kann man neue Formeln herleiten, die unabhängig von dem konkreten Wert von x gültig sind.

Beispiel 5.7.3 *In* $\mathbb{Q}[X]$ *ist z.B.*

$$(x^2 + x + 1) \cdot (x + 1) = x^3 + 2x^2 + 2x + 1$$
$$(x^2 + x + 1) + (x + 1) = x^2 + 2x + 2.$$

Setzen wir den Wert $x = 2$ *in*

$$g = x^2 + x + 1$$
$$h = x + 1$$

und

$$f = g \cdot h = x^3 + 2x^2 + 2x + 1$$

ein, so erhalten wir

$$g(2) = 7$$
$$h(2) = 3$$
$$f(2) = 21$$

Wir beobachten, dass

$$f(2) = g(2) \cdot h(2).$$

Die wesentliche Eigenschaft von Polynomen ist, dass man für die Variable x Zahlen einsetzen kann und es keine Rolle spielt, ob man mit Polynomen rechnet und dann einsetzt oder erst einsetzt und dann rechnet, also für Polynome f, g und eine Zahl s gilt

$$(f + g)(s) = f(s) + g(s) \qquad (f \cdot g)(s) = f(s) \cdot g(s)$$

d.h. Einsetzen ist ein Homomorphismus.

5.7.2 Ausblick: Algebren und Einsetzen in Polynome

In diesem Abschnitt präzisieren wir, was es bedeutet, in ein Polynom einzusetzen. Dazu definiert man:

Definition 5.7.4 *Eine **R-Algebra** S ist gegeben durch einen Homomorphismus kommutativer Ringe $\varphi : R \longrightarrow S$. Man bezeichnet dann*

$$\begin{array}{ccc} R \times S & \longrightarrow & S \\ (r, s) & \longmapsto & r \cdot s := \varphi(r) \cdot s \end{array}$$

*als die **Skalarmultiplikation**.*

Beispiel 5.7.5 *Durch die Inklusion $\mathbb{Z} \subset \mathbb{C}$ ist $\mathbb{C}$ eine $\mathbb{Z}$-Algebra. Mit dem Monomorphismus*

$$R \longrightarrow R[x], \; a_0 \longmapsto a_0 x^0$$

wird $R[x]$ zu einer R-Algebra.

Ist S eine R-Algebra, d.h. gibt es eine Skalarmultiplikation $R \times S \to S$, dann können wir Elemente von S in Polynome über R einsetzen, und wegen der Rechenregel

$$(r + r') \cdot s = r \cdot s + r' \cdot s$$

(warum gilt diese?) verhält sich Einsetzen wie gewünscht:

Satz 5.7.6 *Sei R ein kommutativer Ring mit 1 und S eine R-Algebra und $s \in S$ ein Element. Dann gibt es genau einen Ringhomomorphismus*

$$\psi : R[x] \longrightarrow S$$

mit

$$x \longmapsto s,$$

*den sogenannten **Substitutionshomomorphismus** (oder Einsetzungshomomorphismus). Für $f \in R[x]$ schreiben wir dann*

$$f(s) := \psi(f) \in S$$

für das Bild von f unter dem Homomorphismus, der s für x einsetzt.

Wir bezeichnen das Bild

$$R[s] := \text{Bild}\,(\psi)$$

als den ***von s erzeugten Unterring*** *(R adjungiert s).*

Beweis. Durch

$$\psi\left(a_0x^0 + a_1x^1 + \ldots + a_nx^n\right) := a_0 + a_1s + \ldots + a_ns^n$$

ist der eindeutig bestimmte Homomorphismus gegeben. Man überprüfe als Übung, dass ψ additiv und multiplikativ und $R[s] \subset S$ ein Unterring ist. ■

Beispiel 5.7.7 *Durch Einsetzen in das Polynom $x^2 + 1 \in \mathbb{R}[x]$ erhalten wir die Polynomfunktion*

$$\begin{aligned} \mathbb{R} &\to \mathbb{R} \\ s &\mapsto s^2 + 1 \end{aligned}$$

siehe Abbildung 5.1.

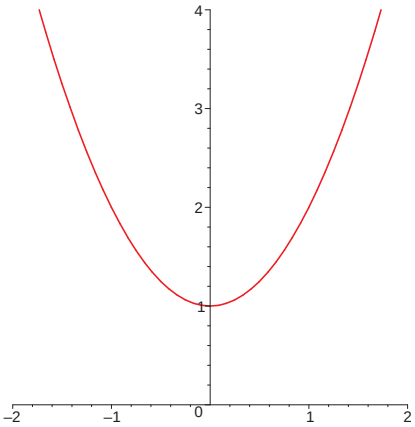


Abbildung 5.1: Polynomfunktion

5.7.3 Ausblick: Ringerweiterungen

Die erste Frage in Bezug auf Polynomfunktionen ist die nach der Existenz von Nullstellen. Das Polynom $x^2+1 \in \mathbb{Q}[x]$ hat in $\mathbb{Q}$ (oder sogar $\mathbb{R}$) keine Nullstellen. Gibt es einen Körper K mit $\mathbb{Q} \subset K$, der die Nullstellen von $x^2+1 \in \mathbb{Q}[X]$ enthält? Sicher liegen die Nullstellen $-i$ und i in den komplexen Zahlen $K = \mathbb{C}$. Allerdings ist der Körper $\mathbb{C}$, so gross, dass er sich (wie auch die reellen Zahlen $\mathbb{R}$) nicht mehr exakt auf dem Computer darstellen lässt. Können wir einen kleineren Körper K finden, mit dem wir exakt rechnen können, und der alle Nullstellen von x^2+1 enthält? In diesem Abschnitt wollen wir einen ersten Eindruck für eine Konstruktion eines solchen Körpers geben. Die wesentliche Idee ist es Ringe der Form $R[s]$ zu betrachten. Wie oben beschreiben erhalten wir durch Einsetzen eines festgelegten Elements $s \in S$ in alle Polynome in $R[x]$ einen neuen Ring

$$R \subset R[s] \subset S.$$

Beispiel 5.7.8 *Sei $d \in \mathbb{Z}$. Betrachte den Substitutionshomomorphismus*

$$\mathbb{Z}[x] \to \mathbb{C},\ x \mapsto \sqrt{d}$$

der in Polynomen mit ganzzahligen Koeffizienten x durch $\sqrt{d} \in \mathbb{C}$ ersetzt. Dann ist

$$\mathbb{Z}\left[\sqrt{d}\right] = \left\{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\right\}$$

denn wegen $\sqrt{d}^2 = d \in \mathbb{Z}$ treten nur konstante und lineare Terme in $\sqrt{d}$ auf.

Für $d = -1 = i^2$ erhält man den Ring der ***Gaußschen Zahlen***

$$\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}.$$

Der Ring der Gausschen Zahlen enthält zwar die Nullstellen von x^2+1 ist aber kein Körper, denn $\mathbb{Z}$ war schon kein Körper.

Beispiel 5.7.9 *Der aus dem Körper $\mathbb{Q}$ durch Adjunktion von i konstruierte Ring*

$$\mathbb{Q}[i] = \{a + ib \mid a, b \in \mathbb{Q}\} \subset \mathbb{C}$$

ist wieder ein Körper, denn für $a+ib \neq 0$ liegt die komplexe Zahl

$$\frac{1}{a+ib} = \frac{a-ib}{a^2+b^2} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i$$

wieder in $\mathbb{Q}[i]$. Elemente von $\mathbb{Q}[i]$ können wir exakt im Computer als Tupel $(a,b) \in \mathbb{Q}^2$ darstellen und mit ihnen rechnen.

Bemerkung 5.7.10 *Allgemein ist für Körper $K \subset L$ und $\alpha \in L$ der Ring*

$$K[\alpha]$$

wieder ein Körper, sofern es ein Polynom $0 \neq f \in K[x]$ gibt mit $f(\alpha) = 0$. Man bezeichnet $K[\alpha]$ dann als ***algebraische Körpererweiterung*** *von K. Lässt sich K exakt im Computer darstellen, dann auch $K[\alpha]$. Die dazu notwendige allgemeine Konstruktion werden wir im Abschnitt über Quotientenringe beschreiben.*

In dem Körper $\mathbb{Q}[i]$ hat x^2+1 die Nullstellen i und $-i$. Es gilt

$$x^2+1 = (x+i)\cdot(x-i).$$

Ebenso liegen z.B. für x^2+2x+2 die Nullstellen

$$x = -1 \pm i \in \mathbb{C}$$

nicht in $\mathbb{Q}$ aber in $\mathbb{Q}[i]$.

Tatsächlich besitzt jedes Polynom $f \in \mathbb{R}[x]$ in $\mathbb{C} = \mathbb{R}[i]$ eine Nullstelle, allgemeiner:

Bemerkung 5.7.11 *Der* ***Fundamentalsatz der Algebra*** *(den wir hier nicht beweisen können) besagt: Jedes Polynom $f \in \mathbb{C}[x]$ vom Grad $n = \deg(f)$ zerfällt in Linearfaktoren*

$$f = (x-c_1)\cdot\ldots\cdot(x-c_n)$$

mit $c_i \in \mathbb{C}$, hat also mit Vielfachheit gezählt genau n Nullstellen in $\mathbb{C}$.

Bemerkung 5.7.12 *Sind $c_1,\ldots,c_n \in \mathbb{C}$ die Nullstellen des Grad n Polynoms $f \in \mathbb{Q}[x]$, dann zerfällt f in dem durch iterative Adjunktion von $c_1,\ldots,c_n$ konstruierten Körper*

$$K := \mathbb{Q}[c_1,\ldots,c_n] := \mathbb{Q}[c_1][c_2]\ldots[c_n]$$

in Linearfaktoren und die Erweiterung

$$\mathbb{Q} \subset K$$

ist algebraisch, d.h. K lässt sich exakt im Computer darstellen.

5.8 Euklidische Ringe

Wir wollen nun Division mit Rest, den Euklidischen Algorithmus und die Lösung von simultanen Kongruenzen auf den Polynomring übertragen. Diese Algorithmen funktionieren völlig analog zu denen in $\mathbb{Z}$. Wir formulieren zunächst das allgemeine Prinzip dahinter:

Definition 5.8.1 *Ein **euklidischer Ring** ist ein kommutativer Ring R mit $1 \neq 0$ ohne nicht-triviale Nullteiler (d.h. 0 ist der einzige Nullteiler) mit einer Abbildung*

$$d : R\backslash\{0\} \longrightarrow \mathbb{N}_0$$

sodass für je zwei Elemente $a, b \in R\backslash\{0\}$ Elemente $g, r \in R$ existieren mit

1) $a = g \cdot b + r$ *und*

2) $r = 0$ *oder* $d(r) < d(b)$.

*Wir bezeichnen dies als **Division** von a durch b **mit Rest** r. Die Abbildung d heißt **euklidische Norm**.*

Beispiel 5.8.2 1) *$\mathbb{Z}$ ist euklidisch mit der Betragsabbildung*

$$d(n) = |n|$$

und der üblichen Division mit Rest, siehe auch Beispiel 3.3.6.

2) *Sei K ein Körper. Der Polynomring $R = K[x]$ in einer Variablen ist ein euklidischer Ring mit der Gradabbildung*

$$d(f) = \deg(f)$$

und der üblichen Polynomdivision (sukzessives Abziehen des Leitterms).

Konkretes Beispiel in $\mathbb{Q}[x]$*:*

Teilen wir $a = x^2 + \frac{1}{2}x + \frac{1}{2}$ *durch* $b = 2x - 1$ *erhalten wir*

$$\begin{array}{rcccc} x^2 + \frac{1}{2}x + \frac{1}{2} & = & (\frac{1}{2}x) \cdot (2x-1) & + & \left(x + \frac{1}{2}\right) \\ & = & \underbrace{(\frac{1}{2}x + \frac{1}{2})}_{g} \cdot (2x-1) & + & \underbrace{1}_{r} \end{array}$$

also $d(r) = 0 < 1 = d(b)$*.*

3) Mit der imaginären Einheit $i \in \mathbb{C}$ *mit* $i^2 = -1$ *ist der* ***Ring der Gaußschen Zahlen***

$$\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$$

euklidisch mit

$$\begin{aligned} d : R\backslash\{0\} &\longrightarrow \mathbb{Z}_{\geq 0} \\ d(a + i \cdot b) &= a^2 + b^2 \end{aligned}$$

(dies zeigen wir in Übung 5.21).

Analog zu Definition 3.3.1 für $\mathbb{Z}$ definiert man in jedem kommutativen Ring mit 1 einen größten gemeinsamen Teiler (ggT) und ein kleinstes gemeinsame Vielfache (kgV).

In euklidischen Ringen kann wie in $\mathbb{Z}$ den euklidische Algorithmus (Satz 3.3.5) zur Bestimmung des ggT durchgeführt werden:

Satz 5.8.3 (Euklidischer Algorithmus) *Ist* R *ein euklidischer Ring, so terminiert die sukzessive Division mit Rest von* $0 \neq a_1, a_2 \in R$ *und liefert eine Darstellung*

$$\mathrm{ggT}(a_1, a_2) = u \cdot a_1 + v \cdot a_2$$

mit $u, v \in R$*. Insbesondere existiert in Euklidischen Ringen ein ggT.*

Auf die Frage der Eindeutigkeit des ggT werden wir gleich noch zu sprechen kommen.

Beispiel 5.8.4 *Wir bestimmen den größten gemeinsamen Teiler von*

$$f = x^4 + x^3 \quad \textit{und} \quad g = x^4 - 1$$

in $\mathbb{Q}[x]$ *mit dem euklidischen Algorithmus*

$$\begin{array}{lcllcll} x^4 + x^3 & = & 1 & \cdot & (x^4 - 1) & + & (x^3+1) \\ x^4 - 1 & = & x & \cdot & (x^3 + 1) & + & (-x - 1) \\ x^3 + 1 & = & (-x^2) & \cdot & (-x - 1) & + & (-x^2 + 1) \\ & = & (-x^2 + x) & \cdot & (-x - 1) & + & (x + 1) \\ & = & (-x^2 + x - 1) & \cdot & (-x - 1) & + & 0 \end{array}$$

(die Reste sind rot markiert) und erhalten

$$\mathrm{ggT}(f, g) = -x - 1.$$

Es stellt sich wie im Fall $\mathbb{Z}$ die Frage inwieweit ggT und kgV eindeutig sind. In den ganzen Zahlen sind ggT und kgV eindeutig bis auf Vorzeichen, äquivalent bis auf Multiplikation mit den Einheiten $\mathbb{Z}^\times = \{1, -1\}$. Dies ist auch im Allgemeinen so, wie wir im nachfolgenden Abschnitt sehen werden: Der ggT und kgV sind eindeutig bis auf Multiplikation mit Einheiten aus $R^\times$ (die natürlich jedes Element von R teilen).

Beispiel 5.8.5 *In Beispiel 5.8.4 können wir also genauso schreiben*

$$\mathrm{ggT}(f, g) = x + 1.$$

Siehe auch Übungsaufgabe 5.21.

5.9 Integritätsringe und Körper

Wir erinnern uns zunächst nochmal:

Definition 5.9.1 *Sei R ein kommutativer Ring mit 1.*

1) *Ein Element $a \in R$ heißt **Nullteiler** von R, wenn ein $x \in R \backslash \{0\}$ existiert mit*

$$x \cdot a = 0.$$

2) *Hat R außer 0 keine Nullteiler und ist $1 \neq 0$, so heißt R **Integritätsring**.*

Wir bemerken, dass 0 immer ein Nullteiler ist, außer $R = \{0\}$ ist der Nullring (in diesem Fall ist 0 eine Einheit und $1 = 0$).

Bemerkung 5.9.2 *In einem Integritätsring R gilt die Kürzungsregel: Sind $a, b, c \in R$ und $c \neq 0$, dann*

$$a \cdot c = b \cdot c \Longrightarrow a = b.$$

Der Beweis ist die leichte Übung 5.10.

Bemerkung 5.9.3 *Entsprechend unserer Definition sind Euklidische Ringe also insbesondere Integritätsringe. Dies garantiert die Eindeutigkeit des ggT (und kgV) bis auf Einheiten:*

Nach unserer Definition des ggT (analog zu Definition 3.3.1), gilt für zwei größte gemeinsame Teiler d_1 und d_2, dass $d_1 \mid d_2$ und $d_2 \mid d_1$. Dies ist genau dann der Fall, wenn sich d_1 und d_2 nur um einen Einheit unterscheiden, d.h. es ein $u \in R^\times$ gibt mit

$$d_1 = u \cdot d_2$$

(äquivalent, wenn es ein $u \in R^\times$ gibt mit $d_2 = u \cdot d_1$).

Beweis. Ist $d_1 = u \cdot d_2$ mit $u \in R^\times$, dann gilt $d_1 \mid d_2$ und $d_2 \mid d_1$. Umgekehrt, gilt $d_1 \mid d_2$ und $d_2 \mid d_1$, dann gibt es $q_1, q_2 \in R$ mit

$$d_2 = d_1 \cdot q_1 \text{ und } d_1 = d_2 \cdot q_2$$

also

$$d_1 = d_1 \cdot q_1 \cdot q_2$$

und somit mit Bemerkung 5.9.2

$$q_1 \cdot q_2 = 1,$$

also $q_1, q_2 \in R^\times$. ■

Im Folgenden diskutieren wir noch an einigen Beispielen die Einheiten und Nullteiler verschiedener Ringe. Wir haben bereits gesehen, dass ein Element eines Rings nicht sowohl eine Einheit und ein Nullteiler sein kann.

Beispiel 5.9.4 *1) $\mathbb{Z}$ ist ein Integritätsring. Die Einheiten sind $+1$ und -1, also*

$$\mathbb{Z}^\times = \{+1, -1\}.$$

2) *Jeder Körper K ist ein Integritätsring, beispielsweise $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Die Einheiten sind $K^\times = K\backslash\{0\}$.*

3) *$\mathbb{Z}/6 = \{\overline{0}, \overline{1}, ...\overline{5}\}$ ist kein Integritätsring, $\overline{2}, \overline{3}, \overline{4}$ (und natürlich $\overline{0}$) sind Nullteiler, $\overline{1}$ und $\overline{5}$ sind Einheiten.*

   Siehe auch Übungsaufgabe 5.2.

4) *Ist R ein Integritätsring, dann auch $R[x]$ und*

$$R[x]^\times = R^\times,$$

   denn falls $f \cdot g = 1$, dann

$$0 = \deg(1) = \deg(f \cdot g) = \deg(f) + \deg(g)$$

   also $\deg(f) = \deg(g) = 0$. In Beispiel 5.8.4 ist also genau jedes konstante Vielfache des ggT wieder ein valider ggT.

5) *Der Ring der Gaußschen Zahlen*

$$\mathbb{Z}[i] = \{a + i \cdot b \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$$

   ist ein Integritätsring und

$$\mathbb{Z}[i]^\times = \{1, -1, i, -i\}.$$

   Offenbar sind dies Einheiten:

$$\begin{aligned} 1 \cdot 1 &= 1 \\ (-1) \cdot (-1) &= 1 \\ i \cdot (-i) &= 1 \end{aligned}$$

   Dass es keine weiteren Einheiten gibt, zeigen wir in Übungsaufgabe 5.21.

Bemerkung 5.9.5 *Für Integritätsringe R können wir analog zur Konstruktion von $\mathbb{Q}$ aus $\mathbb{Z}$ durch Bruchrechnen den* ***Quotientenkörper***

$$Q(R) = \left\{ \frac{a}{b} \mid a, b \in R,\ b \neq 0 \right\}$$

bilden, siehe Übungsaufgabe 5.12.

Beispielsweise ist für einen Körper K

$$K(x) = Q(K[x])$$

der Körper der ***rationalen Funktionen****.*

Für endliche Integritätsringe besteht keine Notwendigkeit für die Quotientenkörperkonstruktion:

Satz 5.9.6 *Jeder endliche Integritätsring ist ein Körper.*

Dies zeigen wir in Übung 5.11. Damit erhalten wir auch nochmals das Resultat aus Corollar 5.3.3:

Corollar 5.9.7 *Ist p eine Primzahl, dann ist*

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$$

ein Körper.

Beweis. Folgt direkt aus Satz 5.9.6: Ist $\overline{a}\cdot\overline{b} = \overline{0}$ für $\overline{a}, \overline{b} \in \mathbb{F}_p$ dann $p \mid ab$, also $p \mid a$ oder $p \mid b$, somit $\overline{a} = \overline{0}$ oder $\overline{b} = \overline{0}$. ∎

5.10 Ideale und Quotientenringe

In diesem Abschnitt wollen wir die Konstruktion des Rings $\mathbb{Z}/n$ verallgemeinern. Dazu untersuchen wir, inwieweit man der Quotientengruppe die Struktur eines Rings geben kann. Sei R ein kommutativer Ring mit 1. Jede Untergruppe $I \subset (R, +)$ ist ein Normalteiler, wir können also die Quotientengruppe R/I bilden und der surjektive Gruppenhomomorphismus

$$\begin{array}{rccc} \pi: & (R,+) & \longrightarrow & (R/I,+) \\ & r & \longmapsto & \overline{r} = r + I \end{array}$$

hat $\operatorname{Ker}\pi = I$ und das neutrale Element von R/I bezüglich $+$ ist $0 + I = I$.

Wollen wir auch eine Multiplikation auf R/I, sodass π ein Ringhomomorphismus ist, dann muss die Multiplikation von der Multiplikation in R induziert sein, denn

$$\overline{r_1}\cdot\overline{r_2} = \pi(r_1)\cdot\pi(r_2) = \pi(r_1 r_2) = \overline{r_1 r_2}.$$

Im Allgemeinen wird die repräsentantenweise Multiplikation jedoch nicht wohldefiniert sein. Ist $r_2' = r_2 + b$ mit $b \in I$ ein anderer Repräsentant von $r_2 + I$, dann gilt

$$r_1 \cdot r_2' = r_1 \cdot r_2 + r_1 \cdot b,$$

es sollte also $r_1 \cdot b \in I$ sein für alle $r_1 \in R$ und $b \in I$. Untergruppen von $(R, +)$ mit dieser Eigenschaft nennt man Ideale:

Definition 5.10.1 *Sei R ein kommutativer Ring mit 1. Ein* ***Ideal*** *ist eine nicht leere Teilmenge $I \subset R$ mit*

$$a + b \in I$$
$$ra \in I$$

für alle $a, b \in I$ und $r \in R$.

Wir bemerken, dass mit $a \in I$ auch das additiv Inverse $-a \in I$ ist.

Insgesamt haben wir also gezeigt (als leichte Übung folgt das Distributivgesetz in R/I direkt aus dem in R):

Satz 5.10.2 *Sei $I \subset R$ ein Ideal. Dann trägt die Quotientengruppe R/I die Struktur eines kommutativen Rings mit 1 mit repräsentantenweiser Multiplikation*

$$(r_1 + I) \cdot (r_2 + I) := r_1 r_2 + I.$$

Das neutrale Element von R/I bezüglich $\cdot$ ist $1+I$. Wir bezeichnen R/I als ***Quotientenring*** *von R nach I.*

Ideale spielen also eine wichtige Rolle in der Ringtheorie.

Beispiel 5.10.3 *1) Sind $I_1, I_2 \subset R$ Ideale, dann auch deren Durchschnitt $I_1 \cap I_2$.*

2) Seien $a_1, ..., a_n \in R$. Dann ist

$$(a_1, ..., a_n) := \{\textstyle\sum_{i=1}^{n} r_i a_i \mid r_i \in R\}$$

ein Ideal, das von von dem ***Erzeugendensystem*** *$a_1, ..., a_n$ erzeugte Ideal.*

3) In Abschnitt 5.1 haben wir schon bewiesen: Die Ideale von $\mathbb{Z}$ sind genau die Untergruppen

$$n\mathbb{Z} = \{na \mid a \in \mathbb{Z}\} = (n)$$

mit $n \in \mathbb{Z}$.

Für das Ideal $I = n\mathbb{Z} \subset \mathbb{Z}$ erhalten wir wieder aus Satz 5.10.2, dass $\mathbb{Z}/n\mathbb{Z}$ ein kommutativer Ring mit 1 ist. Die Elemente sind genau die Restklassen $\bar{0}, \bar{1}, ..., \overline{n-1}$, d.h.

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/n.$$

4) Sei $\varphi : R \longrightarrow S$ ein Ringhomomorphismus. Der Kern

$$\operatorname{Ker}\varphi = \{r \in R \mid \varphi(r) = 0\} \subset R$$

ist ein Ideal, denn ist $r' \in R$ und $\varphi(r) = 0$, so auch

$$\varphi(r' \cdot r) = \varphi(r') \cdot \varphi(r) = 0$$

Wie für Gruppen gilt dann:

Satz 5.10.4 (Homomorphiesatz) *Sei $\varphi : R \longrightarrow S$ ein Ringhomomorphismus. Dann gilt*

$$R/\operatorname{Ker}\varphi \cong \operatorname{Bild}\varphi$$

Beweis. Aus Satz 4.3.11 erhalten wir einen Isomorphismus

$$\begin{aligned} \widetilde{\varphi} : R/\operatorname{Ker}\varphi &\longrightarrow \operatorname{Bild}\varphi \\ \overline{r} = r + \operatorname{Ker}\varphi &\longmapsto \varphi(r) \end{aligned}$$

der additiven abelschen Gruppen. Weiter ist $\widetilde{\varphi}$ ein Ringhomomorphismus, denn

$$\begin{aligned} &\widetilde{\varphi}(\overline{r_1} \cdot \overline{r_2}) = \widetilde{\varphi}(\overline{r_1 \cdot r_2}) = \varphi(r_1 \cdot r_2) \\ &= \varphi(r_1) \cdot \varphi(r_2) = \widetilde{\varphi}(\overline{r_1}) \cdot \widetilde{\varphi}(\overline{r_2}) . \end{aligned}$$

■

Bemerkung 5.10.5 *Sei K ein Körper und*

$$\begin{array}{rccc} \chi : & \mathbb{Z} & \longrightarrow & K \\ & n & \longmapsto & n \cdot 1_K \end{array}$$

die charakteristische Abbildung. Der Kern ist ein Ideal

$$\operatorname{Ker}\chi = p\mathbb{Z}$$

mit $p \geq 0$. Man nennt

$$\operatorname{char}(K) = p \geq 0$$

*die **Charakteristik** von K. Zwei Fälle können auftreten:*

1) $p = 0$, d.h. χ ist injektiv. In diesem Fall ist $\mathbb{Z}$ und damit auch $\mathbb{Q}$ ein Unterring von K.

2) $p > 0$. *Dann ist*

$$\mathbb{Z}/p\mathbb{Z} \to K$$

nach dem Homomorphiesatz 5.10.4 injektiv, also $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ *ein Unterring von* K *und damit ein Integritätsring. Somit muss* p *eine Primzahl sein, denn wäre* $p = a \cdot b$ *mit* $a, b > 1$, *dann* $\bar{a} \cdot \bar{b} = \bar{0}$, *also* $\bar{a}, \bar{b} \neq \bar{0}$ *Nullteiler.*

Jeder Körper enthält also entweder $\mathbb{Q}$ *oder* $\mathbb{F}_p$.

Bemerkung 5.10.6 *Man kann zeigen, dass es bis auf Isomorphie zu jeder Primzahlpotenz* p^r *genau einen Körper* K *mit* $|K| = p^r$ *Elementen gibt. Dieser wird als* $\mathbb{F}_{p^r}$ *bezeichnet. Er hat* $\operatorname{char}(\mathbb{F}_{p^r}) = p$. *Siehe auch Aufgabe 5.9, wo wir einen Körper mit* 4 *Elementen konstruieren.*

Vorsicht: Für $r > 1$ *ist* $\mathbb{F}_{p^r} \neq \mathbb{Z}/p^r$, *etwa ist*

$$\mathbb{F}_4 \neq \mathbb{Z}/4$$

denn $\bar{2} \cdot \bar{2} = \bar{0} \in \mathbb{Z}/4$, *d.h.* $\mathbb{Z}/4$ *ist kein Integritätsring. Allgemein wird* $\mathbb{F}_{p^r}$ *als algebraische Körpererweiterung von* $\mathbb{F}_p$ *konstruiert.*

5.11 Hauptidealringe und Faktorielle Ringe

Genau wie Ideale in $\mathbb{Z}$, haben Ideale in einem Euklidischen Ring R eine besonders einfache Struktur: Die Elemente eines Ideals sind genau die R-Vielfachen eines einzigen Elements des Ideals.

Definition 5.11.1 *Sei* R *ein Integritätsring. Ist jedes Ideal von* R *von einem einzigen Element erzeugt, so heißt* R ***Hauptidealring***.

Ideale der Form

$$I = (a) = \{a \cdot r \mid r \in R\},$$

in einem beliebigen kommutativen Ring R bezeichnet man auch als **Hauptideale**.

Satz 5.11.2 *Euklidische Ringe sind Hauptidealringe.*

Beweis. Sei (R, d) ein euklidischer Ring und $I \subset R$ ein Ideal. Das Ideal $I = (0)$ ist ein Hauptideal. Falls $I \neq (0)$ betrachten wir $b \in I \backslash \{0\}$ mit $d(b)$ minimal.

Sei $a \in I$ beliebig und $a = g \cdot b + r$ mit $r = 0$ oder $d(r) < d(b)$. Da mit a und b auch $r \in I$ ist, muss $r = 0$ sein, denn sonst hätten wir ein Element kleinerer Norm gefunden. Also ist $a \in (b)$. Damit folgt $I \subset (b) \subset I$. ■

Beispiel 5.11.3 *Insbesondere sind $\mathbb{Z}$ und $\mathbb{Q}[x]$ Hauptidealringe.*

Ohne Beweis bemerken wir:

Satz 5.11.4 *Hauptidealringe sind **faktoriell**, d.h. es gibt eine bis auf Einheiten eindeutige Primfaktorisierung (ohne Beweis). Insbesondere existiert der ggT und ist bis auf Einheiten eindeutig.*

Beispiel 5.11.5 *In $\mathbb{Z}$ ist*

$$\mathrm{ggT}(2^2 \cdot 5^3,\ 2^3 \cdot 5) = 2^2 \cdot 5,$$

in $\mathbb{Q}[x]$ ist

$$\mathrm{ggT}(x^4+x^3, x^4-1) = \mathrm{ggT}(x^3 \cdot (x+1),\ (x^3-x^2+x-1) \cdot (x+1)) = x+1.$$

Diesen ggT haben wir in Beispiel 5.8.4 auch schon mit dem Euklidischen Algorithmus berechnet.

Mit Hilfe des ggT können wir zu jedem Ideal einen Erzeuger angeben:

Bemerkung 5.11.6 *Ist R ein Hauptidealring, dann gilt*

$$(a_1, a_2) = (\,\mathrm{ggT}\,(a_1, a_2)\,).$$

Beweis. Da R ein Hauptidealring ist, existiert ein $d \in R$ mit

$$(a_1, a_2) = (d),$$

also $d \mid a_i$. Weiter gibt es $u, v \in R$ mit

$$d = ua_1 + va_2.$$

Somit ist jeder Teiler von allen a_i schon ein Teiler von d, also

$$d = \mathrm{ggT}\,(a_1, a_2)\,.$$

■

Für mehr als zwei Erzeuger geht man induktiv vor.

Beispiel 5.11.7 *1) In $\mathbb{Z}$ gilt*

$$(6, 10) = (2).$$

2) In $\mathbb{Q}[x]$ gilt mit dem oben bestimmten ggT

$$(x^4 + x^3,\ x^4 - 1) = (x + 1).$$

Wir fassen die Beziehungen zwischen den verschiedenen Ringklassen zusammen: {Euklidische Ringe} $\subset$ {Hauptidealringe} $\subset$ {Faktorielle Ringe} $\subset$ {Integritätsringe}, und dies sind echte Inklusionen:

Beispiel 5.11.8 *Der Ring $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ ist ein Hauptidealring, aber kein euklidischer Ring (ohne Beweis).*

Beispiel 5.11.9 *Der Ring $\mathbb{Z}[x]$ ist kein Hauptidealring (siehe auch Übungsaufgabe 5.15), aber faktoriell:*

Satz 5.11.10 (Satz von Gauß) *Sei R ein Integritätsring. Dann gilt*

$$R \text{ faktoriell} \iff R[x] \text{ faktoriell}$$

(ohne Beweis).

Beispiel 5.11.11 *Der Integritätsring*

$$R = K\,[x, y, z, w]\,/(xy - zw)$$

ist nicht faktoriell, denn

$$\bar{x}\bar{y} = \bar{z}\bar{w}.$$

5.12 Chinesischer Restsatz

Wir wollen nun das Lösen von simultanen Kongruenzen, das wir in Kapitel 3 über dem Ring der ganzen Zahlen kennengelernt haben, allgemein für einen kommutativen Ring R mit 1 betrachten. Für ganze Zahlen gilt

$$x \equiv a \bmod n \iff \overline{x} = \overline{a} \in \mathbb{Z}/n\mathbb{Z} \iff x - a \in n\mathbb{Z}.$$

Dabei ist $n\mathbb{Z} \subset \mathbb{Z}$ ein Ideal. Nach Satz 5.10.2 können wir den Quotientenring von R nach einem beliebigen Ideal I bilden, das heißt modulo I rechnen. Deshalb liegt es nahe, den Chinesischen Restsatz auf Kongruenzen modulo Idealen zu verallgemeinern. Wollen wir jedoch eine Lösung algorithmisch bestimmen, so bleiben wir auf Euklidische Ringe beschränkt.

Zunächst formulieren wir Teilerfremdheit für Ideale.

Definition 5.12.1 *Sind $I_1, I_2 \subset R$ Ideale, dann sind die* ***Summe***

$$I_1 + I_2 = \{a + b \mid a \in I_1, b \in I_2\} \subset R$$

und der ***Durchschnitt***

$$I_1 \cap I_2 \subset R$$

wieder Ideale.

Zwei Ideale I_1 und I_2 heißen ***coprim****, wenn*

$$I_1 + I_2 = R.$$

Man beachte, dass $R = (1)$.

Beispiel 5.12.2 *Ist R ein Hauptidealring und $a_1, a_2 \in R$, dann*

$$\begin{aligned}(a_1) + (a_2) &= (\operatorname{ggT}(a_1, a_2))\\ (a_1) \cap (a_2) &= (\operatorname{kgV}(a_1, a_2)).\end{aligned}$$

Insbesondere gilt

$$(a_1) \text{ und } (a_2) \text{ coprim} \iff \operatorname{ggT}(a_1, a_2) = 1.$$

Beweis. Die erste Aussage folgt sofort aus Bemerkung 5.11.6, da $(a_1) + (a_2) = (a_1, a_2)$.

Für die zweite Aussage schreibe das Ideal

$$(a_1) \cap (a_2) = (m)$$

mit $m \in R$. Einerseits gilt $m \in (a_i)$ d.h. $a_i \mid m \ \forall i$. Andererseits ist m das kleinste gemeinsame Vielfache: Angenommen $a_i \mid \tilde{m}$ d.h. $\tilde{m} \in (a_i) \ \forall i$, dann

$$\tilde{m} \in (a_1) \cap (a_2) = (m)$$

also $m \mid \tilde{m}$. Damit ist

$$m = \mathrm{kgV}\,(a_1, a_2)\,.$$

■

Satz 5.12.3 (Chinesischer Restsatz) *Sei R ein kommutativer Ring mit 1 und $I_1, \ldots, I_t$ paarweise coprime Ideale. Dann ist der Ringhomomorphismus*

$$\begin{array}{rccc} \varphi: & R & \longrightarrow & R/I_1 \times \ldots \times R/I_t \\ & r & \longmapsto & (r + I_1, \ldots, r + I_t) \end{array}$$

surjektiv und hat Kern

$$\mathrm{Ker}\,\varphi = I_1 \cap \ldots \cap I_t$$

(ohne Beweis). Mit dem Homomorphiesatz 5.10.4 gilt damit

$$\begin{array}{c} R/\,(I_1 \cap \ldots \cap I_t) \cong R/I_1 \times \ldots \times R/I_t \\ r + (I_1 \cap \ldots \cap I_t) \longmapsto (r + I_1, \ldots, r + I_t) \end{array}$$

Als Corollar zu Satz 5.12.3 erhalten wir für den Fall $R = \mathbb{Z}$ wieder Satz 5.3.8:

Corollar 5.12.4 (Chinesischer Restsatz über $\mathbb{Z}$) *Sind $n_1, \ldots, n_t \in \mathbb{Z}_{>0}$ paarweise teilerfremd, dann gilt*

$$\begin{array}{c} \mathbb{Z}/(n_1 \cdot \ldots \cdot n_t) \cong \mathbb{Z}/(n_1) \times \ldots \times \mathbb{Z}/(n_t) \\ \bar{r} \longmapsto (\bar{r}, \ldots, \bar{r}) \end{array}$$

Beweis. Mit Beispiel 5.12.2 folgt: Die Ideale $I_j = (n_j) \subset \mathbb{Z}$ sind coprim, denn für $i \neq j$ ist

$$(n_i) + (n_j) = (\operatorname{ggT}(n_i, n_j)) = (1) = \mathbb{Z}.$$

Außerdem ist

$$(n_1) \cap \ldots \cap (n_t) = (\operatorname{kgV}(n_1, \ldots, n_t)) = (n_1 \cdot \ldots \cdot n_t).$$

■

Mit dem Euklidischen Algorithmus kann man analog zum Fall $R = \mathbb{Z}$ simultane Kongruenzen auch über $R = K[x]$ lösen:

Beispiel 5.12.5 *Wir bestimmen die Lösungsmenge $L \subset \mathbb{Q}[x]$ der simultanen Kongruenzen*

$$f \equiv 3 \bmod (x+1)$$
$$f \equiv 2 + x \bmod \left(x^2 + x + 1\right)$$

das heißt wir suchen alle Polynome f, sodass $f-3$ ein Vielfaches von $x+1$ und $f-(2+x)$ ein Vielfaches von x^2+x+1 ist. Mit dem Euklidischen Algorithmus erhalten wir, dass $x+1$ und x^2+x+1 teilerfremd sind, und

$$\operatorname{ggT}(x+1, x^2+x+1) = 1 = \qquad (-x)\cdot(x+1) \; + \quad 1 \cdot (x^2+x+1)$$

Weiter ist $\qquad -x^3 + x + 3 = \; (2+x)\cdot(-x)\cdot(x+1) \; + \; 3 \cdot 1 \cdot (x^2+x+1)$

eine Lösung der simultanen Kongruenzen (analog zur Lösungsformel in $\mathbb{Z}$ aus Kapitel 3) und somit

$$\begin{aligned} L \quad &= \{-x^3 + x + 3 \quad + \quad g \cdot (x^3 + 2x^2 + 2x + 1) \mid g \in \mathbb{Q}[x]\} \\ &= -x^3 + x + 3 \quad + \quad (x^3 + 2x^2 + 2x + 1) \\ &= 2x^2 + 3x + 4 \quad + \quad (x^3 + 2x^2 + 2x + 1) \end{aligned}$$

denn die Lösung ist nur eindeutig bis auf Vielfache von

$$(x+1)\cdot(x^2+x+1) = x^3 + 2x^2 + 2x + 1.$$

Insbesondere können wir eine eindeutige Lösung $2x^2+3x+4$ von Grad < 3 durch Division mit Rest von $-x^3+x+3$ nach x^3+2x^2+2x+1 finden:

$$-x^3 + x + 3 = (-1)\cdot(x^3 + 2x^2 + 2x + 1) + 2x^2 + 3x + 4$$

Anders formuliert, der Chinesische Restsatz gibt den Isomorphismus

$$\mathbb{Q}[x]/((x+1)\cdot(x^2+x+1)) \cong \mathbb{Q}[x]/(x+1) \times \mathbb{Q}[x]/(x^2+x+1)$$

unter dem die Lösungsmenge L der simultanen Kongruenzen das eindeutige Urbild von $\left(\overline{3},\ \overline{2+x}\right)$ ist, d.h.

$$L = \overline{2x^2+3x+4} \longmapsto \left(\overline{3},\ \overline{2+x}\right).$$

Siehe auch Übung 5.18.

5.13 Anwendung: Modulares Rechnen

Mit Hilfe des Chinesischen Restsatzes lassen sich viele Algorithmen mit ganzzahligem Input und Output beschleunigen.

Bemerkung 5.13.1 *Der Rechenaufwand der Multiplikation in $\mathbb{Z}$ steigt stärker als linear mit der Bitlänge der Zahlen. Deshalb zerlegt man mit dem Chinesischen Restsatz das Problem in kleinere: Zum Rechnen mit Zahlen $z \in \mathbb{Z}$ mit $|z| < C$ wählt man ein $n = n_1 \cdot \ldots \cdot n_r > 2C$ mit n_i paarweise teilerfremd und alle n_i etwa gleich groß und rechnet in*

$$\mathbb{Z}/n_1 \times \ldots \times \mathbb{Z}/n_r \cong \mathbb{Z}/n$$

ersetzt also eine Operation der Bitlänge N durch r Operationen der Bitlänge $\frac{N}{r}$.

Das Verfahren erlaubt auch die Parallelisierung des Problems, denn die einzelnen Rechnungen in $\mathbb{Z}/n_i$ sind voneinander völlig unabhängig.

Paralleles Rechnen gewinnt an Bedeutung, da Leistungssteigerungen bei Prozessoren zunehmend durch eine größere Zahl von Kernen erreicht werden.

In der Praxis werden für die Multiplikation andere Verfahren verwendet, die jedoch auch auf dem Chinesischen Restsatz beruhen.

Beispiel 5.13.2 *Zur Berechnung von* $32 \cdot 45$ *betrachten wir*

$$\begin{array}{ccccccccccccc}
\mathbb{Z} & \to & \mathbb{Z}/2310 & \cong & \mathbb{Z}/2 & \times & \mathbb{Z}/3 & \times & \mathbb{Z}/5 & \times & \mathbb{Z}/7 & \times & \mathbb{Z}/11 \\
32 & \mapsto & \overline{32} & \mapsto & (\,\overline{0} & , & \overline{2} & , & \overline{2} & , & \overline{4} & , & \overline{10}\,) \\
 & & & & & & & & \cdot & & & & \\
45 & \mapsto & \overline{45} & \mapsto & (\,\overline{1} & , & \overline{0} & , & \overline{0} & , & \overline{3} & , & \overline{1}\,) \\
 & & & & & & & & = & & & & \\
 & & \overline{1440} & \mapsto & (\,\overline{0} & , & \overline{0} & , & \overline{0} & , & \overline{5} & , & \overline{10}\,)
\end{array}$$

Dabei ist $\overline{1440} = 1440 + 2310\mathbb{Z}$ *die Lösungsmenge der simultanen Kongruenzen*

$$\begin{aligned}
x &\equiv 0 \bmod 2 \\
x &\equiv 0 \bmod 3 \\
x &\equiv 0 \bmod 5 \\
x &\equiv 5 \bmod 7 \\
x &\equiv 10 \bmod 11
\end{aligned}$$

Somit erhalten wir

$$32 \cdot 45 = 1440,$$

wobei das Ergebnis nur korrekt bis auf Addition von Vielfachen von 2310 *ist. Man muss also n groß genug wählen, um das korrekte ganzzahlige Ergebnis zu erhalten.*

Die Kongruenz lässt sich in MAPLE *lösen mit:*

```
chrem([0,0,0,5,10], [2,3,5,7,11]);
1440
```

5.14 Anwendung: Interpolation

Eine andere zentrale Anwendung des Chinesischen Restsatzes ist die Interpolation von vorgegebenen Funktionswerten an vorgegebenen Stützstellen durch Polynome. Die wesentliche Idee ist dabei folgende:

Bemerkung 5.14.1 *Für ein Polynom* $f \in K[x]$ *und* $t, c \in K$ *ist die Bedingung*

$$f(t) = c$$

äquivalent zu der Kongruenz

$$f \equiv c \bmod (x - t)$$

Beweis. Letzteres bedeutet, dass es ein $q \in K[x]$ gibt mit

$$f = q \cdot (x - t) + c$$

also folgt $f(t) = q(t) \cdot 0 + c = c$.

Umgekehrt, ist $f(t) = c$ und schreiben wir $f = q \cdot (x - t) + d$ mit Division mit Rest und einer Konstanten d, dann gilt $c = f(t) = q(t) \cdot 0 + d = d$. ■

Wir können also das Interpolationsproblem als ein System simultaner Kongruenzen formulieren. Die Existenz einer Lösung und den maximal notwendigen Grad des Lösungspolynoms f erhalten wir aus dem Chinesischen Restsatz, denn es gibt ein $q \in K[x]$ mit $f = q \cdot (x - t) + c$ genau dann, wenn $\overline{f} = \overline{c} \in K[x]/(x-t)$.

Satz 5.14.2 (Lagrange-Interpolation) *Sei K ein Körper. Sind $t_1, ..., t_k \in K$ paarweise verschiedene Stützstellen und $c_1, ..., c_k \in K$, dann gibt es genau ein Polynom $f \in K[x]$ mit* $\deg f < k$ *und*

$$f(t_i) = c_i \ \forall i.$$

Beweis. Es gilt für alle $i \neq j$, dass

$$1 \in (t_i - t_j) \text{ und } t_i - t_j \in (x - t_i) + (x - t_j)$$

also

$$K[x] = (1) \subset (t_i - t_j) \subset (x - t_i) + (x - t_j) \subset K[x]$$

d.h.

$$(x - t_i) + (x - t_j) = K[x].$$

Somit liefert der Chinesische Restsatz

$$K[x] / \left(\prod_{i=1}^{k} (x - t_i)\right) \cong K[x]/(x-t_1) \times ... \times K[x]/(x-t_k) \cong K^k$$

also existiert ein eindeutiges Urbild $\overline{g}$ mit

$$\overline{g} \longmapsto (\overline{c_1}, ..., \overline{c_k}).$$

Dabei ist g eine Lösung der simultanen Kongruenzen

$$g \equiv c_i \bmod (x - t_i) \ \forall i,$$

Nach Bemerkung 5.14.1 gilt also $g(t_i) = c_i \ \forall i$.
Division mit Rest

$$g = q \cdot \prod_{i=1}^{k} (x - t_i) + f$$

gibt ein eindeutiges $f \in \overline{g}$ mit $\deg(f) < k$. Weiter ist $g(t_i) = f(t_i)$ $\forall i$. ■

Beispiel 5.14.3 *Wir suchen das eindeutige Polynom $f \in \mathbb{R}[x]$ vom Grad 1 mit*

$$f(-1) = 1$$
$$f(1) = 2$$

Der erweiterte Euklidische Algorithmus liefert

$$1 = \frac{1}{2} \cdot (x + 1) + (-\frac{1}{2}) \cdot (x - 1)$$

also ist

$$f = 2 \cdot \frac{1}{2} \cdot (x + 1) + 1 \cdot (-\frac{1}{2}) \cdot (x - 1) = \frac{1}{2}x + \frac{3}{2}$$

siehe Abbildung 5.2.

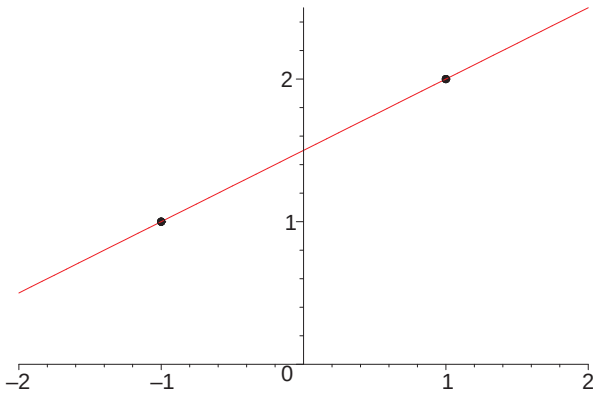


Abbildung 5.2: Interpolation

Division mit Rest der Lösung nach $(x+1)(x-1)$ ist in diesem Beispiel nicht nötig, da die Lösung schon Grad 1 hat.

Da alle Moduli von der speziellen Form $x - t_i$ sind, können wir sogar eine Lösungsformel für f angeben, müssen also nicht immer die Kongruenzen neu lösen:

Bemerkung 5.14.4 *Mit den* ***Lagrangepolynomen***

$$f_i = \prod_{\substack{j=1 \\ j \neq i}}^{k} \frac{x - t_j}{t_i - t_j}$$

ist

$$\begin{aligned} f_i &\equiv 1 \bmod (x - t_i) \\ f_i &\equiv 0 \bmod (x - t_j) \quad \text{für } j \neq i \end{aligned}$$

also erhalten wir f direkt als

$$f = \sum_{i=1}^{k} c_i f_i.$$

Man beachte: Will man das Interpolationsproblem mehrfach für dieselben t_i, aber verschiedene c_i lösen, so müssen die f_i nur einmal bestimmt werden.

Beispiel 5.14.5 *Wollen wir zum Beispiel ein Polynom $f \in \mathbb{R}[x]$ finden mit*

$$f(-1) = 1,\ f(0) = 0,\ f(2) = 1$$

müssen wir nur

$$\begin{aligned} f &= 1 \cdot \frac{(x-0)(x-2)}{(-1-0)(-1-2)} + 0 \cdot \frac{(x+1)(x-2)}{(0+1)(0-2)} + 1 \cdot \frac{(x+1)(x-0)}{(2+1)(2-0)} \\ &= \frac{1}{3}\left(x^2 - 2x\right) + \frac{1}{6}\left(x^2 + x\right) \\ &= \frac{1}{2}x^2 - \frac{1}{2}x \end{aligned}$$

berechnen. Abbildung 5.3 zeigt den Graphen der Funktion $\mathbb{R} \to \mathbb{R}$, $x \mapsto f(x)$.

In MAPLE *ist die Lagrange-Interpolation implementiert in dem Befehl* `interp`*:*

```
f:=interp([-1,0,2],[1,0,1],x);
```

$f = \frac{1}{2}x^2 - \frac{1}{2}x$

Den Funktionsgraphen können wir plotten durch:

```
plot(f,x=-2..2);
```

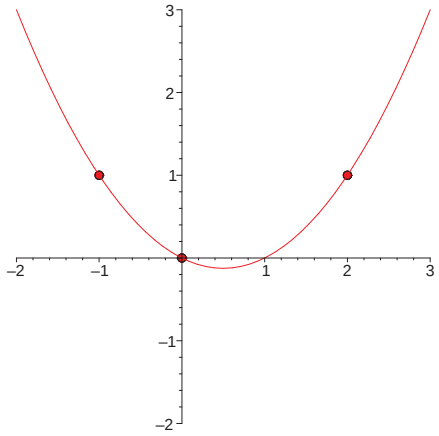


Abbildung 5.3: Interpolation

5.15 Übungsaufgaben

Übung 5.1 *Sei R ein Ring. Zeigen Sie durch Verwendung der Ringaxiome, dass für alle $x, y \in R$ gilt*

$$\begin{aligned} 0x = x0 &= 0 \\ (-x)\,y = x\,(-y) &= -xy \\ (-x)\,(-y) &= xy \end{aligned}$$

Übung 5.2 *Stellen Sie die Verknüpfungstafeln der Multiplikation und Addition des Rings $\mathbb{Z}/10\mathbb{Z}$ auf. Welche Elemente von $\mathbb{Z}/10\mathbb{Z}$ sind Einheiten und welche Nullteiler? Geben Sie auch die Gruppentafel der Einheitengruppe $(\mathbb{Z}/10\mathbb{Z})^\times$ an.*

Können Sie ein Kriterium formulieren, wann ein Element von $\mathbb{Z}/n\mathbb{Z}$ eine Einheit oder ein Nullteiler ist?

Übung 5.3 *Der öffentliche RSA-Schlüssel von Alice ist*

$$\begin{aligned} n_A &= 18644474572985789975837398427254139850324935 1... \\ &\quad ...26641700069973864213317227128326512480310245 9 \\ e_A &= 2^{16} + 1 \end{aligned}$$

Bob hat eine verschlüsselte Nachricht

$$\begin{aligned} c = 15917814291607767775764814768751952354004527 6... \\ ...15745611347067309751477522997699596869819091 4 \end{aligned}$$

an Alice geschickt. Was war der Inhalt der Nachricht?

Hinweise: Alice hat ungeschickterweise einen Primfaktor p von $n_A = p \cdot q$ so gewählt, dass $\varphi(p)$ nur Primpotenzfaktoren ≤ 200000 hat.

Mit MAPLE *lässt sich $a^b \bmod n$ für $a, b, n \in \mathbb{N}$ effizient berechnen durch*

```
Power(a,b) mod n
```

Testen Sie, ob auch die MAPLE*-Funktion* `ifactor` *zum Ziel führt.*

Übung 5.4 *1) Implementieren Sie das Faktorisierungsverfahren von Pollard.*

2) Testen Sie Ihre Implementierung an Beispielen, insbesondere auch an Aufgabe 5.3.

Übung 5.5 *Seien $a, b, n \in \mathbb{N}$ und*

$$b = b_0 2^0 + b_1 2^1 + b_2 2^2 + \ldots$$

mit $b_i \in \{0, 1\}$ die Darstellung von b als Binärzahl.

1) Implementieren Sie ein effizientes Verfahren zu Berechnung von

$$a^b \bmod n$$

durch sukzessives Quadrieren.

2) Testen Sie Ihre Implementierung an Beispielen, insbesondere auch an Aufgabe 5.3.

Übung 5.6 *Der Fermatsche Primzahltest: Eine Zahl $n \in \mathbb{N}$ heißt* ***Fermatsche Pseudoprimzahl*** *zur Basis $a \in \mathbb{N}$, wenn n nicht prim ist, aber dennoch $a^{n-1} \equiv 1 \bmod n$ gilt.*

Bestimmen Sie mit Computerhilfe jeweils alle Pseudoprimzahlen $n \leq 1000$ zur Basis a mit $a = 2, 3, 5$ und vergleichen Sie deren Anzahl mit der Anzahl der Primzahlen.

Hinweis: MAPLE*-Funktionen* `nextprime` *und* `mod`*.*

Übung 5.7 *Sei $q \in \mathbb{Z}_{\geq 2}$. Für ein $a \in \mathbb{Z}$ gelte $a^{q-1} \equiv 1 \bmod q$ und $a^{\frac{q-1}{p}} \not\equiv 1 \bmod q$ für jeden Primteiler p von $q - 1$. Zeigen Sie, dass dann q prim ist.*

Übung 5.8 *Sei K ein Körper.*

1) *Zeigen Sie: Die Menge der Polynome $K[x]$ mit Koeffizienten in K ist mit der Addition und Multiplikation aus Definition 5.7.1 ein Integritätsring.*

2) *Implementieren Sie die Addition und Multiplikation in $K[x]$.*

Übung 5.9 *Zeigen Sie, dass es einen Körper K mit genau 4 Elementen gibt, indem Sie die Verknüpfungstafeln der Addition und Multiplikation aufstellen.*

Hinweis: Bezeichnen Sie die Elemente von K als $0, 1, a, a+1$.

Übung 5.10 *In einem Integritätsring R gilt die Kürzungsregel: Sind $a, b, c \in R$ und $c \neq 0$, dann*

$$a \cdot c = b \cdot c \Longrightarrow a = b.$$

Übung 5.11 *Zeigen Sie:*

1) *Jeder Integritätsring mit endlich vielen Elementen ist ein Körper.*

2) *In einem endlichen Ring (kommutativ mit 1) ist jedes Element entweder eine Einheit oder ein Nullteiler.*

Übung 5.12 *Sei R ein Integritätsring und $S = R\backslash\{0\}$. Wir konstruieren den Ring von Brüchen*

$$Q(R) = \left\{ \frac{r}{s} \mid r \in R,\ s \in S \right\}$$

als $Q(R) = (R \times S) / \sim$ mit der Äquivalenzrelation

$$(r, s) \sim (r', s') \Leftrightarrow rs' - sr' = 0$$

und schreiben $\frac{r}{s} := [(r, s)]$. Addition und Multiplikation sind gegeben durch

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1 s_2 + r_2 s_1}{s_1 s_2}$$
$$\frac{r_1}{s_1} \cdot \frac{r_2}{s_2} = \frac{r_1 r_2}{s_1 s_2}$$

1) *Zeigen Sie: Addition und Multiplikation sind wohldefiniert und $Q(R)$ ist ein Körper.*

2) *Implementieren Sie die Arithmetik in $\mathbb{Q} = Q(\mathbb{Z})$, d.h. Addition, Multiplikation, Inverse, eine Funktion zur Entscheidung von Gleichheit, und eine Funktion, die für jedes Element einen gekürzten Repräsentanten bestimmt.*

3) *Können Sie Ihre Implementierung so modifizieren oder verallgemeinern, dass sie auch für den Körper der rationalen Funktionen $\mathbb{Q}(X) = Q(\mathbb{Q}[X])$ funktioniert?*

Übung 5.13 *Sei R ein Integritätsring. Zeigen Sie:*

1) *Für $a, b, c \in R$, $c \neq 0$ folgt aus $ac = bc$, dass schon $a = b$.*

2) *Für alle $a \in R$ gilt $a \mid 0$ und $a \mid a$ und $1 \mid a$.*

3) *Seien $a, b, c \in R$. Gilt $c \mid b$ und $b \mid a$, dann $c \mid a$.*

4) *Ist $a \in R$ und $u \in R^\times$ und $a \mid u$, dann ist $a \in R^\times$.*

5) *Seien $a, b, d \in R$ mit $d \mid a$ und $d \mid b$. Dann gilt $d \mid (xa + yb)$ für alle $x, y \in R$.*

6) *Seien $a, b \in R$. Dann ist $(a) \subset (b) \iff b \mid a$.*

7) *Sind $a, b \in R$, so gilt*

$$a \mid b \text{ und } b \mid a \iff \exists u \in R^\times \text{ mit } a = ub \iff (a) = (b)$$

Man sagt dann, a und b sind assoziiert.

Dies ist eine Äquivalenzrelation.

Übung 5.14 *Sei K ein Körper. Zeigen Sie, dass $K[x, y]$ kein Hauptidealring ist.*
Hinweis: Betrachten Sie das Ideal $(x, y) \subset K[x, y]$.

Übung 5.15 *Zeigen Sie, dass $\mathbb{Z}[x]$ kein Hauptidealring ist.*
Hinweis: Betrachten Sie das Ideal $(2, x)$.

Übung 5.16 *Sei $\mathbb{F}_2$ der Körper mit den zwei Elementen 0 und 1. Bestimmen Sie alle Elemente von*

$$K = \mathbb{F}_2[x]/(x^2 + x + 1)$$

und die Additions- und Multiplikationstabelle von K. Zeigen Sie, dass K ein Körper ist.

Übung 5.17 *Bestimmen Sie in $\mathbb{Q}[x]$ den größten gemeinsamen Teiler $\mathrm{ggT}(f,g)$ von*

$$f = x^2 + 2x + 1 \qquad g = x^2 - 2x + 1$$

und $a, b \in \mathbb{Q}[x]$ mit

$$\mathrm{ggT}(f,g) = a \cdot f + b \cdot g.$$

Überprüfen Sie Ihr Ergebnis mit dem MAPLE*-Befehl* `gcdex`*.*

Übung 5.18 *Bestimmen Sie die Menge $L \subset \mathbb{R}[x]$ aller Lösungen f der simultanen Kongruenzen*

$$f \equiv 2 + 3(x-1) \bmod (x-1)^2$$
$$f \equiv 1 + 2(x+1) \bmod (x+1)^2$$

Finden Sie die eindeutige Lösung $f \in L$ minimalen Grades. Siehe auch Abbildung 5.4.

Übung 5.19 *Finden Sie das eindeutige Polynom $f \in \mathbb{R}[x]$ von Grad $\deg f \leq 3$ mit*

$$f(-2) = 0 \quad f(0) = 1 \quad f(1) = 0 \quad f(4) = 0,$$

und zeichnen Sie den Funktionsgraphen. Überprüfen Sie Ihre Lösung mit dem MAPLE*-Befehl* `interp`*.*

Hinweis: Sie können den MAPLE*-Befehl* `plot` *verwenden.*

Übung 5.20 *Seien $a_1, \ldots, a_r \in \mathbb{R}$ paarweise verschieden und $m_1, \ldots, m_r \in \mathbb{N}$ mit $\sum_{j=1}^{r} m_j = d + 1$. Zeigen Sie mit Hilfe des Chinesischen Restsatzes, dass es für alle*

$$b_{1,0}, \ldots, b_{1,m_1-1}, \ldots, b_{r,0}, \ldots, b_{r,m_r-1} \in \mathbb{R}$$

ein eindeutiges Polynom $f \in \mathbb{R}[x]_{\leq d}$ gibt mit

$$f^{(j)}(a_i) = b_{i,j}$$

für alle $j = 0, \ldots, m_i - 1$ und $i = 1, \ldots, r$.

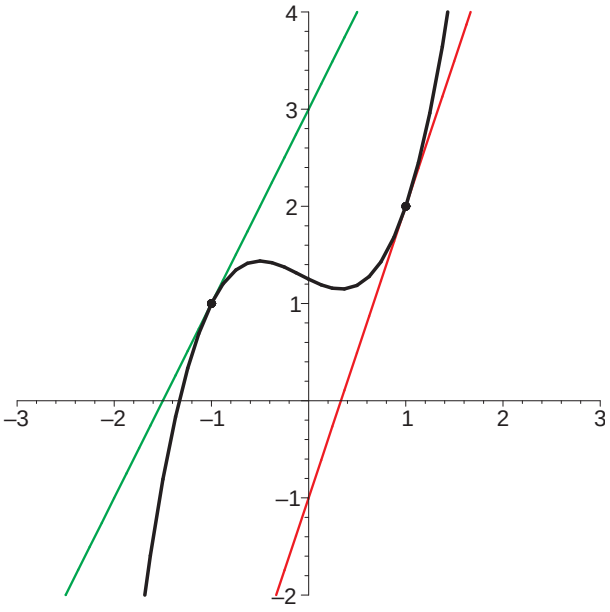


Abbildung 5.4: Polynom mit vorgegebenen Funktionswerten und Ableitungen

Übung 5.21 *Sei $i \in \mathbb{C}$ die imaginäre Einheit, also $i^2 = -1$, $R = \mathbb{Z}[i]$ und*

$$\begin{array}{rccc} d: & R\backslash\{0\} & \to & \mathbb{N}_0 \\ & a+b\cdot i & \mapsto & a^2+b^2 \end{array}$$

1) Zeigen Sie, dass

$$d((a+b\cdot i)\cdot(c+d\cdot i)) = d(a+b\cdot i)\cdot d(c+d\cdot i).$$

2) Folgern Sie, dass $\mathbb{Z}[i]^\times = \{1,-1,i,-i\}$.

3) Zeigen Sie, dass (R,d) ein euklidischer Ring ist. Hinweis: Berechnen Sie zur Division mit Rest von $a+b\cdot i$ durch $c+d\cdot i$ zunächst

$$\frac{a+b\cdot i}{c+d\cdot i} \in \mathbb{Q}[i].$$

4) Bestimmen Sie einen Erzeuger des Ideals

$$(3+4i,\ -1+12i) \subset \mathbb{Z}[i] \quad .$$

Übung 5.22 *Zeigen Sie für* $n = -1, -2, 2, 3$*, dass* $R = \mathbb{Z}\left[\sqrt{n}\right]$ *zusammen mit*

$$\begin{array}{rccl} d: & R\backslash\{0\} & \to & \mathbb{N}_0 \\ & a+b\sqrt{n} & \mapsto & \left|\left(a+b\sqrt{n}\right)\left(a-b\sqrt{n}\right)\right| \end{array}$$

ein euklidischer Ring ist. Geben Sie ein Verfahren an, um die Division mit Rest durchzuführen.

Übung 5.23 *Schreiben Sie ein* MAPLE *Programm, das in* $R = \mathbb{Z}\left[\sqrt{n}\right]$, $n = -1, -2, 2, 3$ *die Division mit Rest und den Euklidischen Algorithmus zur Bestimmung des ggT durchführt.*

Übung 5.24 *Bestimmen Sie jeweils einen Erzeuger der Ideale*

$$(2-i, 2+i) \subset \mathbb{Z}[i] \qquad (11+8\sqrt{3}, 7+2\sqrt{3}) \subset \mathbb{Z}\left[\sqrt{3}\right].$$

6

Vektorräume

6.1 Übersicht

Die lineare Algebra beschäftigt sich mit der Beschreibung von Vektorräumen, der am häufigsten vorkommenden Struktur in der Mathematik. Der Grund dafür liegt darin, dass sie zur Beschreibung der Lösungsmenge von linearen Gleichungssystemen dienen. Wir illustrieren dies zunächst an einem Beispiel: Wollen wir etwa die Menge M aller Polynome

$$f = x_1t^3 + x_2t^2 + x_3t + x_4 \in \mathbb{R}[t]$$

vom Grad 3 mit Nullstellen in $t = -1$ und $t = 2$ und Wendepunkt in $t = 0$ bestimmen, so müssen wir alle f finden mit

$$\begin{aligned} f(-1) &= 0 \\ f''(0) &= 0 \\ f(2) &= 0. \end{aligned}$$

Die Koeffizienten von f müssen also das Gleichungssystem

$$\begin{array}{rcrcrcrcl} -x_1 & + & x_2 & - & x_3 & + & x_4 & = & 0 \\ & & 2x_2 & & & & & = & 0 \\ 8x_1 & + & 4x_2 & + & 2x_3 & + & x_4 & = & 0 \end{array}$$

erfüllen. Alle diese Gleichungen sind linear (d.h. von Grad 1) in den Variablen x_i. Man spricht dann auch von einem **linearen Gleichungssystem**. Da in den Gleichungen kein konstanter Term vorkommt, spricht man von einem **homogenen** linearen Gleichungssystem. Allgemein definiert man:

Definition 6.1.1 *Ein Polynom $f \in K[x_1, \ldots, x_n]$ heißt* ***homogen****, wenn alle Terme von f denselben Grad haben.*

Beispiel 6.1.2 *Die Polynome $x_1 + x_2$ und $x_1^2x_2 + x_1x_2^2$ sind homogen, $x_1 + 1$ und $x_1^2x_2 + x_1x_2$ dagegen nicht.*

Im Gegensatz zu Systemen polynomialer Gleichungen höheren Grades, kann man lineare Gleichungssysteme sehr einfach lösen. Die Idee dabei ist, ein äquivalentes System zu finden, von dem wir die Lösungsmenge sofort ablesen können. Dazu verwendet man die folgende offensichtliche Beobachtung: Man kann in Gleichungssystemen

- Vielfache einer Gleichung zu einer anderen addieren,
- Gleichungen mit einer Konstanten $c \neq 0$ multiplizieren und
- die Reihenfolge der Gleichungen ändern,

ohne dass sich die Lösungsmenge ändert. Diese Transformationen verwendet man nun, um systematisch das Gleichungssystem so zu vereinfachen, dass in den Gleichungen die Variablen x_i kleinsten Index i paarweise verschieden sind. Dieses Verfahren bezeichnet man als den **Gaußalgorithmus**. Der Gaußalgorithmus und der Euklidische Algorithmus sind die beiden wichtigsten Algorithmen in der Mathematik. Sie bilden die Basis von vielen anderen Algorithmen.

6.2 Gaußalgorithmus

Wir formulieren den Gaußalgorithmus allgemein für ein beliebiges Gleichungssystem homogener linearer Polynome über einem beliebigen Körper K. Wie schon diskutiert, können wir das System wie folgt manipulieren:

Bemerkung 6.2.1 *Sind $l_1, l_2 \in K[x_1, \ldots, x_n]$ Polynome und $0 \neq c \in K$, dann gilt für alle $x \in K^n$*

$$\left.\begin{array}{l} l_1(x) = 0 \\ l_2(x) = 0 \end{array}\right\} \Longleftrightarrow \left\{\begin{array}{r} l_1(x) = 0 \\ l_2(x) + c \cdot l_1(x) = 0 \end{array}\right.$$

und

$$l_1(x) = 0 \Longleftrightarrow c \cdot l_1(x) = 0$$

und

$$\left.\begin{array}{l} l_1(x) = 0 \\ l_2(x) = 0 \end{array}\right\} \Longleftrightarrow \left\{\begin{array}{l} l_2(x) = 0 \\ l_1(x) = 0 \end{array}\right.$$

Um dies systematisch durchzuführen, müssen wir eine Reihenfolge für die Variablen festlegen. Die Idee ist hier, bezüglich einer Totalordnung auf der Menge der Variablen den größten Term auszuwählen, man könnte aber auch jede andere Sortierung der Variablen verwenden. Typischerweise verwenden die Totalordnung

$$x_1 > x_2 > ... > x_n$$

bei Variablennamen x_i. Bezüglich dieser Reihenfolge definieren wir:

Definition 6.2.2 *Ist* $f = c_s x_s + c_{s+1} x_{s+1} + ... + c_n x_n$ *mit* $c_s \neq 0$, *dann heißt*

$$\mathrm{L}(f) = x_s$$

die ***Leitvariable*** *(oder das Leitmonom) von* f,

$$\mathrm{LC}(f) = c_s$$

der ***Leitkoeffizient*** *von* f,

$$\mathrm{LT}(f) = c_s x_s$$

der ***Leitterm*** *von* f, *und*

$$\mathrm{tail}(f) = f - \mathrm{LT}(f) = c_{s+1} x_{s+1} + ... + c_n x_n$$

der ***Tail*** *von* f.

Beispiel 6.2.3 *Für*

$$f = \mathbf{2x_2} + 5x_3 + x_4$$

ist

$$\begin{aligned} \mathrm{L}(f) &= x_2 \\ \mathrm{LC}(f) &= 2 \\ \mathrm{LT}(f) &= 2x_2 \\ \mathrm{tail}(f) &= 5x_3 + x_4. \end{aligned}$$

Leitterme markieren wir im Text typischerweise in rot.

Satz 6.2.4 *Für ein homogenes lineares Gleichungssystem gegeben durch $l_1, \dots, l_r \in K[x_1, \dots, x_n]$, alle $l_i \neq 0$, berechnet Algorithmus 6.1 ein äquivalentes System, sodass alle Leitvariablen paarweise verschieden sind.*

Siehe auch Aufgabe 6.2.

Algorithmus 6.1 Gaußalgorithmus

1: **for all** i **do** $l_i = \frac{1}{\mathrm{LC}(l_i)} \cdot l_i$
2: **while** exist $i \neq j$ with $\mathrm{L}(l_i) = \mathrm{L}(l_j)$ **do**
3: $\quad l_j = l_j - l_i$
4: $\quad$ **if** $l_j = 0$ **then**
5: $\quad\quad$ **delete** l_j
6: $\quad$ **else**
7: $\quad\quad l_j = \frac{1}{\mathrm{LC}(l_j)} \cdot l_j$

Beispiel 6.2.5 *In dem obigen Beispiel*

$$\begin{array}{lrcrcrcrcl} l_1 = & \mathbf{-x_1} & + & x_2 & - & x_3 & + & x_4 & = & 0 \\ l_2 = & & & \mathbf{2x_2} & & & & & = & 0 \\ l_3 = & \mathbf{8x_1} & + & 4x_2 & + & 2x_3 & + & x_4 & = & 0 \end{array}$$

geht der Algorithmus wie folgendermaßen vor:

- $l_1 := -l_1$, $l_2 := \frac{1}{2} l_2$ *und* $l_3 := \frac{1}{8} l_3$

$$\begin{array}{rcrcrcrcl} \mathbf{x_1} & - & x_2 & + & x_3 & - & x_4 & = & 0 \\ & & \mathbf{x_2} & & & & & = & 0 \\ \mathbf{x_1} & + & \frac{1}{2}x_2 & + & \frac{1}{4}x_3 & + & \frac{1}{8}x_4 & = & 0 \end{array}$$

- $l_3 := l_3 - l_1$

$$\begin{array}{rcrcrcrcl} \mathbf{x_1} & - & x_2 & + & x_3 & - & x_4 & = & 0 \\ & & \mathbf{x_2} & & & & & = & 0 \\ & & \mathbf{\frac{3}{2}x_2} & - & \frac{3}{4}x_3 & + & \frac{9}{8}x_4 & = & 0 \end{array}$$

- $l_3 := \frac{2}{3} l_3$

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

- $l_3 := l_3 - l_2$

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

- $l_3 := -2l_3$

$$\begin{array}{rcrcrcrcl} \boldsymbol{x_1} & - & x_2 & + & x_3 & - & x_4 & = & 0 \\ & & \boldsymbol{x_2} & & & & & = & 0 \\ & & & & \boldsymbol{x_3} & - & \frac{3}{2}x_4 & = & 0 \end{array}$$

Bemerkung 6.2.6 *Durch Sortieren der l_i nach aufsteigendem Index der Leitvariable $\mathrm{L}(l_i)$ erhält man die* ***Zeilenstufenform*** *des Systems.*

Beispiel 6.2.7 *In Beispiel 6.2.5 ist das System schon in Zeilenstufenform, das System*

$$\begin{array}{rcrcrcrcl} l_1 = & & \boldsymbol{x_1} & & & & & = & 0 \\ l_2 = & & & & & & \boldsymbol{x_3} & = & 0 \\ l_3 = & & & & \boldsymbol{x_2} & & & = & 0 \end{array}$$

dagegen nicht. Durch Vertauschen von l_2 und l_3 erhält man das System in Zeilenstufenform.

$$\begin{array}{rcrcrcrcl} l_1 = & & \boldsymbol{x_1} & & & & & = & 0 \\ l_2 = & & & & \boldsymbol{x_2} & & & = & 0 \\ l_3 = & & & & & & \boldsymbol{x_3} & = & 0 \end{array}$$

Bemerkung 6.2.8 *Durch Algorithmus 6.2 können wir erreichen, dass die Variable $\mathrm{L}(l_i)$ genau in l_i vorkommt. Man spricht dann von einer* ***reduzierten Zeilenstufenform****.*

Siehe auch Aufgabe 6.2.

Algorithmus 6.2 Reduktion

1: **while** exist $i \neq j$ with $\mathrm{L}(l_j)$ in tail(l_i) with coeff c **do**
2: $\quad l_i = l_i - c \cdot l_j$

Beispiel 6.2.9 *In Beispiel 6.2.5 erhalten wir durch* $l_1 := l_1 + l_2$

$$\begin{array}{rrrrrrr} \boldsymbol{x_1} & & + & x_3 & - & x_4 & = & 0 \\ & \boldsymbol{x_2} & & & & & = & 0 \\ & & & \boldsymbol{x_3} & - & \frac{3}{2}x_4 & = & 0 \end{array}$$

und $l_1 := l_1 - l_3$ *die reduzierte Zeilenstufenform*

$$\begin{array}{rrrrrrr} \boldsymbol{x_1} & & & + & \frac{1}{2}x_4 & = & 0 \\ & \boldsymbol{x_2} & & & & = & 0 \\ & & \boldsymbol{x_3} & - & \frac{3}{2}x_4 & = & 0 \end{array}$$

Bemerkung 6.2.10 (Lösungsmenge) *Von der reduzierten Zeilenstufenform lässt sich die Lösungsmenge des Gleichungssystems direkt ablesen, denn die Gleichungen der reduzierten Zeilenstufenform können wir nach den Leitvariablen auflösen, wobei die restlichen Variablen beliebige Werte annehmen können: Zunächst schreiben wir die Lösungsmenge als*

$$V = \{x \in K^n \mid \mathrm{L}(l_i) = -\operatorname{tail}(l_i) \text{ für alle } i\}.$$

Aus dieser impliziten (d.h. durch Gleichungen gegebenen) Darstellung erhalten wir die ***parametrische*** *Darstellung der Lösungsmenge, indem wir in dem Vektor* x *für* $\mathrm{L}(l_i)$ *noch* $-\operatorname{tail}(l_i)$ *einsetzen.*

Beispiel 6.2.11 *Die Lösungsmenge des Gleichungssystems aus Beispiel 6.2.5 ist*

$$V = \left\{x \in \mathbb{R}^4 \mid \boldsymbol{x_1} = -\frac{1}{2}x_4,\ \boldsymbol{x_2} = 0,\ \boldsymbol{x_3} = \frac{3}{2}x_4\right\}.$$

Die Variable x_4 *kann beliebige Werte annehmen, während* x_1, x_2, x_3 *dann bestimmt sind. Durch Einsetzen lässt sich die Lösungsmenge damit auch in der parametrischen Darstellung schreiben als*

$$V = \left\{\left(-\frac{1}{2}x_4, 0, \frac{3}{2}x_4, x_4\right) \mid x_4 \in \mathbb{R}\right\}$$

Beispiel 6.2.12 *Die Menge der in dem Beispiel in Abschnitt 6.1 gesuchten Polynome*

$$f = x_1t^3 + x_2t^2 + x_3t + x_4 \in \mathbb{R}[t]$$

vom Grad 3 mit Nullstellen in $t = -1$ und $t = 2$ und Wendepunkt in $t = 0$ ist also

$$M = \left\{ -\frac{1}{2} x_4 \cdot t^3 + \frac{3}{2} x_4 \cdot t + x_4 \mid x_4 \in \mathbb{R} \right\}.$$

Abbildung 6.1 zeigt die Graphen von einigen $f \in V$ (aufgefasst als Abbildungen $\mathbb{R} \to \mathbb{R}$, $x \mapsto f(x)$). Insbesondere sehen wir, dass jede solche Funktion bei $t = -1$ sogar eine doppelte Nullstelle hat.

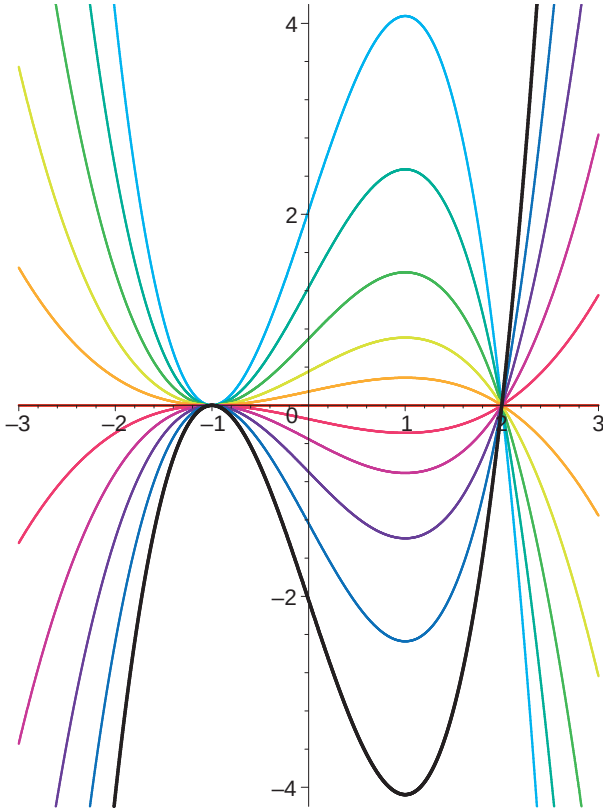


Abbildung 6.1: Kubische Polynome mit Nullstellen bei −1 und 2 und Wendepunkt bei 0

Für weitere Beispiele siehe Aufgabe 6.16.1.
Wir können M in Beispiel 6.2.11 auch schreiben als

$$M = \{x_4 \cdot f \mid x_4 \in \mathbb{R}\}$$

mit

$$f = -\frac{1}{2}t^3 + \frac{3}{2}t + 1.$$

Die wesentliche Eigenschaft von M ist also, dass mit einem Element auch alle seine $\mathbb{R}$-Vielfachen in M liegen. Tatsächlich gilt dies für die Lösungsmenge jedes homogenen linearen Gleichungssystems über einem Körper K:

Bemerkung 6.2.13 *Summen und K-Vielfache von Lösungen eines homogenen linearen Gleichungssystems für $x_1, ..., x_n$ über dem Körper K sind wieder Lösungen.*

Beweis. Betrachte das System

$$\begin{aligned} a_{1,1}x_1 + ... + a_{1,n}x_n &= 0 \\ &\vdots \\ a_{r,1}x_1 + ... + a_{r,n}x_n &= 0 \end{aligned}$$

über einem Körper K. Sind $x, y \in K^n$ Lösungen, dann auch $x + y$ und $\lambda \cdot x$ für alle $\lambda \in K$:

Ist $\sum_{j=1}^n a_{i,j}x_j = 0$ und $\sum_{j=1}^n a_{i,j}y_j = 0$ für alle $i = 1, ..., r$, dann auch

$$\sum_{j=1}^n a_{i,j}(x_j + y_j) = \sum_{j=1}^n a_{i,j}x_j + \sum_{j=1}^n a_{i,j}y_j = 0$$

und

$$\sum_{j=1}^n a_{i,j}(\lambda \cdot x_j) = \lambda \cdot \sum_{j=1}^n a_{i,j}x_j = 0.$$

■

Eine Menge mit dieser Eigenschaft, dass Summen und K-Vielfache von Elementen wieder in der Menge liegen, bezeichnet man als einen K-Vektorraum. In dem Beispiel ist jedes Element von M ein Vielfaches von f, und man nennt f deshalb einen Erzeuger von M. Im Allgemeinen benötigt ein K-Vektorraum V mehr als einen Erzeuger, d.h.

$$V = \{x_1 \cdot f_1 + ... + x_r \cdot f_r \mid x_i \in K\}$$

mit geeigneten $f_i \in V$. Man bezeichnet dann $f_1, ..., f_r$ als Erzeugendensystem von V. Kann man kein Element eines Erzeugendensystems weglassen, so spricht man von einer Basis. In dem Beispiel ist also das Polynom f eine Basis von M. Die Anzahl

der Elemente einer Basis bezeichnet man als Dimension des Vektorraums. Beispielsweise ist die Menge $\mathbb{R}[t]_{\leq 3}$ der Polynome in $\mathbb{R}[t]$ vom Grad ≤ 3 ein Vektorraum der Dimension 4 mit Basis $1, t, t^2, t^3$, denn jedes $g \in \mathbb{R}[t]_{\leq 3}$ lässt sich auf eindeutige Weise schreiben als

$$x_1 t^3 + x_2 t^2 + x_3 t + x_4.$$

Die Menge $M \subset \mathbb{R}[t]_{\leq 3}$ aus dem obigen Beispiel ist ein Vektorraum der Dimension 1. Auch $\mathbb{R}[t]$ ist ein $\mathbb{R}$-Vektorraum, dieser benötigt aber unendlich viele Erzeuger, z.B. bilden $1, t, t^2, ...$ eine Basis, und somit hat $\mathbb{R}[t]$ unendliche Dimension.

Das Konzept der Vektorräume, Erzeugendensysteme und Basen wollen wir im folgenden Abschnitt allgemein einführen.

6.3 Vektorräume und Basen

Definition 6.3.1 *Sei K ein Körper. Ein K-**Vektorraum** ist eine Menge V zusammen mit zwei Verknüpfungen*

$$\begin{array}{lcll} V \times V & \longrightarrow & V & \textit{(Addition)} \\ (v, w) & \longmapsto & v + w & \end{array}$$

$$\begin{array}{lcll} K \times V & \longrightarrow & V & \textit{(Skalarmultiplikation)} \\ (\lambda, v) & \longmapsto & \lambda \cdot v & \end{array}$$

die folgenden Axiomen genügen:

(V1) $(V, +)$ *ist eine abelsche Gruppe,*

(V2) Assoziativgesetz

$$\lambda \cdot (\mu \cdot v) = (\lambda \cdot \mu) \cdot v$$

für alle $\lambda, \mu \in K$ und $v \in V$,

(V3) $1 \cdot v = v$ *für alle $v \in V$,*

(V4) Distributivgesetze

$$(\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot v$$
$$\lambda \cdot (v + w) = \lambda \cdot v + \lambda \cdot w$$

für alle $\lambda, \mu \in K$ und $v, w \in V$.

Die Elemente eines Vektorraums nennen wir auch ***Vektoren****.*

Man beachte, dass hier + sowohl für die Addition in K als auch in V verwendet wird, und $\cdot$ sowohl für die Multiplikation in K als auch die Skalarmultiplikation. Welche der beiden Möglichkeiten gemeint ist, ist aber aus dem Typ der verknüpften Elemente klar.

Beispiel 6.3.2 *Sei K ein Körper. Beispiele von K-Vektorräumen sind:*

1) $K^n = \{(a_1, ..., a_n) \mid a_i \in K\}$ *mit*

$$(a_1, ..., a_n) + (b_1, ..., b_n) := (a_1 + b_1, ..., a_n + b_n)$$
$$\lambda\,(a_1, ..., a_n) := (\lambda a_1, ..., \lambda a_n)$$

wobei man Elemente von K^n auch als Spaltenvektoren schreibt, d.h. als

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \in K^n,$$

Das neutrale Element der Addition von K^n ist der Nullvektor

$$0 = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

2) der Polynomring $K[x]$,

3) die Menge der Folgen in K

$$K^{\mathbb{N}} = \{a : \mathbb{N} \longrightarrow K\}$$

mit

$$(a + b)\,(m) := a\,(m) + b\,(m)$$
$$(\lambda \cdot f)\,(m) := \lambda \cdot f\,(m)$$

für $m \in \mathbb{N}$.

Bemerkung 6.3.3 *Sei V ein K-Vektorraum. Dann gilt:*

1) $0_K \cdot v = 0_V$ *für alle $v \in V$,*
$\lambda \cdot 0_V = 0_V$ *für alle $\lambda \in K$,*

2) $(-1)\cdot v = -v$ *für alle* $v \in V$,

3) $\lambda \cdot v = 0 \Longrightarrow \lambda = 0$ *oder* $v = 0$ *für alle* $\lambda \in K$, $v \in V$.

Dabei bezeichnet 0_K *das Neutrale von* $(K,+)$ *und* 0_V *das Neutrale von* $(V,+)$. *Ist aus dem Kontext klar, ob die Konstante* 0_K *oder der Nullvektor* 0_V *gemeint ist, schreiben wir einfach* 0.

Beweis. (1) und (2) sind leichte Übungen (siehe auch Aufgabe 6.1). Zu (3): Für $\lambda \cdot v = 0$ und $0 \neq \lambda \in K$, $v \in V$ gilt

$$v = 1 \cdot v = (\lambda^{-1}\lambda)v = \lambda^{-1}(\lambda v) = \lambda^{-1}0_V = 0_V.$$

■

Beispiel 6.3.4 *Wir geben Beispiele für die Aussagen in Bemerkung 6.3.3:*

1)

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

2)

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

3)

$$\lambda \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} \lambda x_1 \\ \lambda x_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

genau dann, wenn $\lambda x_1 = 0$ *und* $\lambda x_2 = 0$, *d.h. genau dann, wenn* $\lambda = 0$ *oder* $x_1 = x_2 = 0$.

Bemerkung 6.3.5 *Man könnte* K *in der Definition von* V *durch einen kommutativen Ring* R *mit* 1 *ersetzen (z.B.* $\mathbb{Z}$ *oder einen Polynomring). Dann spricht man von einem* ***R-Modul****. Die Strukturtheorie von Moduln ist wesentlich komplizierter als die von Vektorräumen. Ein wesentlicher Grund hierfür liegt darin, dass die Aussage* (3) *in Bemerkung 6.3.3 im Allgemeinen nicht mehr*

korrekt ist. Beispielsweise ist $\mathbb{Z}/2$ ein $\mathbb{Z}$-Modul mit der Skalarmultiplikation

$$\begin{array}{rcl} \mathbb{Z} \times \mathbb{Z}/2 & \to & \mathbb{Z}/2 \\ (n, \overline{a}) & \mapsto & n \cdot \overline{a} = \underbrace{\overline{a} + \ldots + \overline{a}}_{n} = \overline{n \cdot a} \end{array}$$

und es gilt

$$2 \cdot \overline{1} = \overline{2} = \overline{0},$$

obwohl $2 \neq 0$ und $\overline{1} \neq 0$.

Wir bemerken noch: Ein $\mathbb{Z}$-Modul ist das gleiche wie eine abelsche Gruppe, denn genau wie bei $\mathbb{Z}/2$ können wir einer abelschen Gruppe durch n-fache Addition

$$\begin{array}{rcl} \mathbb{Z} \times G & \to & G \\ (n, g) & \mapsto & n \cdot g = \underbrace{g + \ldots + g}_{n} \end{array}$$

eine $\mathbb{Z}$-Modulstruktur geben.

Summen und Vielfache von Lösungen $(x_1, \ldots, x_n)$ eines homogenen linearen Gleichungssystems für $x_1, \ldots, x_n$ sind wieder Lösungen, aber im Allgemeinen ist nicht jeder Vektor im K^n eine Lösung. Deshalb definieren wir:

Definition 6.3.6 *Sei V ein K-Vektorraum. Eine nichtleere Teilmenge $U \subset V$ heißt **Untervektorraum**, wenn*

$$\begin{aligned} u_1, u_2 \in U &\Longrightarrow u_1 + u_2 \in U \\ \lambda \in K,\ u \in U &\Longrightarrow \lambda \cdot u \in U. \end{aligned}$$

Bemerkung 6.3.7 *1) U mit der von V induzierten Addition und Skalarmultiplikation ist ein K-Vektorraum (siehe Übung 6.1).*

2) Jeder Untervektorraum U enthält die $0 \in V$ (denn es gibt ein $u \in U$ und $0 = 0 \cdot u \in U$).

Satz 6.3.8 *Die Lösungsmenge eines homogenen linearen Gleichungssystems für $x_1, \ldots, x_n$ über dem Körper K ist ein Untervektorraum von K^n.*

Beweis. Folgt direkt aus Bemerkung 6.2.13. ■

Die Lösungsmengen von inhomogenen linearen Gleichungssystemen (also mit einem konstanten Term $\neq 0$ in einer der Gleichungen) sind dagegen keine Untervektorräume, denn sie enthalten nicht die $0 \in K^n$.

Beispiel 6.3.9 *Eine Gerade $L \subset \mathbb{R}^n$ ist ein Untervektorraum genau dann, wenn $0 \in L$ (siehe Abbildung 6.2).*

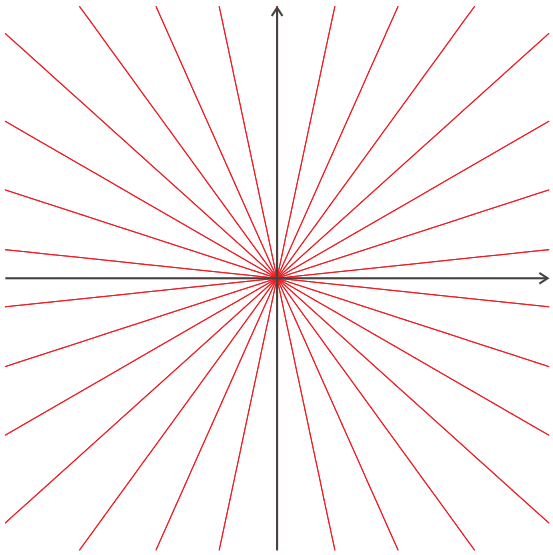


Abbildung 6.2: Geraden im $\mathbb{R}^2$, die Untervektorräume sind

Beweis. Die Notwendigkeit von $0 \in L$ ist Bemerkung 6.3.7(2). Umgekehrt, falls $0 \in L$, dann

$$L = \{\lambda v \mid \lambda \in \mathbb{R}\}$$

mit $0 \neq v \in L$. Somit ist

$$\begin{aligned} \lambda_1 v + \lambda_2 v &= (\lambda_1 + \lambda_2)\, v \in L \\ \lambda_1 (\lambda_2 v) &= (\lambda_1 \lambda_2)\, v \in L \end{aligned}$$

für alle $\lambda_i \in \mathbb{R}$. ■

Beispiel 6.3.10 *1) Untervektorräume von* $\mathbb{R}^3$ *sind* $\{0\}$*, die Geraden durch* 0*, die Ebenen durch* 0 *(Übung) und* $\mathbb{R}^3$ *selbst. Dass dies alle möglichen Untervektorräume sind, werden wir später zeigen.*

2) $K[x]_{\leq d} = \{f \in K[x] \mid \deg f \leq d\} \subset K[x]$ *ist ein Untervektorraum.*

3) Die Mengen

$$U_1 = \left\{(x, y) \in \mathbb{R}^2 \mid y \geq a\right\}$$

mit $a \in \mathbb{R}$ *(siehe Abbildung 6.3 für* $a = 0$*) und*

$$U_2 = \left\{(x, y) \in \mathbb{R}^2 \mid y = x^2\right\}$$

(siehe Abbildung 6.4) sind keine Untervektorräume von $\mathbb{R}^2$*. Warum?*

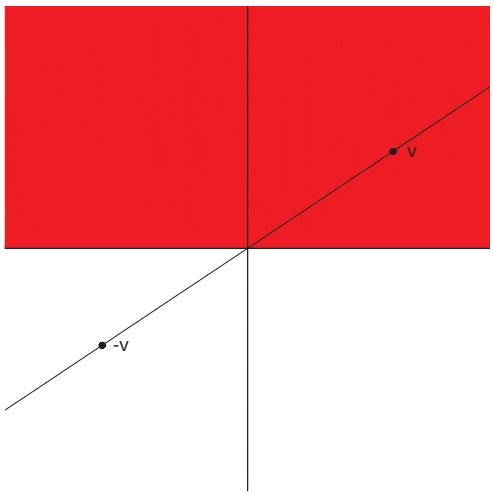


Abbildung 6.3: Halbebene

4) Sind $a_1, \ldots a_n \in K$*, dann ist die Hyperebene*

$$H = \{(x_1, \ldots, x_n) \in K^n \mid a_1x_1 + \ldots + a_nx_n = 0\}$$

ein Untervektorraum. Dies haben wir schon allgemeiner in Bemerkung 6.3.8 für Lösungsmengen von homogenen linearen Gleichungssystemen beobachtet.

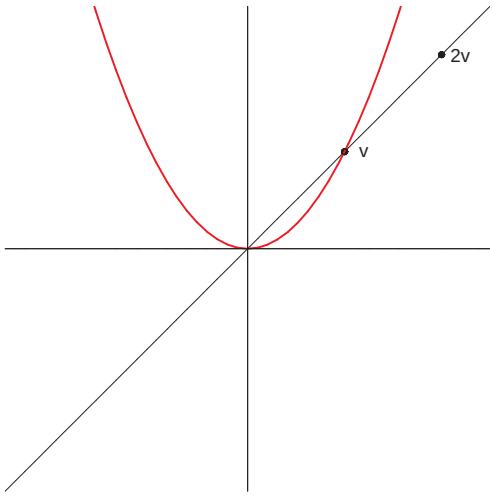


Abbildung 6.4: Parabel

Definition und Satz 6.3.11 *Sei V ein K-Vektorraum und $v_1, ..., v_n \in V$. Ein Vektor $v \in V$ ist eine* ***Linearkombination*** *von $v_1, ..., v_n$, wenn es $\lambda_i \in K$ gibt mit*

$$v = \lambda_1 v_1 + ... + \lambda_n v_n.$$

Die Menge aller Linearkombinationen

$$\langle v_1, ..., v_n \rangle := \{\lambda_1 v_1 + ... + \lambda_n v_n \mid \lambda_i \in K\} \subset V$$

ist ein Untervektorraum, der ***von $v_1, ..., v_n$ aufgespannte Untervektorraum****.*

Beweis. Sind $v, w \in \langle v_1, ..., v_n \rangle$ also $v = \sum_{i=1}^n \lambda_i v_i$ und $w = \sum_{i=1}^n \mu_i v_i$ mit $\lambda_i, \mu_i \in K$, dann

$$v + w = \sum_{i=1}^{n} (\lambda_i + \mu_i) v_i \in \langle v_1, ..., v_n \rangle$$

und

$$\lambda v = \sum_{i=1}^{n} (\lambda \cdot \lambda_i) v_i \in \langle v_1, ..., v_n \rangle .$$

■

Beispiel 6.3.12 *1) Die Vektoren*

$$v_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad v_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \in \mathbb{R}^3$$

spannen die Ebene $E = \{z = 0\}$ auf, denn für jeden Vektor in der Ebene gilt

$$E \ni \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ 0 \end{pmatrix} = \lambda_1 v_1 + \lambda_2 v_2.$$

Die Vektoren

$$w_1 = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \quad w_2 = \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix} \in \mathbb{R}^3$$

spannen ebenfalls die Ebene auf, d.h.

$$E = \langle v_1, v_2 \rangle = \langle w_1, w_2 \rangle$$

denn $w_1 = v_1 + v_2$ und $w_2 = v_1 - v_2$ also

$$\langle w_1, w_2 \rangle \subset \langle v_1, v_2 \rangle$$

und $v_1 = \frac{1}{2}w_1 + \frac{1}{2}w_2$ und $v_2 = \frac{1}{2}w_1 - \frac{1}{2}w_2$, also

$$\langle v_1, v_2 \rangle \subset \langle w_1, w_2 \rangle .$$

Siehe auch Abbildung 6.5.

2) Die Polynome $1, x, ..., x^d \in K[x]$ spannen $K[x]_{\leq d}$ auf.

Definition 6.3.13 *Sei V ein K-Vektorraum.*

*1) Vektoren $v_1, ..., v_n \in V$ heißen ein **Erzeugendensystem** von V, wenn*

$$V = \langle v_1, ..., v_n \rangle .$$

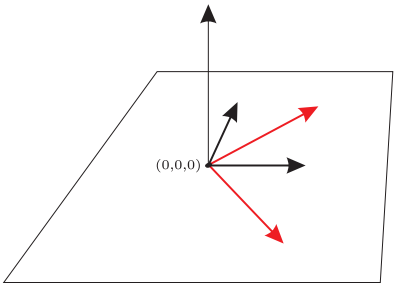


Abbildung 6.5: Zwei Erzeugendensysteme der Ebene $\{z = 0\} \subset \mathbb{R}^3$

2) *Vektoren* $v_1, ..., v_n \in V$ *heißen* ***linear unabhängig****, wenn aus*

$$\lambda_1 v_1 + ... + \lambda_n v_n = 0$$

folgt, dass

$$\lambda_1 = ... = \lambda_n = 0,$$

anderenfalls ***linear abhängig****.*

3) *Ein Erzeugendensystem* $v_1, ..., v_n$ *von* V *aus linear unabhängigen Vektoren heißt* ***Basis*** *von* V*.*

Algorithmus 6.3.14 *Vektoren* $v_1, ..., v_n \in K^m$ *sind linear unabhängig genau dann, wenn das homogene lineare Gleichungssystem*

$$x_1 v_1 + ... + x_n v_n = 0$$

nur die Lösung

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

hat. Dies können wir mit dem Gaußalgorithmus entscheiden.

Beispiel 6.3.15 1) *Die Vektoren*

$$v_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix},\ v_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix},\ v_3 = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \in \mathbb{R}^2$$

sind linear abhängig, denn das Gleichungssystem

$$x_1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + x_2 \begin{pmatrix} 0 \\ 1 \end{pmatrix} + x_3 \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

d.h.

$$\begin{array}{rcrcl} x_1 & & + & x_3 & = & 0 \\ & x_2 & + & x_3 & = & 0 \end{array}$$

hat den Lösungsraum

$$\left\{ \begin{pmatrix} -x_3 \\ -x_3 \\ x_3 \end{pmatrix} \mid x_3 \in \mathbb{R} \right\} \neq \left\{ \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \right\}$$

Das heißt, die Vektoren v_1, v_2, v_3 erfüllen die (bis auf Vielfache eindeutige) Relation

$$-v_1 - v_2 + v_3 = 0.$$

Die Vektoren v_1 und v_2 bilden dagegen eine Basis von $\mathbb{R}^2$. Allgemeiner:

2) Die ***Einheitsvektoren***

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots, e_n = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \in K^n$$

bilden eine Basis von K^n, die sogenannte ***Standardbasis****: Jeder Vektor in K^n lässt sich schreiben als*

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = a_1 e_1 + \ldots + a_n e_n$$

und $e_1, \ldots, e_n$ sind linear unabhängig, denn

$$a_1 e_1 + \ldots + a_n e_n = 0 \Longrightarrow a_1 = \ldots = a_n = 0$$

3) Die Polynome $1, x, \ldots, x^d$ bilden eine Basis von $K[x]_{\leq d}$, denn

$$a_0 \cdot 1 + \ldots + a_d \cdot x^d = 0 \Longrightarrow a_0 = \ldots = a_d = 0.$$

Siehe auch Übungsaufgabe 6.4.

Mit Hilfe einer Basis kann man den Lösungsraum eines homogenen linearen Gleichungssystems wesentlich kompakter schreiben. Die Basis liest man von der reduzierten Zeilenstufenform ab:

Bemerkung 6.3.16 (Basis des Lösungsraums) *Eine Basis des Lösungsraums eines homogenen linearen Gleichungssystems erhalten wir indem wir in der parametrischen Darstellung der Lösungsmenge aus Bemerkung 6.2.10 für die freien Variablen eine Einheitsbasis einsetzen.*

Beweis. Sei

$$\begin{aligned} l_1 &= x_{i_1} + t_{i_1}(x_{j_1}, ..., x_{j_{n-r}}) = 0 \\ &\vdots \\ l_r &= x_{i_r} + t_{i_r}(x_{j_1}, ..., x_{j_{n-r}}) = 0 \end{aligned}$$

mit $l_i \in K[x_1, .., x_n]$ homogen linear in reduzierter Zeilenstufenform mit **Leitvariablen**

$$x_{i_1}, ..., x_{i_r}$$

und **freien Variablen**

$$x_{j_1}, ..., x_{j_{n-r}}$$

(also $\{j_1, ..., j_{n-r}\} = \{1, ..., n\} \backslash \{i_1, ..., i_r\}$). Mit

$$g_i := \begin{cases} -t_i(x_{j_1}, ..., x_{j_{n-r}}) & \text{falls } x_i \text{ eine Leitvariable} \\ x_i & \text{falls } x_i \text{ eine freie Variable} \end{cases}$$

können wir die Lösungsmenge schreiben als

$$L = \left\{ \begin{pmatrix} g_1(x_{j_1}, ..., x_{j_{n-r}}) \\ \vdots \\ g_n(x_{j_1}, ..., x_{j_{n-r}}) \end{pmatrix} \mid x_{j_1}, ..., x_{j_{n-r}} \in K \right\}$$

Da die g_i homogene lineare Polynome in $x_{j_1}, ..., x_{j_{n-r}}$ sind und somit

$$\begin{pmatrix} g_1(x_{j_1}, ..., x_{j_{n-r}}) \\ \vdots \\ g_n(x_{j_1}, ..., x_{j_{n-r}}) \end{pmatrix} = x_{j_1} \cdot \begin{pmatrix} g_1(1, 0, ..., 0) \\ \vdots \\ g_n(1, 0, ..., 0) \end{pmatrix} + ... + x_{j_{n-r}} \cdot \begin{pmatrix} g_1(0, ..., 0, 1) \\ \vdots \\ g_n(0, ..., 0, 1) \end{pmatrix}$$

erhalten wir ein Erzeugendensystem

$$L = \left\langle \begin{pmatrix} g_1(1, 0, ..., 0) \\ \vdots \\ g_n(1, 0, ..., 0) \end{pmatrix}, ..., \begin{pmatrix} g_1(0, ..., 0, 1) \\ \vdots \\ g_n(0, ..., 0, 1) \end{pmatrix} \right\rangle$$

Da in den Koordinaten $x_{j_1}, ..., x_{j_{n-r}}$ der Erzeuger eine Einheitsbasis von K^{n-r} steht, sind diese linear unabhängig und bilden somit eine Basis von L. ■

Siehe auch Aufgabe 6.2.

Beispiel 6.3.17 *Das System*

$$\begin{array}{lllllllllll} l_1 & = & \boldsymbol{x_1} & + & 2x_2 & & & & - & 2x_5 & = & 0 \\ l_2 & = & & & & \boldsymbol{x_3} & & & + & x_5 & = & 0 \\ l_3 & = & & & & & \boldsymbol{x_4} & + & 2x_5 & = & 0 \end{array}$$

in $\mathbb{Q}[x]$ *ist schon in reduzierter Zeilenstufenform, also die Lösungsmenge*

$$V = \left\{ \begin{pmatrix} -2x_2 + 2x_5 \\ x_2 \\ -x_5 \\ -2x_5 \\ x_5 \end{pmatrix} \mid x_2, x_5 \in \mathbb{Q} \right\}$$

und somit erhalten wir mit $(x_2, x_5) = (1, 0)$ *und* $(x_2, x_5) = (0, 1)$ *eine Basis:*

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

Wir überprüfen nochmals in diesem Spezialfall, dass es sich tatsächlich um eine Basis handelt: Jedes Element von V *lässt sich als eindeutige Linearkombination darstellen*

$$\begin{pmatrix} -2x_2 + 2x_5 \\ x_2 \\ -x_5 \\ -2x_5 \\ x_5 \end{pmatrix} = x_2 \cdot \begin{pmatrix} -2 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + x_5 \cdot \begin{pmatrix} -2 \\ 0 \\ -1 \\ -2 \\ 1 \end{pmatrix}$$

und die Vektoren sind linear unabhängig, denn

$$x_2 \cdot \begin{pmatrix} -2 \\ \mathbf{1} \\ 0 \\ 0 \\ \mathbf{0} \end{pmatrix} + x_5 \cdot \begin{pmatrix} -2 \\ \mathbf{0} \\ -1 \\ -2 \\ \mathbf{1} \end{pmatrix} = \begin{pmatrix} 0 \\ \mathbf{0} \\ 0 \\ 0 \\ \mathbf{0} \end{pmatrix} \Longrightarrow \begin{array}{l} x_2 = 0 \\ x_5 = 0 \end{array}$$

Für weitere Beispiele siehe auch die Aufgaben 6.16.1 und 6.16.2.

6.4 Dimension

In diesem Abschnitt wollen wir zeigen, dass je zwei (endliche) Basen eines Vektorraums gleich viele Elemente haben. Diese Zahl ist eine wichtige Invariante des Vektorraums, genannt Dimension. Damit werden wir dann Vektorräume im darauffolgenden Abschnitt klassifizieren: Jeder n-dimensionale K-Vektorraum ist isomorph zu K^n.

Satz 6.4.1 *Sei V ein K-Vektorraum und $\Omega = (v_1, ..., v_n)$ eine Liste von Vektoren in V. Dann sind äquivalent:*

1) Ω ist eine Basis von V.

2) Ω ist ein unverkürzbares Erzeugendensystem von V.

3) Ω ist ein unverlängerbares System linear unabhängiger Vektoren in V.

4) Jeder Vektor in V lässt sich eindeutig als Linearkombination von Ω darstellen.

Beweis. $(1 \Rightarrow 2)$: Angenommen

$$v_1, ..., v_{i-1}, v_{i+1}, ..., v_n$$

sind auch ein Erzeugendensystem von V. Dann ist insbesondere

$$v_i = \lambda_1 v_1 + ... + \lambda_{i-1} v_{i-1} + \lambda_{i+1} v_{i+1} + ... + \lambda_n v_n$$

eine Linearkombination mit $\lambda_j \in K$, also

$$\lambda_1 v_1 + ... + \lambda_{i-1} v_{i-1} - v_i + \lambda_{i+1} v_{i+1} + ... + \lambda_n v_n = 0,$$

ein Widerspruch zur linearen Unabhängigkeit von $v_1, ..., v_n$.

$(2 \Rightarrow 3)$: Wir zeigen zunächst, dass $v_1, ..., v_n$ linear unabhängig sind. Angenommen

$$\lambda_1 v_1 + ... + \lambda_n v_n = 0$$

und $\lambda_i \neq 0$. Dann ist

$$v_i = -\frac{1}{\lambda_i} \left(\lambda_1 v_1 + ... + \lambda_{i-1} v_{i-1} + \lambda_{i+1} v_{i+1} + ... + \lambda_n v_n \right)$$

also $v_1, ..., v_{i-1}, v_{i+1}, ..., v_n$ ein kürzeres Erzeugendensystem von V (d.h. eines mit weniger Elementen), ein Widerspruch zu (2).

Da nach (2) die Vektoren $v_1, ..., v_n$ den Vektorraum V erzeugen, wäre jedes weitere $v \in V$ eine Linearkombination von $v_1, ..., v_n$ und somit $v_1, ..., v_n, v$ linear abhängig.

$(3 \Rightarrow 4)$: Wir zeigen, dass $v_1, ..., v_n$ ein Erzeugendensystem von V sind: Sei $v \in V$ beliebig. Nach Voraussetzung sind $v_1, ..., v_n, v$ linear abhängig, also gibt es $\lambda_i, \lambda \in K$, nicht alle 0, mit

$$\lambda_1 v_1 + ... + \lambda_n v_n + \lambda v = 0.$$

Angenommen $\lambda = 0$. Dann ist $\lambda_1 v_1 + ... + \lambda_n v_n = 0$, wegen $v_1, ..., v_n$ linear unabhängig also auch $\lambda_1 = ... = \lambda_n = 0$, ein Widerspruch. Somit lässt sich v darstellen als

$$v = -\frac{\lambda_1}{\lambda} v_1 - ... - \frac{\lambda_n}{\lambda} v_n.$$

Zum Beweis der Eindeutigkeit nehmen wir an, dass

$$\lambda_1 v_1 + ... + \lambda_n v_n = v = \mu_1 v_1 + ... + \mu_n v_n$$

also

$$(\lambda_1 - \mu_1) v_1 + ... + (\lambda_n - \mu_n) v_n = 0.$$

Da $v_1, ..., v_n$ linear unabhängig sind, folgt $\lambda_i = \mu_i \ \forall i$.

$(4 \Rightarrow 1)$: Nach Voraussetzung ist $v_1, ..., v_n$ ein Erzeugendensystem. Wären die Vektoren linear abhängig, dann gäbe es zwei unterschiedliche Darstellungen der 0

$$\lambda_1 v_1 + ... + \lambda_n v_n = 0 = 0 v_1 + ... + 0 v_n.$$

■

Bemerkung 6.4.2 *Mit Hilfe von Satz 6.4.1 können wir Vektoren eines K-Vektorraums V im Computer darstellen: Dazu wählen wir eine Basis $\Omega = (v_1, ..., v_n)$ von V. Da jedes $v \in V$ eine eindeutige Darstellung*

$$v = a_1 v_1 + ... + a_n v_n$$

mit $a_i \in K$ hat, können wir v im Computer durch

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \in K^n$$

repräsentieren. Anders ausgedrückt, die ***Linearkombinationsabbildung***

$$\begin{array}{rccl} \mathrm{lc}_\Omega: & K^n & \longrightarrow & V \\ & \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} & \longmapsto & a_1v_1 + ... + a_nv_n \end{array}$$

ist bijektiv. Ihre Umkehrabbildung

$$\mathrm{co}_\Omega = \mathrm{lc}_\Omega^{-1} : V \longrightarrow K^n$$

bezeichnen wir als ***Koordinatendarstellung*** *bezüglich Ω. Vom praktischen Standpunkt können wir uns co_Ω als Parser und lc_Ω als Ausgaberoutine vorstellen.*

Beispiel 6.4.3 *Wählen wir für den Vektorraum $V = K[x]_{\leq 2}$ der Polynome vom Grad ≤ 2 die Basis $\Omega = (1, x, x^2)$, so erhalten wir die Bijektion*

$$\begin{array}{rccl} \mathrm{lc}_\Omega: & K^3 & \longrightarrow & K[x]_{\leq 2} \\ & \begin{pmatrix} a_0 \\ a_1 \\ a_2 \end{pmatrix} & \longmapsto & a_0 + a_1x + a_2x^2 \end{array}$$

Somit ist z.B. die Koordinatendarstellung des Polynoms $3x^2 + x$

$$\mathrm{co}_\Omega(3x^2 + x) = \begin{pmatrix} 0 \\ 1 \\ 3 \end{pmatrix}$$

Wie aber findet man eine Basis? Auch dieses Problem wir von Satz 6.4.1 gelöst, dann wir können aus einem Erzeugendensystem durch sukzessives Weglassen von Erzeugern ein unverkürzbares Erzeugendensystem, d.h. eine Basis, erhalten:

Corollar 6.4.4 (Basisauswahlsatz) *Ist V ein K-Vektorraum und $v_1, ..., v_m$ ein Erzeugendensystem von V, dann gibt es $i_1, ..., i_n \in \{1, ..., m\}$, sodass $v_{i_1}, ..., v_{i_n}$ eine Basis von V bilden.*

Siehe auch Übungsaufgabe 6.7.

Beispiel 6.4.5 *Die Vektoren*

$$v_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix},\ v_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix},\ v_3 = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix},\ v_4 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

erzeugen $\mathbb{R}^3$*. Der Lösungsraum des Gleichungssystems* $\sum_i \lambda_i v_i = 0$*, d.h.*

$$\begin{array}{ccccccc} \lambda_1 & & + & \lambda_3 & & = & 0 \\ & \lambda_2 & + & \lambda_3 & & = & 0 \\ & & & & \lambda_4 & = & 0 \end{array}$$

ist

$$V = \left\langle \begin{pmatrix} -1 \\ -1 \\ 1 \\ 0 \end{pmatrix} \right\rangle$$

also gilt die Relation

$$-v_1 - v_2 + v_3 = 0$$

d.h. wir können einen der drei Vektoren streichen. Da es keine weiteren Relationen zwischen den $v_1, ..., v_4$ *gibt, erhalten wir dann linear unabhängige Vektoren und somit eine Basis. Die möglichen Basisauswahlen sind also*

$$v_1, v_2, v_4$$
$$v_1, v_3, v_4$$
$$v_2, v_3, v_4$$

Im Allgemeinen haben Vektorräume viele verschiedene Basen: Sowohl

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

als auch

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

bilden eine Basis von $\mathbb{R}^2$. Für jedes $b \in \mathbb{R}$ sind die Polynome

$$1, (x-b), (x-b)^2, ..., (x-b)^d$$

eine Basis von $\mathbb{R}[x]_{\leq d}$ (siehe Übungsaufgabe 6.5). Insbesondere für $b = 0$ erhalten wir die Standardbasis $1, x, ..., x^d$.

Die Anzahl der Basiselemente ist jedoch von der Wahl der Basis unabhängig. Dies werden wir im folgenden Satz zeigen.

Definition 6.4.6 *Ein Vektorraum heißt* ***endlichdimensional****, wenn er ein endliches Erzeugendensystem besitzt.*

Bemerkung 6.4.7 *Mit dem Basisauswahlsatz 6.4.4 hat jeder endlichdimensionale Vektorraum dann auch eine (endliche) Basis.*

Definition und Satz 6.4.8 (Hauptsatz über Vektorräume) *Sei V ein endlichdimensionaler K-Vektorraum. Dann haben je zwei Basen dieselbe Anzahl von Elementen.*

Diese Anzahl bezeichnen wir als die ***Dimension*** $\dim_K V$ *von V über K. Ist V nicht endlichdimensional, so setzen wir $\dim_K V = \infty$. Ist aus dem Zusammenhang klar, über welchem Körper wir V betrachten, so schreiben wir auch kurz $\dim V$.*

Beispiel 6.4.9 *Mit Satz 6.4.8 und den Basen aus Beispiel 6.3.15 folgt:*

1) $\dim K^n = n$,

2) $\dim K[x]_{\leq d} = d + 1$,

3) $\dim K[x] = \infty$, *denn jede endliche Menge von Polynomen erzeugt nur einen Untervektorraum, da sie nur Polynome beschränkten Grades enthält.*

4) $\mathbb{R}$ *ist ein $\mathbb{Q}$-Vektorraum unendlicher Dimension (hätte $\mathbb{R}$ Dimension n über $\mathbb{Q}$, dann gäbe es wie oben eine bijektive Abbildung $\mathbb{Q}^n \to \mathbb{R}$. Somit wäre mit $\mathbb{Q}$ auch $\mathbb{R}$ abzählbar, ein Widerspruch). Also* $\dim_{\mathbb{Q}} \mathbb{R} = \infty$ *(aber* $\dim_{\mathbb{R}} \mathbb{R} = 1$ *mit der Basis* $e_1 = 1$*).*

Der Beweis von Satz 6.4.8 beruht auf folgendem Lemma:

Lemma 6.4.10 (Austauschlemma) *Sei $v_1, ..., v_n$ eine Basis von V und $0 \neq w \in V$ ein weiterer Vektor. Dann existiert ein $i \in \{1, ..., n\}$, sodass auch $v_1, ..., v_{i-1}, w, v_{i+1}, ..., v_n$ eine Basis von V bilden.*

Beweis. Da $v_1, ..., v_n$ ein Erzeugendensystem sind, gibt es $\lambda_1, ..., \lambda_n \in K$ mit

$$w = \lambda_1 v_1 + ... + \lambda_n v_n.$$

Hier muss ein $\lambda_i \neq 0$ sein, da $w \neq 0$. Nach Umnummerieren können wir $\lambda_1 \neq 0$ annehmen. Also ist

$$v_1 = \frac{1}{\lambda_1}(w - (\lambda_2 v_2 + ... + \lambda_n v_n))$$

eine Linearkombination von $w, v_2, ..., v_n$ und somit diese Vektoren Erzeuger von V. Hier verwenden wir essentiell die Körpereigenschaft von K. Über einem Ring würde $\frac{1}{\lambda_1}$ im Allgemeinen nicht existieren.

Zur linearen Unabhängigkeit: Angenommen

$$\mu w + \mu_2 v_2 + ... + \mu_n v_n = 0,$$

also

$$\mu\lambda_1 v_1 + (\mu_2 + \mu\lambda_2) v_2 + ... + (\mu_n + \mu\lambda_n) v_n = 0.$$

Da $v_1, ..., v_n$ linear unabhängig sind, gilt

$$\mu\lambda_1 = \mu_2 + \mu\lambda_2 = ... = \mu_n + \mu\lambda_n = 0$$

Aus $\lambda_1 \neq 0$ folgt $\mu = 0$ und somit $\mu_2 = ... = \mu_n = 0$. ■

Beispiel 6.4.11 *Die Einheitsvektoren $e_1, e_2, e_3 \in \mathbb{R}^3$ bilden eine Basis. Da*

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

können wir sowohl e_1 als auch e_2 durch w ersetzen und erhalten die Basen w, e_2, e_3 bzw. e_1, w, e_3.

Mit dem Austauschlemma folgt durch Induktion:

Satz 6.4.12 (Austauschsatz) *Sei V ein K-Vektorraum, $v_1, ..., v_n$ eine Basis von V und $w_1, ..., w_s$ linear unabhängig. Dann gilt*

$$s \leq n.$$

Weiter gibt es $i_1, ..., i_{n-s} \in \{1, ..., n\}$, sodass

$$w_1, ..., w_s, v_{i_1}, ..., v_{i_{n-s}}$$

eine Basis von V bilden.

Beweis. Für $s = 1$ ist dies Lemma 6.4.10. Induktionsschritt $s-1 \mapsto s$: Nach Induktionsvoraussetzung können wir $w_1, ..., w_{s-1}$ austauschen. Nach Umnummerieren ist also

$$w_1 \dots, w_{s-1}, v_s, \dots, v_n$$

eine Basis von V. Somit existieren $\lambda_i \in K$ mit

$$w_s = \lambda_1 w_1 + ... + \lambda_{s-1} w_{s-1} + \lambda_s v_s + ... + \lambda_n v_n.$$

Wären $\lambda_s = ... = \lambda_n = 0$, dann $w_1, \dots, w_s$ linear abhängig, ein Widerspruch. Es gibt also ein $i \geq s$ mit $\lambda_i \neq 0$, und damit können wir v_i mit Lemma 6.4.10 gegen w_s austauschen. ■

Insbesondere erhalten wir:

Corollar 6.4.13 (Basisergänzungssatz) *Ist V ein endlichdimensionaler K-Vektorraum und $v_1, \dots, v_m$ linear unabhängig. Dann gibt es $v_{m+1}, ..., v_n \in V$, sodass $v_1, ..., v_n$ eine Basis bilden.*

Beweis. Nach Corollar 6.4.4 hat V eine Basis und nach Satz 6.4.12 lassen sich in der Basis Vektoren durch $v_1, \dots, v_m$ austauschen. ■

Der Austauschsatz impliziert auch direkt Satz 6.4.8:

Beweis. Satz 6.4.12 angewendet auf zwei Basen der Länge n und s liefert sowohl $s \leq n$ als auch $n \leq s$. ■

Wir demonstrieren den Austauschsatz an einem Beispiel:

Beispiel 6.4.14 *Die Polynome*

$$x^2 + 1, x^2 + x, x + 1 \in \mathbb{Q}[x]_{\leq 2}$$

bilden eine Basis: In der Standardbasis $1, x, x^2$ können wir x^2 durch $x^2 + 1$ austauschen, denn

$$x^2 + 1 = \underset{\neq 0}{1} \cdot x^2 + 1 \cdot 1,$$

und wir erhalten die Basis

$$1, x, x^2 + 1.$$

Weiter lässt sich x durch $x^2 + x$ austauschen, denn

$$x^2 + x = 1 \cdot (x^2 + 1) + \underset{\neq 0}{1} \cdot x + (-1) \cdot 1,$$

und wir erhalten die Basis

$$1, x^2 + x, x^2 + 1.$$

Schließlich kann man 1 *durch* $x + 1$ *ersetzen, denn*

$$x + 1 = \underset{\neq 0}{2} \cdot 1 + 1 \cdot \left(x^2 + x\right) + (-1) \cdot \left(x^2 + 1\right).$$

Aus dem Austauschsatz folgt auch:

Corollar 6.4.15 *Sei* $U \subset V$ *ein Untervektorraum. Dann gilt*

$$\dim U \leq \dim V.$$

Falls $\dim U = \dim V$*, so ist* $U = V$*.*

Beweis. Für $\dim V = \infty$ ist die erste Behauptung trivial. Ist $v_1, ..., v_n$ eine Basis von V und $w_1, ..., w_s$ eine Basis von U, so gilt $s \leq n$ mit Satz 6.4.12.

Für $s = n$ lassen sich $v_1, ..., v_n$ mit Satz 6.4.12 vollständig gegen $w_1, ..., w_n$ austauschen. Somit bilden $w_1, ..., w_n$ eine Basis. ■

Bemerkung 6.4.16 *Sei* V *ein Vektorraum der Dimension* $n < \infty$ *und* $v_1, ..., v_n \in V$*. Dann sind äquivalent:*

1) $v_1, ..., v_n$ *bilden eine Basis,*

2) $v_1, ..., v_n$ *sind linear unabhängig,*

3) $v_1, ..., v_n$ *sind ein Erzeugendensystem von* V*.*

Beweis. Seien $v_1, ..., v_n$ linear unabhängig. Dann bilden $v_1, ..., v_n$ eine Basis von $U = \langle v_1, ..., v_n \rangle$ und somit ist

$$\dim U = n = \dim V$$

also mit Corollar 6.4.15 $U = V$.

Seien $v_1, ..., v_n$ ein Erzeugendensystem von V. Somit können wir $v_1, ..., v_n$ mit Corollar 6.4.4 zu einer Basis verkürzen. Wäre die Basis echt kürzer, dann wäre $\dim V < n$, ein Widerspruch. Also sind $v_1, ..., v_n$ ein unverkürzbares Erzeugendensystem, d.h. nach Satz 6.4.1 eine Basis. ■

6.5 Vektorraumhomomorphismen

In Bemerkung 6.4.2 haben wir gesehen, wie sich Vektoren eines beliebigen endlichdimensionalen Vektorraums im Computer darstellen lassen. Dazu wählen wir eine Basis $\Omega = (v_1, ..., v_n)$ von V. Da jedes $v \in V$ eine eindeutige Darstellung

$$v = a_1 v_1 + ... + a_n v_n$$

mit $a_i \in K$ hat, können wir v durch den Vektor der Koeffizienten a_i repräsentieren. Die Linearkombinationsabbildung bezüglich Ω

$$\begin{array}{rccc} \mathrm{lc}_\Omega : & K^n & \longrightarrow & V \\ & \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} & \longmapsto & a_1 v_1 + ... + a_n v_n \end{array}$$

ist also bijektiv, wobei wir die Umkehrabbildung, die Koordinatendarstellung bezüglich Ω, mit

$$\mathrm{co}_\Omega = \mathrm{lc}_\Omega^{-1} : V \longrightarrow K^n$$

bezeichnen.

Soll die Darstellung von Elementen von V durch Vektoren in K^n von Nutzen sein, müssen lc_Ω und co_Ω die Vektorraumstrukturen von K^n und V respektieren, d.h. es darf keine Rolle spielen, ob wir Rechnungen in V oder mit den Koordinatendarstellungen in K^n durchführen. Dies ist tatsächlich der Fall, denn

$$\begin{aligned} \mathrm{lc}_\Omega\left(\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} + \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}\right) &= \mathrm{lc}_\Omega \begin{pmatrix} a_1 + b_1 \\ \vdots \\ a_n + b_n \end{pmatrix} = \sum_{i=1}^{n} (a_i + b_i)\, v_i \\ &= \sum_{i=1}^{n} a_i v_i + \sum_{i=1}^{n} b_i v_i = \mathrm{lc}_\Omega \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} + \mathrm{lc}_\Omega \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \end{aligned}$$

und

$$\begin{aligned} \mathrm{lc}_\Omega\left(\lambda \cdot \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}\right) &= \mathrm{lc}_\Omega \begin{pmatrix} \lambda a_1 \\ \vdots \\ \lambda a_n \end{pmatrix} = \sum_{i=1}^{n} (\lambda a_i)\, v_i \\ &= \lambda \sum_{i=1}^{n} a_i v_i = \lambda \cdot \mathrm{lc}_\Omega \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}. \end{aligned}$$

Das heißt, dass lc_Ω ein Homomorphismus von Vektorräumen ist:

Definition 6.5.1 *Ein K-**Vektorraumhomomorphismus** ist eine K-lineare Abbildung $F : V \to W$ zwischen K-Vektorräumen, d.h.*

$$F(v_1 + v_2) = F(v_1) + F(v_2)$$

für alle $v_i \in V$ und

$$F(\lambda v) = \lambda F(v)$$

für alle $v \in V$ und $\lambda \in K$.

Die Begriffe Mono-, Epi- und Isomorphismus werden analog wie bei Gruppen und Ringen verwendet.

Beispiel 6.5.2 *1) Analog können wir die Linearkombinationsabbildung lc_Ω auch für eine beliebige Liste $\Omega = (v_1, ..., v_n)$ von Vektoren in V definieren, nach unserem obigen Beweis ist sie immer noch ein Homomorphimus, aber i.A. weder injektiv noch surjektiv. Es gilt offenbar:*

$$\begin{aligned} \mathrm{lc}_\Omega \text{ Epimorphismus} &\Leftrightarrow \Omega \text{ Erzeugendensystem von } V \\ \mathrm{lc}_\Omega \text{ Monomorphismus} &\Leftrightarrow \Omega \text{ linear unabhängig} \\ \mathrm{lc}_\Omega \text{ Isomorphismus} &\Leftrightarrow \Omega \text{ Basis von } V \end{aligned}$$

Man zeigt wie üblich, dass mit lc_Ω auch $\mathrm{co}_\Omega = \mathrm{lc}_\Omega^{-1}$ ein Isomorphismus ist.

2) Insbesondere ist z.B.

$$\begin{array}{rccl} \mathrm{lc}_{(1,x,...,x^d)} : & K^{d+1} & \longrightarrow & K[x]_{\leq d} \\ & \begin{pmatrix} a_0 \\ \vdots \\ a_d \end{pmatrix} & \longmapsto & a_0 + a_1 x + ... + a_d x^d \end{array}$$

ein K-Vektorraumisomorphismus.

Die Klassifikation von endlichdimensionalen Vektorräumen bis auf Isomorphie ist sehr einfach, die Dimension ist dafür schon ausreichend:

Satz 6.5.3 (Klassifikationssatz für Vektorräume) *Sei V ein K-Vektorraum der Dimension $n < \infty$. Dann ist V isomorph zu K^n. Schreibe*

$$V \cong K^n.$$

Beweis. Nach Bemerkung 6.4.7 und Definition und Satz 6.4.8 hat V eine Basis $\Omega = (v_1, ..., v_n)$ mit n Elementen, und nach Beispiel 6.5.2.(1) ist

$$\mathrm{lc}_\Omega : K^n \to V$$

ein Isomorphismus. ■

Definition und Satz 6.5.4 *Eine $n \times m$-**Matrix** A über K ist eine Tabelle*

$$A = \begin{pmatrix} a_{1,1} & \cdots & a_{1,m} \\ \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,m} \end{pmatrix} = (a_{i,j})_{\substack{i=1,...,n \\ j=1,...,m}}$$

Die Menge der $n \times m$-Matrizen bezeichnen wir mit $K^{n\times m}$.

*Durch die **Matrixmultiplikation***

$$\begin{pmatrix} a_{11} & \cdots & a_{1,m} \\ \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,m} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} := \begin{pmatrix} \left(\sum_{j=1}^m a_{1,j} x_j\right) \\ \vdots \\ \left(\sum_{j=1}^m a_{n,j} x_j\right) \end{pmatrix}$$

ist ein Vektorraumhomomorphismus

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

gegeben, den wir wieder mit A bezeichnen. Das Bild von x ist also einfach die x_j-Linearkombination der Spalten $A_i \in K^n$ von $A = (A_1 \mid ... \mid A_m)$, d.h.

$$(A_1 \mid ... \mid A_m) \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = \sum_{j=1}^m x_j \cdot A_j.$$

Beweis. Die Abbildung $A = \mathrm{lc}_{(A_1,...,A_m)}$, sie ist also eine Linearkombinationsabbildung und somit wie oben bemerkt ein Homomorphismus. ■

Beispiel 6.5.5 *Es gilt*

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} = \begin{pmatrix} 1\cdot 1 + 2\cdot 2 + 3\cdot 3 \\ 4\cdot 1 + 5\cdot 2 + 6\cdot 3 \end{pmatrix} = \begin{pmatrix} 14 \\ 32 \end{pmatrix}$$

mit der Multiplikationsformel. Alternativ mit der Interpretation als Linearkombinationsabbildung erhalten wir dasselbe Ergebnis:

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} = 1 \cdot \begin{pmatrix} 1 \\ 4 \end{pmatrix} + 2 \cdot \begin{pmatrix} 2 \\ 5 \end{pmatrix} + 3 \cdot \begin{pmatrix} 3 \\ 6 \end{pmatrix} = \begin{pmatrix} 14 \\ 32 \end{pmatrix}$$

Beispiel 6.5.6 *Die Ableitung*

$$\tfrac{d}{dx} : \quad \mathbb{R}[x] \quad \longrightarrow \quad \mathbb{R}[x]$$

ist ein $\mathbb{R}$-Vektorraumhomomorphismus, da

$$\frac{d}{dx}\left(\textstyle\sum_{i=0}^{d} a_i x^i\right) = \textstyle\sum_{i=1}^{d} i a_i x^{i-1}$$

also das Bild linear von den Koeffizienten a_i des Polynoms abhängt (überprüfen Sie das). Sie ist kein Monomorphimus, denn z.B.

$$\frac{d}{dx} 0 = \frac{d}{dx} 1,$$

aber ein Epimorphismus, denn

$$\frac{d}{dx}\left(\textstyle\sum_{i=0}^{d} \frac{a_i}{i+1} x^{i+1}\right) = \textstyle\sum_{i=0}^{d} a_i x^i,$$

d.h. jedes Polynom besitzt eine Stammfunktion.

Lemma 6.5.7 *Sei $F : V \to W$ ein Vektorraumhomomorphismus. Dann sind* $\mathrm{Ker}(F) \subset V$ *und* $\mathrm{Bild}(F) \subset W$ *Untervektorräume. Die Dimension des Bildes bezeichnen wir auch als* ***Rang*** *von F*

$$\mathrm{rk}(F) := \dim \mathrm{Bild}(F).$$

Beweis. Für den Kern: Ist $F(v_1) = 0$ und $F(v_2) = 0$, dann auch

$$F(v_1 + v_2) = F(v_1) + F(v_2) = 0$$

und

$$F(\lambda \cdot v_1) = \lambda \cdot F(v_1) = 0$$

für alle $\lambda \in K$.

Die Aussage für das Bild zeigt man analog. ∎

Bemerkung 6.5.8 *Da ein Vektorraumhomomorphismus $F : V \to W$ insbesondere ein Gruppenhomomorphismus $(V, +) \to (W, +)$ ist, gilt nach Lemma 4.2.13, dass*

$$F \text{ Monomorphismus} \iff \mathrm{Ker}(F) = \{0\},$$

wobei $\mathrm{Ker}(F) = \{v \in V \mid F(v) = 0\}$.

In Verallgemeinerung von 6.5.2.(1) haben wir:

Bemerkung 6.5.9 *Sei $F : V \to W$ ein Homomorphismus, $\Omega = (v_1, ..., v_n)$ eine Basis von V und $\Delta = (F(v_1), ..., F(v_n))$ das Bild von Ω unter F. Dann gilt*

$$\begin{array}{lcl} F \text{ Epimorphismus} & \Leftrightarrow & \Delta \text{ Erzeugendensystem von } W \\ F \text{ Monomorphismus} & \Leftrightarrow & \Delta \text{ linear unabhängig} \\ F \text{ Isomorphismus} & \Leftrightarrow & \Delta \text{ Basis von } W \end{array}$$

Beweis. Jeder Vektor in V ist von der Form $\sum_{i=1}^n \lambda_i v_i$ mit $\lambda_i \in K$. Es gilt also

$$\begin{aligned} \mathrm{Bild}(F) &= \{F\left(\textstyle\sum_{i=1}^n \lambda_i v_i\right) \mid \lambda_i \in K\} \\ &= \{\textstyle\sum_{i=1}^n \lambda_i F(v_i) \mid \lambda_i \in K\}. \end{aligned}$$

Somit ist $\mathrm{Bild}(F) = W$ genau dann, wenn die $F(v_i)$ ein Erzeugendensystem bilden.

Weiter ist

$$\begin{aligned} \mathrm{Ker}(F) &= \{\textstyle\sum_{i=1}^n \lambda_i v_i \mid F\left(\sum_{i=1}^n \lambda_i v_i\right) = 0,\ \lambda_i \in K\} \\ &= \{\textstyle\sum_{i=1}^n \lambda_i v_i \mid \sum_{i=1}^n \lambda_i F(v_i) = 0,\ \lambda_i \in K\} \end{aligned}$$

Somit ist $\mathrm{Ker}(F) = \{0\}$ genau dann, wenn die $F(v_i)$ linear unabhängig sind. ■

Insbesondere sehen wir da ein Erzeugendensystem mindestens so viele Elemente hat wie eine Basis und eine linear unabhängige Familie höchstens so viele Vektoren:

$$\begin{array}{lcl} F \text{ Epimorphismus} & \Rightarrow & \dim V \geq \dim W \\ F \text{ Monomorphismus} & \Rightarrow & \dim V \leq \dim W \\ F \text{ Isomorphismus} & \Rightarrow & \dim V = \dim W \end{array}$$

6.6 Darstellende Matrix eines Homomorphismus

Im letzten Abschnitt haben wir gesehen, dass sich durch Matrixmultiplikation gegebene Homomorphismen $A : K^m \to K^n$ im Computer algorithmisch handhaben lassen. Beispielsweise können wir mit Hilfe des Gaußalgorithmus den Kern als die Lösungsmenge des homogenen linearen Gleichungssystems $Ax = 0$ und allgemeiner das Urbild eines Vektors $b \in K^n$ als die Lösungsmenge des inhomogenen Systems $Ax = b$ bestimmen.

Im Folgenden werden wir dieses Verfahren auf beliebige Vektorraumhomomorphismen (zwischen endlichdimensionalen Vektorräumen) verallgemeinern.

Definition 6.6.1 *Sei $F : V \longrightarrow W$ ein K-Vektorraumhomomorphismus. Für Basen $\Omega = (v_1, ..., v_m)$ von V und $\Delta = (w_1, ..., w_n)$ von W definiere den K-Vektorraumhomomorphismus*

$$M_\Delta^\Omega(F) : K^m \longrightarrow K^n$$

durch

$$M_\Delta^\Omega(F) := \mathrm{co}_\Delta \circ F \circ \mathrm{lc}_\Omega \,.$$

Wir haben also ein Diagramm

$$\begin{array}{ccccc} & V & \xrightarrow{F} & W & \\ \mathrm{lc}_\Omega & \uparrow & & \uparrow & \mathrm{lc}_\Delta \\ & K^m & \underset{M_\Delta^\Omega(F)}{\longrightarrow} & K^n & \end{array}$$

Wegen

$$F = \mathrm{lc}_\Delta \circ M_\Delta^\Omega(F) \circ \mathrm{co}_\Omega$$

können wir F also im Computer wie folgt implementieren: Erst wenden wir den Parser co_Ω an, dann den Homomorphismus $M_\Delta^\Omega(F)$ und schließlich die Ausgaberoutine lc_Δ. Entscheidend für dieses Verfahrens ist, dass sich $M_\Delta^\Omega(F)$ durch Matrixmultiplikation darstellen lässt (und damit der Gaußalgorithmus und die darauf aufbauenden Algorithmen anwendbar sind):

Satz 6.6.2 *Sei $F : K^m \to K^n$ ein Homomorphismus und $A = (a_{i,j}) \in K^{n\times m}$ mit*

$$F(e_j) = \sum_{i=1}^{n} a_{i,j} e_i$$

d.h. in den Spalten von

$$A = (F(e_1) \mid ... \mid F(e_m))$$

stehen die Bilder der Einheitsbasisvektoren. Dann gilt

$$F(c) = A \cdot c.$$

Beweis. Für

$$c = \begin{pmatrix} c_1 \\ \vdots \\ c_m \end{pmatrix} \in K^m$$

ist

$$F(c) = F\left(\sum_{j=1}^{m} c_j e_j\right) = \sum_{j=1}^{m} c_j F(e_j) = \sum_{j=1}^{m} c_j \sum_{i=1}^{n} a_{i,j} e_i$$
$$= \sum_{i=1}^{n} \left(\sum_{j=1}^{m} a_{i,j} c_j\right) e_i = \begin{pmatrix} \left(\sum_{j=1}^{m} a_{1,j} c_j\right) \\ \vdots \\ \left(\sum_{j=1}^{m} a_{n,j} c_j\right) \end{pmatrix} = A \cdot c.$$

■

Jeder Homomorphismus $F : K^m \to K^n$ ist also gegeben durch Multiplikation mit einer $n \times m$-Matrix A.

Definition 6.6.3 *Für einen K-Vektorraumhomomorphismus $F : V \longrightarrow W$ und Basen $\Omega = (v_1, ..., v_m)$ von V und $\Delta = (w_1, ..., w_n)$ von W bezeichnen wir $M_\Delta^\Omega(F) \in K^{n\times m}$ auch als die **darstellende Matrix** von F bezüglich der Basen Ω von V und Δ von W.*

Die darstellende Matrix lässt sich mit der folgenden Bemerkung leicht bestimmen:

Bemerkung 6.6.4 *In der i-ten Spalte von $M_\Delta^\Omega(F)$ stehten die Koeffizienten der Darstellung von $F(v_i)$ bezüglich der Basis Δ.*

Beweis. Die i-te Spalte von $M_\Delta^\Omega(F)$ ist

$$M_\Delta^\Omega(F)(e_i) = (\mathrm{co}_\Delta \circ F \circ \mathrm{lc}_\Omega)(e_i) = (\mathrm{co}_\Delta \circ F)(v_i) = \mathrm{co}_\Delta(F(v_i)),$$

also

$$M_\Delta^\Omega(F) = (\mathrm{co}_\Delta(F(v_1)) \mid \ldots \mid \mathrm{co}_\Delta(F(v_m))) \in K^{n\times m}$$

■

Beispiel 6.6.5 *Betrachte die Ableitung*

$$\tfrac{d}{dx}: \quad \mathbb{R}[x]_{\leq 3} \quad \longrightarrow \quad \mathbb{R}[x]_{\leq 2}$$

und die Basen $\Omega = (1, x, x^2, x^3)$ *und* $\Delta = (1, x, x^2)$. *Dann ist*

$$\frac{d}{dx}(x^s) = s \cdot x^{s-1}$$

also

$$M_\Delta^\Omega(\frac{d}{dx}) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}.$$

Damit berechnen wir z.B.

$$\begin{aligned} \frac{d}{dx}\left(x^3 - 5x^2 + 7x - 11\right) &= \mathrm{lc}_\Delta\left(M_\Delta^\Omega(\frac{d}{dx}) \cdot \mathrm{co}_\Omega\left(x^3 - 5x^2 + 7x - 11\right)\right) \\ &= \mathrm{lc}_\Delta\left(\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix} \cdot \begin{pmatrix} -11 \\ 7 \\ -5 \\ 1 \end{pmatrix}\right) \\ &= \mathrm{lc}_\Delta\begin{pmatrix} 7 \\ -10 \\ 3 \end{pmatrix} = 3x^2 - 10x + 7 \end{aligned}$$

Siehe auch die Übungsaufgaben 6.13 und 6.12.

Die Implementierung eines K-Vektorraumhomomorphismus $F : V \to W$ im Computer können wir also so zusammenfassen: Nachdem co_Δ den Input in V in einen Vektor im K^m umgewandelt hat, wird die eigentliche Berechnung als Multiplikation mit der darstellenden Matrix $M_\Delta^\Omega(F)$ implementiert, und der Output

durch lc_Ω als Vektor in W interpretiert. Dabei kann $M_\Delta^\Omega(F)$ vorausberechnet werden und steht dann für jeden beliebigen Input zur Verfügung.

Auch die Komposition von Vektorraumhomomorphismen lässt sich aus den darstellenden Matrizen bestimmen. Die Idee ist es, die Matrixmultiplikation aus Definition 6.5.4 spaltenweise zu verwenden:

Definition 6.6.6 *Für $A = (a_{i,j}) \in K^{n\times m}$ und $B = (b_{j,l}) \in K^{m\times r}$ definiere das **Matrizenprodukt** durch*

$$A \cdot B := \left(\sum_{j=1}^m a_{i,j}b_{j,l}\right)_{\substack{i=1,\dots,n\\ l=1,\dots,r}} \in K^{n\times r}.$$

Das heißt, sind

$$B = (b_1 \mid \dots \mid b_r)$$

die Spalten von B, so ist

$$A \cdot B = (A \cdot b_1 \mid \dots \mid A \cdot b_r).$$

Siehe auch die Übungsaufgaben 6.9 und 6.15.

Satz 6.6.7 *Betrachte folgende K-Vektorraumhomomorphismen*

$$\begin{array}{ccccc} V & \xrightarrow{F} & W & \xrightarrow{G} & U \\ \mathrm{lc}_\Omega \uparrow & & \mathrm{lc}_\Delta \uparrow & & \uparrow \mathrm{lc}_\Gamma \\ K^r & \xrightarrow[M_\Delta^\Omega(F)]{} & K^m & \xrightarrow[M_\Gamma^\Delta(G)]{} & K^n \end{array}$$

Dann lässt sich die darstellende Matrix der Komposition von G mit F mit dem Matrizenprodukt berechnen als

$$M_\Gamma^\Omega(G \circ F) = M_\Gamma^\Delta(G) \cdot M_\Delta^\Omega(F).$$

Beweis. Folgt als leichte Übung aus der Definition der darstellenden Matrix. ∎

Beispiel 6.6.8 *Für*

$$F = \frac{d}{dx} : \mathbb{R}[x]_{\le 3} \to \mathbb{R}[x]_{\le 2}$$
$$G = \frac{d}{dx} : \mathbb{R}[x]_{\le 2} \to \mathbb{R}[x]_{\le 1}$$

und $\Omega = (1, x, x^2, x^3)$, $\Delta = (1, x, x^2)$, $\Gamma = (1, x)$ *erhalten wir*

$$M_\Sigma^\Omega(G \circ F) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 6 \end{pmatrix}$$

das heißt für die zweite Ableitung $\left(\frac{d}{dx}\right)^2 = G \circ F$ *gilt*

$$\left(\tfrac{d}{dx}\right)^2 1 = 0 \qquad \left(\tfrac{d}{dx}\right)^2 x = 0 \qquad \left(\tfrac{d}{dx}\right)^2 x^2 = 2 \qquad \left(\tfrac{d}{dx}\right)^2 x^3 = 6x.$$

Abschließend bemerken wir noch, dass sowohl die Menge der Homomorphismen zwischen zwei gegebenen Vektorräumen als auch die Menge der Matrizen entsprechender Dimension isomorphe Vektorräume sind.

Bemerkung 6.6.9 *Die Menge der* $n \times m$*-Matrizen* $K^{n\times m}$ *ist ein* K*-Vektorraum durch*

$$(a_{i,j}) + (b_{i,j}) = (a_{i,j} + b_{i,j})$$
$$\lambda \cdot (a_{i,j}) = (\lambda a_{i,j})$$

ebenso die Menge

$$\mathrm{Hom}_K(V, W) = \{F : V \to W \mid F \text{ Vektorraumhomomorphismus}\}$$

der K*-Vektorraumhomomorphismen* $V \to W$ *durch*

$$(f + g)(v) = f(v) + g(v)$$
$$(\lambda \cdot f)(v) = \lambda \cdot f(v)$$

für $f, g \in \mathrm{Hom}_K(V, W)$, $v \in V$ *und* $\lambda \in K$.

Bemerkung 6.6.10 *Mit Satz 6.6.2 folgt dann (leichte Übung)*

$$\mathrm{Hom}_K(K^m, K^n) \cong K^{n\times m},\ F \mapsto (a_{i,j}),$$

wobei

$$F(e_j) = \sum_{i=1}^{n} a_{i,j} e_i$$

für $j = 1, \ldots, m$.

Bemerkung 6.6.11 *Mit dieser Identifikation und Definition 6.6.1 erhalten wir, dass für Basen $\Omega = (v_1, ..., v_m)$ von V und $\Delta = (w_1, ..., w_n)$ von W*

$$\begin{array}{rccc} M_\Delta^\Omega : & \mathrm{Hom}_K(V,W) & \cong & K^{n\times m} \\ & F & \mapsto & M_\Delta^\Omega(F) \end{array}$$

ein Isomorphismus ist. Die Umkehrabbildung

$$\begin{array}{rccc} L_\Delta^\Omega : & K^{n\times m} & \cong & \mathrm{Hom}_K(V,W) \\ & A & \mapsto & L_\Delta^\Omega(A) \end{array}$$

ordnet einer Matrix $A = (a_{ij}) \in K^{n\times m}$ die lineare Abbildung

$$\begin{array}{rccc} L_\Delta^\Omega(A) : & V & \to & W \\ & v & \mapsto & \mathrm{lc}_\Delta\left(A \cdot \mathrm{co}_\Omega(v)\right) \end{array}$$

zu (siehe Beispiel 6.6.5). Für die Details siehe Übungsaufgabe 6.14.

6.7 Inhomogene lineare Gleichungssysteme

In vielen praktischen Anwendungen möchte man (in Verallgemeinerung von homogenen linearen Gleichungssystemen) **inhomogene lineare Gleichungssysteme** der Form

$$\begin{aligned} a_{1,1}x_1 + ... + a_{1,m}x_m &= b_1 \\ &\vdots \\ a_{n,1}x_1 + ... + a_{n,m}x_m &= b_n \end{aligned} \tag{6.1}$$

lösen.

Beispiel 6.7.1 (Lagrange-Interpolation) *Will man alle*

$$f = x_1t^3 + x_2t^2 + x_3t + x_4 \in \mathbb{R}[t]_{\leq 3}$$

finden mit

$$f(-1) = 1,\ f(0) = 0,\ f(2) = 1,$$

so muss man

$$\begin{array}{rcrcrcrcl} -x_1 & + & x_2 & - & x_3 & + & x_4 & = & 1 \\ & & & & & & x_4 & = & 0 \\ 8x_1 & + & 4x_2 & + & 2x_3 & + & x_4 & = & 1 \end{array}$$

lösen.

Mit der Matrix $A = (a_{i,j}) \in K^{n\times m}$ und dem Vektor $b = (b_i) \in K^n$ können wir das inhomogene lineare Gleichungssystem (6.1) mit Hilfe der Matrixmultiplikation auch übersichtlich schreiben als

$$A \cdot x = b$$

wobei $x = (x_j) \in K^m$.

Beispiel 6.7.2 *Das Gleichungssystem aus Beispiel 6.7.1 schreibt sich so als*

$$\underbrace{\begin{pmatrix} -1 & 1 & -1 & 1 \\ 0 & 0 & 0 & 1 \\ 8 & 4 & 2 & 1 \end{pmatrix}}_{A} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \underbrace{\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}}_{b}$$

Notation 6.7.3 *Wir bezeichnen die Lösungsmenge von $A \cdot x = b$ mit*

$$L(A, b) = \{x \in K^m \mid A \cdot x = b\}.$$

Bemerkung 6.7.4 *Mit dem durch die Matrix $A \in K^{n\times m}$ definierten Vektorraumhomomorphismus*

$$A : K^m \to K^n$$

ist

$$L(A, b) = \{x \in K^m \mid A \cdot x = b\} = A^{-1}(\{b\})$$

die Menge der Urbilder von b. Im Fall eines homogenen linearen Gleichungssystems ist $b = 0$ und

$$L(A, 0) = \{x \in K^m \mid A \cdot x = 0\} = \ker(A)$$

ist der Kern von A.

Welche Form haben Lösungsmengen von inhomogenen linearen Gleichungssystemen?

Beispiel 6.7.5 *Sei*

$$A = \begin{pmatrix} 1 & 2 \end{pmatrix} \in \mathbb{R}^{1\times 2} \text{ und } b = 1.$$

Auflösen der entsprechenden inhomogenen linearen Gleichung

$$x_1 + 2x_2 = 1$$

nach $x_1 = 1 - 2x_2$*, gibt die Lösungsmenge*

$$\begin{aligned} L &= \left\{ \begin{pmatrix} 1 - 2x_2 \\ x_2 \end{pmatrix} | x_2 \in \mathbb{R} \right\} \\ &= \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix} + x_2 \begin{pmatrix} -2 \\ 1 \end{pmatrix} | x_2 \in \mathbb{R} \right\} \subset \mathbb{R}^2 \end{aligned}$$

in Abbildung 6.6. Mit

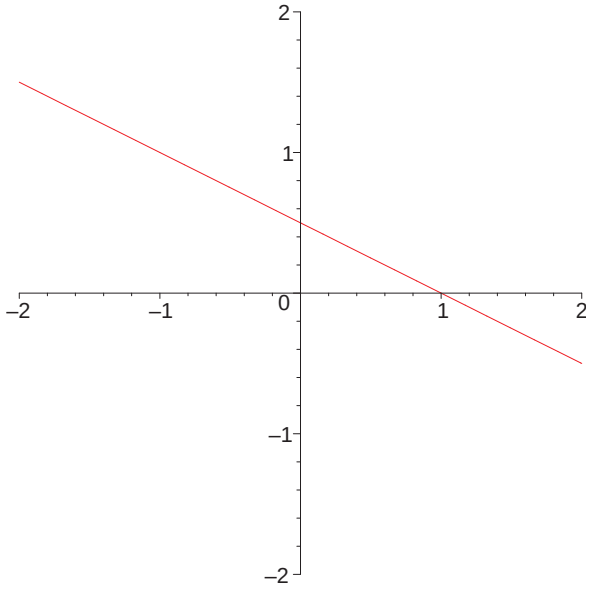


Abbildung 6.6: Affine Gerade

$$c = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ und } U = \left\langle \begin{pmatrix} -2 \\ 1 \end{pmatrix} \right\rangle \subset \mathbb{R}^2$$

lässt sich L *schreiben als die Nebenklasse*

$$L = c + U = \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \left\langle \begin{pmatrix} -2 \\ 1 \end{pmatrix} \right\rangle$$

von c *modulo dem Untervektorraum* $U \subset \mathbb{R}^2$*. Das heißt wir verschieben die Gerade* U *durch* 0 *so parallel, dass sie durch* c *geht. Eine solche Menge bezeichnet man auch als eine* ***affine Gerade****.*

Allgemein definiert man:

Definition 6.7.6 *Ein **affiner Unterraum** von V ist eine Nebenklasse*

$$\overline{v} = v + U$$

*eines Untervektorraums $U \subset V$. Dabei bezeichnen wir den Repräsentanten $v \in V$ als den **Aufpunkt**. Jedes Element von $\overline{v}$ ist ein valider Aufpunkt, denn $\overline{v}$ ist eine Äquivalenzklasse.*

Bemerkung 6.7.7 *Ein affiner Unterraum ist ein Untervektorraum genau dann, wenn er 0 enthält.*

Lösungsmengen von inhomogenen linearen Gleichungssystemen sind affine Unterräume:

Satz 6.7.8 *Sei $A \in K^{n\times m}$ und $b \in K^n$.*

1) *Das inhomogene Gleichungssystem $A\cdot x = b$ ist nach $x \in K^m$ lösbar genau dann, wenn $b \in \mathrm{Bild}(A)$, d.h. wenn b eine Linearkombination der Spalten von A ist.*

2) *Sei $c \in K^m$ eine beliebige Lösung von $A\cdot x = b$. Dann ist die Lösungsmenge der affine Unterraum*

$$L(A,b) = c + \mathrm{Ker}(A) \subset K^m.$$

Beweis. Zu (1): $\mathrm{Bild}(A) = \{A \cdot x \mid x \in K^m\}$
Zu (2): Für $v \in \mathrm{Ker}(A)$ ist

$$A \cdot (c + v) = A \cdot c + 0 = b$$

Gilt umgekehrt $A\cdot x = b$, dann ist $A\cdot(x-c) = 0$, also $x-c \in \mathrm{Ker}(A)$.
■

Wie bestimmt man nun $L(A,b)$ praktisch? Dazu führen wir das Lösen des inhomogenen Gleichungssystems

$$A \cdot x = b$$

für $x_1, \ldots, x_m \in K$ auf die Lösung des homogenen Gleichungssystem

$$A \cdot x - b \cdot x_{m+1} = 0$$

für $x_1, \dots, x_m, x_{m+1} \in K$ zurück. Dieses sogenannte **homogenisierte** System bringen wir zunächst mit dem Gaußalgorithmus aus Abschnitt 6.2 auf reduzierte Zeilenstufenform und bestimmen dann mit Bemerkung 6.3.16 eine Basis des Lösungsvektorraums

$$\begin{pmatrix} c_1 \\ d_1 \end{pmatrix}, \dots, \begin{pmatrix} c_r \\ d_r \end{pmatrix}$$

mit $c_i \in K^m$ und $d_i \in K$. Das heißt wir bestimmen eine Basis des Kerns von

$$A' = (A \mid -b) \in K^{n \times (m+1)}.$$

Es gibt nun zwei Möglichkeiten:

- Ist x_{m+1} eine Leitvariable, dann enthält die reduzierte Zeilenstufenform die Gleichung $x_{m+1} = 0$ und somit liefert Bemerkung 6.3.16 eine Basis mit $d_i = 0$ für alle i, also ist die Basis von der Form

$$\begin{pmatrix} c_1 \\ 0 \end{pmatrix}, \dots, \begin{pmatrix} c_r \\ 0 \end{pmatrix}.$$

- Ist x_{m+1} eine freie Variable, dann gibt es genau ein $d_j = 1$ und allen anderen $d_i = 0$, also ist die Basis von der Form

$$\begin{pmatrix} c_1 \\ 0 \end{pmatrix}, \dots, \begin{pmatrix} c_{j-1} \\ 0 \end{pmatrix}, \begin{pmatrix} c_j \\ 1 \end{pmatrix}, \begin{pmatrix} c_{j+1} \\ 0 \end{pmatrix}, \dots, \begin{pmatrix} c_r \\ 0 \end{pmatrix}$$

In beiden Fällen können wir von dieser Basis können dann direkt die Lösungsmenge ablesen (siehe Algorithmus 6.3). Zur Korrektheit des Algorithmus:

- Ist x_{m+1} eine Leitvariable, so muss einerseits $b \neq 0$ sein (sonst käme x_{m+1} in dem homogenisierten System nicht vor), und andererseits hat jede Lösung von $A \cdot x - b \cdot x_{m+1} = 0$ die Koordinate $x_{m+1} = 0$, d.h. $A \cdot x = 0$ und somit ist $A \cdot x = b \neq 0$ nicht lösbar.

- Ist x_{m+1} eine freie Variable in

$$A \cdot x - b \cdot x_{m+1} = 0$$

Algorithmus 6.3 Löse inhomogenes lineares Gleichungssystem

Input: $A \in K^{n\times m}$, $b \in K^n$

Output: $L(A,b)$

1: Bestimme mit Bemerkung 6.3.16 eine Basis von $\ker(A \mid -b)$

$$\begin{pmatrix} c_1 \\ d_1 \end{pmatrix}, \ldots, \begin{pmatrix} c_r \\ d_r \end{pmatrix}$$

wobei $c_i \in K^m$ und $d_i \in K$.

2: **if** exist j with $d_j = 1$ **then**

3: **return** $L(A,b) = c_j + \langle c_i \mid i \neq j \rangle$

4: **else**

5: **return** $L(A,b) = \varnothing$

dann ist

$$0 = A' \cdot \begin{pmatrix} c_j \\ 1 \end{pmatrix} = A \cdot c_j - b$$

und

$$0 = A' \cdot \begin{pmatrix} c_i \\ 0 \end{pmatrix} = A \cdot c_i$$

für alle $i \neq j$. Korrektheit folgt dann mit Satz 6.7.8.

Man beachte: Ist $b = 0$, so ist x_{m+1} eine freie Variable und die Basis enthält den Einheitsvektor e_{m+1}. Somit erhalten wir $L(A,0) = 0 + \ker A = \ker A$.

Beispiel 6.7.9 *Für die Gleichung*

$$x_1 + 2x_2 = 1$$

aus Beispiel 6.7.5 erhalten wir die homogenisierte Gleichung

$$x_1 + 2x_2 = x_3,$$

äquivalent

$$x_1 + 2x_2 - x_3 = 0.$$

Diese ist als einzelne Gleichung schon in reduzierter Zeilenstufenform, hat Leitvariable x_1, und freie Variablen x_2 und x_2, und eine Basis des Lösungsraums ist

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

also

$$L(A,b) = \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \left\langle \begin{pmatrix} -2 \\ 1 \end{pmatrix} \right\rangle$$

Beispiel 6.7.10 *Im Fall von Beispiel 6.7.1 bestimmen wir im Algorithmus für das homogenisierte System*

$$\begin{array}{rcrcrcrcrcl} -x_1 & + & x_2 & - & x_3 & + & x_4 & - & x_5 & = & 0 \\ & & & & & & x_4 & & & = & 0 \\ 8x_2 & + & 4x_2 & + & 2x_3 & + & x_4 & - & x_5 & = & 0 \end{array}$$

die reduzierte Zeilenstufenform

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

und erhalten damit die Basis des Lösungsraums

$$\begin{pmatrix} -\frac{1}{2} \\ \frac{1}{2} \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} -\frac{1}{4} \\ \frac{3}{4} \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Das inhomogene System hat also die affine Gerade

$$L(A,b) = \begin{pmatrix} -\frac{1}{4} \\ \frac{3}{4} \\ 0 \\ 0 \end{pmatrix} + \left\langle \begin{pmatrix} -\frac{1}{2} \\ \frac{1}{2} \\ 1 \\ 0 \end{pmatrix} \right\rangle$$

als Lösungsmenge. Zur Probe:

$$\begin{pmatrix} -1 & 1 & -1 & 1 \\ 0 & 0 & 0 & 1 \\ 8 & 4 & 2 & 1 \end{pmatrix} \left(\begin{pmatrix} -\frac{1}{4} \\ \frac{3}{4} \\ 0 \\ 0 \end{pmatrix} + \lambda \cdot \begin{pmatrix} -\frac{1}{2} \\ \frac{1}{2} \\ 1 \\ 0 \end{pmatrix} \right) = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$$

für alle $\lambda \in \mathbb{R}$.

Die gesuchten Polynome im Interpolationsproblem aus Beispiel 6.7.1 sind also

$$\left\{ \left(-\frac{1}{4} - \frac{1}{2}\lambda \right) t^3 + \left(\frac{3}{4} + \frac{1}{2}\lambda \right) t^2 + \lambda t \mid \lambda \in \mathbb{R} \right\}$$

In MAPLE *können wir das inhomogene Gleichungssystem mit folgendem Code lösen:*

```
with(LinearAlgebra):
A := <<-1,0,8>|<1,0,4>|<-1,0,2>|<1,1,1>>:
b := <1,0,1>:
LinearSolve(A,b);
```

$$\begin{bmatrix} \frac{1}{2} - t_2 \\ t_2 \\ -\frac{3}{2} + 2t_2 \\ 0 \end{bmatrix}$$

Überprüfen Sie, dass für $t_2 \in \mathbb{R}$ dies genau die oben bestimmte Lösungsmenge $L(A,b)$ beschreibt.

Für weitere Beispiele siehe die Übungen 6.17, 6.18 und 6.11.

6.8 Gauß mit Zeilen- und Spaltentransformationen

Wie im letzten Abschnitt diskutiert, können wir annehmen, dass ein Vektorraumhomomorphismus zwischen endlichdimensionalen K-Vektorräumen durch eine Matrix $A \in K^{n\times m}$ dargestellt ist. Wie in Abschnitt 6.7 beschrieben, können wir dann z.B. den Kern bestimmen als die Lösungsmenge des homogenen linearen Gleichungssystems $A \cdot x = 0$ mit $x \in K^n$. Mittels der Korrespondenz

$$\left.\begin{array}{c} a_{1,1}x_1 + \ldots + a_{1,m}x_m = 0 \\ \vdots \\ a_{n,1}x_1 + \ldots + a_{n,m}x_m = 0 \end{array}\right\} \Longleftrightarrow \overset{A:=}{\begin{pmatrix} a_{1,1} & \cdots & a_{1,m} \\ \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,m} \end{pmatrix}} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = 0$$

zwischen den Koeffizienten der Gleichungen und der Einträge der Matrix A entsprechen die einzelnen Operationen im Gaußalgorithmus den folgenden Operationen mit den Zeilen von A:

Definition 6.8.1 *Die **elementaren Zeilenoperationen** auf A sind:*

1) *Multiplikation der i-ten Gleichung mit $0 \neq \lambda \in K$ entspricht Multiplikation der i-ten Zeile von A mit λ.*

2) *Addition des λ-fachen der i-ten Gleichung zur j-ten Gleichung entspricht Addition des λ-fachen der i-ten Zeile zur j-ten Zeile.*

3) *Vertauschen der i-ten und j-ten Gleichung entspricht Vertauschen der i-ten und j-ten Zeile.*

Statt ein lineares Gleichungssystem in lineare Polynome zu codieren, verwenden wir als Datenstruktur das Array der Koeffizienten dieser Polynome. Die elementaren Zeilenoperationen lassen sich dann durch Matrixmultiplikation realisieren:

Satz 6.8.2 *Sei $A = (a_{i,j}) \in K^{n\times m}$. Die elementaren Zeilenoperationen auf der Matrix A sind dargestellt durch*

$$A \mapsto T \cdot A$$

für die folgenden Isomorphismen $T : K^n \to K^n$:

1) *Multiplikation der i-ten Zeile mit $0 \neq \lambda \in K$ entspricht*

$$T = \begin{array}{c} \\ \\ \\ i \\ \\ \\ \\ \end{array} \begin{pmatrix} 1 & & & & & & 0 \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & \lambda & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ 0 & & & & & & 1 \end{pmatrix} \in K^{n\times n}$$

2) *Addition des λ-fachen der i-ten Zeile zur j-ten Zeile entspricht*

$$T = \begin{array}{c} \\ j \\ \\ \\ \\ \\ \\ \\ i \end{array} \begin{pmatrix} 1 & & & & & & 0 \\ & \ddots & & & & & \\ & & \ddots & & & & \\ & \lambda & & 1 & & & \\ & & & & \ddots & & \\ 0 & & & & & & 1 \end{pmatrix} \in K^{n\times n}$$

3) Vertauschen der i-ten und j-ten Zeile entspricht

$$T = \begin{array}{c} \\ \\ i \\ \\ \\ \\ \\ j \\ \\ \\ \end{array} \begin{pmatrix} 1 & & & & & & & & & & \\ & \ddots & & & & & & & & 0 & \\ & & 1 & & & & & & & & \\ & & & 0 & & & & 1 & & & \\ & & & & 1 & & & & & & \\ & & & & & \ddots & & & & & \\ & & & & & & 1 & & & & \\ & & & 1 & & & & 0 & & & \\ & & & & & & & & 1 & & \\ & 0 & & & & & & & & \ddots & \\ & & & & & & & & & & 1 \end{pmatrix} \in K^{n\times n}$$

Beweis. Folgt direkt aus der Definition des Matrixprodukts: Mit $A = (A_1 \mid \ldots \mid A_m)$ ist

$$T \cdot A = (T \cdot A_1 \mid \ldots \mid T \cdot A_m)$$

und $T \cdot A_i$ ist die Linearkombination der Spalten von T mit den Einträgen des Vektors A_i. Multiplikation von T in (1) kopiert also alle Einträge von A_i aus den i-ten Eintrag, der mit λ multipliziert wird. In den Fällen (2) und (3) argumentiert man analog. Zu jedem T die Umkehrabbildung anzugeben ist ebenso eine leichte Übung. ■

Für jedes dieser T haben nach Bemerkung 6.2.1 $A \cdot x = 0$ und $(T \cdot A) \cdot x = 0$ dieselbe Lösungsmenge $\mathrm{Ker}(A) = \mathrm{Ker}(T \cdot A)$. Allgemein gilt:

Lemma 6.8.3 *Ist $T : K^n \to K^n$ ein Isomorphismus, dann gilt*

$$\mathrm{Ker}(T \cdot A) = \mathrm{Ker}(A).$$

Beweis. Wir haben ein Diagramm

$$\begin{array}{ccc} K^m & \overset{A}{\to} & K^n \\ & {\scriptstyle T\cdot A}\searrow & \downarrow \mathrm{T} \\ & & K^n \end{array}$$

Für $y = A \cdot x$ gilt $T \cdot y = 0$ genau dann, wenn $y = 0$. ■

Der Gaußalgorithmus bestimmt ein solches T als Produkt von elementaren Zeilenoperationen, sodass $\mathrm{Ker}(T \cdot A)$ sofort ablesbar ist. Satz 6.2.4 können wir also auch wie folgt formulieren:

Satz 6.8.4 (Matrix-Gaußalgorithmus) *Sei $A \in K^{n\times m}$. Es gibt einen Isomorphismus $T : K^n \to K^n$, sodass $T \cdot A$* ***Zeilenstufenform*** *hat, d.h.*

$$T \cdot A = \begin{pmatrix} & \overset{j_1}{\boxed{1}} & & \overset{j_2}{} & & \overset{j_r}{} & \\ & & \boxed{1} & & & & * \\ & & & & \ddots & & \\ & & & & & \boxed{1} & \\ 0 & & & & & & \end{pmatrix}$$

Es gilt dann

$$\dim \mathrm{Bild}(A) = r \qquad \dim \mathrm{Ker}(A) = m - r \ ,$$

insbesondere ist

$$\dim \mathrm{Bild}(A) + \dim \mathrm{Ker}(A) = m.$$

Die Variablen $x_{j_1}, ..., x_{j_r}$ sind die Leitvariablen im Gleichungssystem $(T \cdot A) \cdot x = 0$.

Beweis. Mit dem Gaußalgorithmus 6.1 und Satz 6.8.2 gibt es $T_1, ..., T_s$ sodass

$$(T_s \cdot ... \cdot T_1 \cdot A) \cdot x = 0$$

Zeilenstufenform hat. Als Produkt von Isomorphismen ist

$$T = T_s \cdot ... \cdot T_1$$

ein Isomorphismus.

Zu den Dimensionsaussagen: Mit Bemerkung 6.3.16 ist

$$\dim \mathrm{Ker}(A) = m - r.$$

Da T ein Isomorphismus ist, gilt

$$\dim(\mathrm{Bild}(A)) = \dim(\mathrm{Bild}(T \cdot A)).$$

Weiter ist $\mathrm{Bild}(T \cdot A) \subset \langle e_1, ..., e_r \rangle$ und somit $\dim(\mathrm{Bild}(T \cdot A)) \leq r$. Andererseits sind die Spalten $j_1, ..., j_r$ wegen der Stufenform linear unabhängig (leichte Übung mit Algorithmus 6.3.14), und somit $\dim(\mathrm{Bild}(T \cdot A)) \geq r$. ■

Bemerkung 6.8.5 *Durch Zeilenoperationen entsprechend Bemerkung 6.2.8 können wir außerdem noch die Einträge oberhalb der Stufen $a_{i,j_i} = 1$ zu Null machen. Dann spricht man von der* ***reduzierten Zeilenstufenform*** *von A. Diese ist eindeutig bestimmt (ohne Beweis).*

Beispiel 6.8.6 *Für*

$$A = \begin{pmatrix} \mathbf{1} & 1 & 0 & 0 & 1 \\ \mathbf{1} & 1 & 2 & 2 & 1 \\ \mathbf{1} & 1 & 1 & 1 & 1 \end{pmatrix} \in \mathbb{Q}^{3\times 5}$$

erhalten wir durch Abziehen der ersten Zeile von der 2-ten und 3-ten,Multiplikation der 2-ten Zeile mit $\frac{1}{2}$, und Abziehen der 2-ten von der 3-ten Zeile:

$$A \mapsto \begin{pmatrix} \mathbf{1} & 1 & 0 & 0 & 1 \\ 0 & 0 & \mathbf{2} & 2 & 0 \\ 0 & 0 & \mathbf{1} & 1 & 0 \end{pmatrix} \mapsto \begin{pmatrix} \mathbf{1} & 1 & 0 & 0 & 1 \\ 0 & 0 & \mathbf{1} & 1 & 0 \\ 0 & 0 & \mathbf{1} & 1 & 0 \end{pmatrix}$$
$$\mapsto \begin{pmatrix} \mathbf{1} & 1 & 0 & 0 & 1 \\ 0 & 0 & \mathbf{1} & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

In MAPLE *können wir die reduzierte Zeilenstufenform berechnen mit:*

```
with(LinearAlgebra):
A := <<1,1,1>|<1,1,1>|<0,2,1>|<0,2,1>|<1,1,1>>;
GaussianElimination(A);
```

$$\begin{bmatrix} 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 2 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Satz 6.8.7 *Führen wir die Zeilentransformationen zur Bestimmung der reduzierten Zeilenstufenform parallel auch mit der $n\times n$* ***Einheitsmatrix***

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

durch, so erhalten wir ein T wie in Satz 6.8.4.

Beweis. Seien $T_1, ..., T_s \in K^{n\times n}$ die den elementaren Zeilentransformationen entsprechenden Matrizen, sodass

$$\underbrace{T_s \cdot ... \cdot T_1}_{T:=} \cdot A$$

Zeilenstufenform hat. Anwenden der Transformationen auf die Einheitsmatrix gibt

$$T_s \cdot ... \cdot T_1 \cdot E = T_s \cdot ... \cdot T_1 = T.$$

■

Beispiel 6.8.8 *Mit den Zeilentransformationen aus Beispiel 6.8.6 ergibt sich*

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ -1 & 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 \\ -\frac{1}{2} & \frac{1}{2} & 0 \\ -1 & 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 \\ -\frac{1}{2} & \frac{1}{2} & 0 \\ -\frac{1}{2} & -\frac{1}{2} & 1 \end{pmatrix} = T$$

und

$$T \cdot A = \begin{pmatrix} 1 & 0 & 0 \\ -\frac{1}{2} & \frac{1}{2} & 0 \\ -\frac{1}{2} & -\frac{1}{2} & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 2 & 2 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} \mathbf{1} & 1 & 0 & 0 & 1 \\ 0 & 0 & \mathbf{1} & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

hat Zeilenstufenform.

Beispiel 6.8.9 *Wir bestimmen für das Beispiel noch eine Basis von* $\operatorname{Ker} A = \operatorname{Ker}(T \cdot A)$*: Die Lösungsmenge des linearen Gleichungssystems* $(T \cdot A) \cdot x = 0$*, d.h.*

$$\begin{array}{ccccccccc} \boldsymbol{x_1} & + & x_2 & & & & + & x_5 & = & 0 \\ & & & & \boldsymbol{x_3} & + & x_4 & & = & 0 \end{array}$$

ist

$$\operatorname{Ker} A = \left\{ \begin{pmatrix} -x_2 - x_5 \\ x_2 \\ -x_4 \\ x_4 \\ x_5 \end{pmatrix} \mid x_2, x_4, x_5 \in \mathbb{Q} \right\} = \left\langle \begin{pmatrix} -1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ -1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right\rangle$$

In MAPLE *können wir* $\mathrm{Ker}(A)$ *mit folgendem Code bestimmen:*

```
with(LinearAlgebra):
A := <<1,1,1>|<1,1,1>|<0,2,1>|<0,2,1>|<1,1,1>>;
NullSpace(A);
```

$$\left[\begin{bmatrix}-1\\1\\0\\0\\0\end{bmatrix},\begin{bmatrix}0\\0\\-1\\1\\0\end{bmatrix},\begin{bmatrix}-1\\0\\0\\0\\1\end{bmatrix}\right]$$

Mit Hilfe der darstellenden Matrix können wir noch die Dimensionsaussage aus Satz 6.8.4 von Matrizen auf beliebige Homomorphismen übertragen.

Satz 6.8.10 (Dimensionsformel) *Für jeden Vektorraumhomomorphismus* $F : V \to W$ *ist*

$$\dim(V) = \dim \mathrm{Ker}(F) + \dim \mathrm{Bild}(F).$$

Beweis. Für $\dim V = \infty$ ist die Behauptung klar, da dann auch $\dim \mathrm{Ker}(F) = \infty$ oder $\dim \mathrm{Bild}(F) = \infty$. Für $\dim V < \infty$ können wir auch annehmen, dass $\dim W < \infty$, da wir zum Beweis der Aussage sicherlich W durch $\mathrm{Bild}(F)$ ersetzen können. Durch Wahl von Basen Ω von V und Δ von W

$$\begin{array}{ccccc} & V & \xrightarrow{F} & W & \\ \mathrm{lc}_\Omega & \uparrow & & \uparrow & \mathrm{lc}_\Delta \\ & K^m & \xrightarrow[M_\Delta^\Omega(F)]{} & K^n & \end{array}$$

können wir F durch die darstellende Matrix ersetzen, denn durch Einschränken der Isomorphismen lc_Ω und lc_Δ erhalten wir Isomorphismen

$$\begin{aligned} \mathrm{lc}_\Omega &: \mathrm{Ker}(M_\Delta^\Omega(F)) \to \mathrm{Ker}(F) \\ \mathrm{lc}_\Delta &: \mathrm{Bild}(M_\Delta^\Omega(F)) \to \mathrm{Bild}(F). \end{aligned}$$

Mit Satz 6.8.4 folgt dann die Behauptung. ■

Bilder von Matrizen spielen ebenfalls eine wichtige Rolle, denn jeder Untervektorraum von K^n ist das Bild einer Matrix:

Lemma 6.8.11 *Ist*

$$A = (a_1 \mid ... \mid a_m) \in K^{n\times m}$$

mit den Spalten $a_1, ..., a_m$*, so gilt*

$$\text{Bild}(A) = \langle a_1, ..., a_m \rangle .$$

Beweis. Wegen

$$A \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = x_1 \cdot a_1 + ... + x_n \cdot a_n.$$

besteht das Bild von A genau aus allen Linearkombinationen der Spalten von A. ■

Wir kennen also ein Erzeugendensystem des Bildes. Im Folgenden beschreiben wir, wie man eine Basis bestimmt.

Bemerkung 6.8.12 *Führen wir (analog zu Definition 6.8.2) mit* A ***elementare Spaltentransformationen*** *durch, können wir entsprechend eine* ***Spaltenstufenform*** *erreichen.*

Algorithmus 6.4 berechnet dann eine Basis des Bilds. Wir

Algorithmus 6.4 Bild

Input: $A \in K^{n\times m}$

Output: Basis von Bild(A)

1: Berechne mit Bemerkung 6.8.12 eine Spaltenstufenform A' von A.

2: **return** Spalten $\neq 0$ von A'.

zeigen die Korrektheit von Algorithmus 6.4:

Beweis. Für jeden Isomorphismus $S : K^m \to K^m$ gilt

$$\text{Bild}(A) = \text{Bild}(A \cdot S),$$

denn Bild$(S) = K^m$. In unserem Fall ist S eine Komposition von Spaltentransformationen, sodass $A \cdot S$ Spaltenstufenform hat. Die Spalten ungleich 0 in $A \cdot S$ sind per Konstruktion linear unabhängig und somit eine Basis des Bildes. ■

Bemerkung 6.8.13 *Durch weitere Spaltenoperationen können wir eine* ***reduzierte Spaltenstufenform*** *erreichen. Man kann zeigen, dass diese eindeutig durch A bestimmt ist. Damit können wir z.B. Gleichheit von Untervektorräumen entscheiden, denn* $\mathrm{Bild}(A) = \mathrm{Bild}(B)$ *genau dann, wenn die reduzierten Spaltenstufenformen von A und B übereinstimmen.*

Beispiel 6.8.14 *Für A wie in Beispiel 6.8.6 erhalten wir durch Multiplikation der 3-ten und 4-ten Spalte mit $\frac{1}{2}$, Abziehen der ersten Spalte von der 2-ten und 5-ten, Abziehen der 3-ten von der 4-ten, Vertauschen der 2-ten und 3-ten Spalte und Abziehen der 2-ten von der 1-ten*

$$A = \begin{pmatrix} \mathbf{1} & \mathbf{1} & 0 & 0 & \mathbf{1} \\ 1 & 1 & \mathbf{2} & \mathbf{2} & 1 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix} \mapsto \begin{pmatrix} \mathbf{1} & \mathbf{1} & 0 & 0 & \mathbf{1} \\ 1 & 1 & \mathbf{1} & \mathbf{1} & 1 \\ 1 & 1 & \frac{1}{2} & \frac{1}{2} & 1 \end{pmatrix}$$
$$\mapsto \begin{pmatrix} \mathbf{1} & 0 & 0 & 0 & 0 \\ 1 & 0 & \mathbf{1} & 0 & 0 \\ 1 & 0 & \frac{1}{2} & 0 & 0 \end{pmatrix} \mapsto \begin{pmatrix} \mathbf{1} & 0 & 0 & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 & 0 \\ \frac{1}{2} & \frac{1}{2} & 0 & 0 & 0 \end{pmatrix}$$

und somit eine Basis des Bilds

$$\mathrm{Bild}(A) = \left\langle \begin{pmatrix} 1 \\ 0 \\ \frac{1}{2} \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ \frac{1}{2} \end{pmatrix} \right\rangle$$

In Maple *können wir* $\mathrm{Bild}(A)$ *wie folgt berechnen:*

```
with(LinearAlgebra):
A := <<1,1,1>|<1,1,1>|<0,2,1>|<0,2,1>|<1,1,1>>;
ColumnSpace(A);
```

$$\left[\begin{bmatrix} 1 \\ 0 \\ \frac{1}{2} \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ \frac{1}{2} \end{bmatrix}\right]$$

6.9 Homomorphiesatz

Sei V ein K-Vektorraum. Ein Untervektorraum $U \subset V$ ist insbesondere eine Untergruppe von $(V, +)$.

Definition und Satz 6.9.1 *Die Quotientengruppe V/U ist ein K-Vektorraum mit*

$$\lambda\overline{v} = \overline{\lambda v}$$

für $\lambda \in K$ und $v \in V$, der ***Quotientenvektorraum****.*

Satz 6.9.2 (Homomorphiesatz) *Sei $F : V \to W$ ein Vektorraumhomomorphismus. Dann gilt*

$$V/\operatorname{Ker}(F) \cong \operatorname{Bild}(F)$$

Beweis. Für die Gruppenstruktur bezüglich + haben wir dies schon in Satz 4.3.11 gezeigt. Weiter ist

$$\widetilde{F} : V/\operatorname{Ker}(F) \to \operatorname{Bild}(F),\ \overline{v} \mapsto F(v)$$

ein Vektorraumhomomorphismus, denn

$$\widetilde{F}(\lambda \cdot \overline{v}) = \widetilde{F}(\overline{\lambda \cdot v}) = F(\lambda \cdot v) = \lambda \cdot F(v) = \lambda \cdot \widetilde{F}(\overline{v})$$

für $\lambda \in K$. ■

Corollar 6.9.3 *Für $\dim V < \infty$ gilt*

$$\dim(V/U) = \dim(V) - \dim(U).$$

Beweis. Für $F : V \to V/U$, $v \mapsto \overline{v}$ gilt $\operatorname{Ker}(F) = U$ und $\operatorname{Bild}(F) = V/U$. Mit dem Homomorphiesatz 6.9.2 und Satz 6.8.10 folgt die Behauptung. ■

Die Elemente $\overline{v} \in V/U$ des Quotientenvektorraums sind affine Unterräume von V, d.h.

$$\overline{v} = v + U.$$

Betrachten wir inhomogene Gleichungssysteme noch einmal von einem höheren Standpunkt:

Bemerkung 6.9.4 *Mit Hilfe des Quotientenvektorraums lässt sich die Aussage von Satz 6.7.8 elegant formulieren: Nach Satz 6.9.2 ist*

$$\begin{array}{rccc} \widetilde{A}: & K^m/\operatorname{Ker}(A) & \to & \operatorname{Bild}(A) \\ & \overline{x} & \mapsto & A \cdot x \end{array}$$

ein Isomorphismus.

Sei $b \in K^n$. Ist $A \cdot x = b$ lösbar, d.h. $b \in \mathrm{Bild}(A)$, dann hat b ein eindeutiges Urbild

$$\overline{c} := \widetilde{A}^{-1}(b) \in K^m / \mathrm{Ker}(A).$$

Dieser affine Unterraum von K^m ist genau die Lösungsmenge von $A \cdot x = b$, denn $A \cdot c = b$ und somit

$$\begin{aligned} \overline{c} &= c + \mathrm{Ker}\, A = \{c + v \mid v \in \mathrm{Ker}(A)\} \\ &= L(A, b) \subset K^m \end{aligned}$$

Die Klasse $\overline{c}$ (d.h. die affine Ebene) ist eindeutig bestimmt, nicht aber der Aufpunkt c.

Beispiel 6.9.5 *Für*

$$A = \begin{pmatrix} 1 & 2 \end{pmatrix} \in \mathbb{R}^{1\times 2} \text{ und } b = 1.$$

ist das eindeutige Urbild von $b = 1$ unter

$$\begin{array}{rccc} \widetilde{A}: & K^m/\mathrm{Ker}(A) & \to & \mathrm{Bild}(A) \\ & \overline{\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}} & \mapsto & x_1 + 2x_2 \end{array}$$

die Nebenklasse

$$\widetilde{A}^{-1}(1) = \overline{\begin{pmatrix} 1 \\ 0 \end{pmatrix}} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \left\langle \begin{pmatrix} -2 \\ 1 \end{pmatrix} \right\rangle = L(A, b),$$

d.h. die affine Gerade in Abbildung 6.6.

6.10 Isomorphismen

Die Matrix T, die im Gauß-Algorithmus 6.8.4 die elementaren Zeilentransformationen zusammenfasst, ist ein Beispiel eines Vektorraumisomorphismus. Sie identifiziert die Standardbasis von K^n mit einer anderen Basis von K^n (die in den Spalten von T steht). Allgemein gilt (Bemerkung 6.5.9): Ist $F : V \to W$ ein Homomorphismus und $\Omega = (v_1, ..., v_n)$ eine Basis von V, dann ist

$$F \text{ Isomorphismus} \Leftrightarrow (F(v_1), ..., F(v_n)) \text{ Basis von } W,$$

insbesondere also

$$\dim V = \dim W$$

und damit die darstellende Matrix $M_\Delta^\Omega(F)$ für jede Wahl von Basen Ω von V und Δ von W quadratisch.

Definition 6.10.1 *Eine Matrix $A \in K^{n\times n}$ heißt **invertierbar**, wenn der Homomorphismus $K^n \to K^n$, $x \mapsto A\cdot x$ ein Isomorphismus ist.*

Die Umkehrabbildung von A ist wieder ein Isomorphismus und somit durch eine eindeutig bestimmte invertierbare Matrix $A^{-1} \in K^{n\times n}$ gegeben. Die identische Abbildung $\mathrm{id} : K^n \to K^n$ ist gegeben durch die $n \times n$-Einheitsmatrix

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

Somit gilt (mit Satz 2.3.21 über die Umkehrabbildung und Satz 6.6.7 über die Komposition von Homomorphismen) als Produkt von Matrizen

$$A \cdot A^{-1} = E.$$
$$A^{-1} \cdot A = E.$$

Weiter ist die Komposition von zwei Isomorphismen wieder ein Isomorphismus. Damit folgt:

Satz 6.10.2 *Die Menge der invertierbaren Matrizen*

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

*bildet bezüglich der Multiplikation von Matrizen eine Gruppe, die **allgemeine lineare Gruppe** (general linear group). Das neutrale Element ist die Einheitsmatrix*

Bemerkung 6.10.3 *Man beachte, dass $\mathrm{GL}(n,K)$ für $n \geq 2$ nicht kommutativ ist, z.B.*

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

Mit Bemerkung 4.2.3.(3) erhalten wir die Inverse des Produkts von $A, B \in \mathrm{GL}(n,K)$ als

$$(A \cdot B)^{-1} = B^{-1} \cdot A^{-1}.$$

Algorithmus 6.5 berechnet mit dem Gaußalgorithmus die Inverse von $A \in \mathrm{GL}(n, K)$: Wegen Satz 6.8.4 und $\dim \ker(A) = 0$ hat die reduzierte Zeilenstufenform von A genau n Einträge 1 auf der Diagonalen, ist also die Einheitsmatrix E.

Algorithmus 6.5 Inverse

Input: $A \in \mathrm{GL}(n, K)$
Output: A^{-1}

1: Bestimme mit Satz 6.8.4 und Satz 6.8.7 ein $T \in K^{n \times n}$ mit $T \cdot A$ in reduzierter Zeilenstufenform, also $T \cdot A = E$.
2: **return** T.

Insbesondere zeigt dies: Jede invertierbare Matrix ist das Produkt von elementaren Zeilentransformationen (d.h. von Matrizen T wie in Definition 6.8.2). Oder anders ausgedrückt: Die Gruppe $\mathrm{GL}(n, K)$ wird von der Menge aller dieser Matrizen erzeugt.

Beispiel 6.10.4 *Wir bestimmen die Inverse von*

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

indem wir die Zeilentransformationen parallel auf E ausführen:

$$A = \begin{pmatrix} 1 & 0 & 0 \\ -\frac{1}{2} & \frac{1}{2} & 0 \\ -\frac{1}{2} & -\frac{1}{2} & 1 \end{pmatrix} \qquad E = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{2} & 0 \\ 0 & -\frac{1}{2} & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 & 0 \\ \frac{1}{2} & 1 & 0 \\ \frac{1}{2} & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{2} & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 & 0 \\ \frac{1}{2} & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

$$E = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad A^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 2 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

Dann gilt tatsächlich

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

Siehe auch die Aufgaben 6.21 und 6.22.

Für inhomogene lineare Gleichungssysteme $A \cdot x = b$ mit $A \in K^{n\times n}$ invertierbar kann man mit der Inversen eine Lösungsformel angeben:

Bemerkung 6.10.5 *Sei $A \in \mathrm{GL}(n, K)$ und $b \in K^n$. Dann gilt hat $A \cdot x = b$ eine eindeutige Lösung, und diese können wir berechnen als*

$$x = A^{-1} \cdot b.$$

Beweis. Es gilt

$$x = E \cdot x = A^{-1} \cdot A \cdot x = A^{-1} \cdot b.$$

■

Beispiel 6.10.6 *Um (wie in Beispiel 5.14.5) alle Polynome*

$$f = x_1 t^2 + x_2 t + x_3 \in \mathbb{R}[t]_{\leq 2}$$

zu finden mit

$$f(-1) = 1,\ f(0) = 0,\ f(2) = 1$$

bestimmen wir die Lösungsmenge $L(A, b)$ von

$$\begin{aligned} x_1 - x_2 + x_3 &= 1 \\ x_3 &= 0 \\ 4x_1 + 2x_2 + x_3 &= 1 \end{aligned}$$

d.h. von

$$\underbrace{\begin{pmatrix} 1 & -1 & 1 \\ 0 & 0 & 1 \\ 4 & 2 & 1 \end{pmatrix}}_{A} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \underbrace{\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}}_{b}$$

Die eindeutige Lösung ist

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \underbrace{\begin{pmatrix} \frac{1}{3} & -\frac{1}{2} & \frac{1}{6} \\ -\frac{2}{3} & \frac{1}{2} & \frac{1}{6} \\ 0 & 1 & 0 \end{pmatrix}}_{A^{-1}} \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{2} \\ -\frac{1}{2} \\ 0 \end{pmatrix}$$

entsprechend dem Polynom

$$f = \frac{1}{2}t^2 - \frac{1}{2}t.$$

Man beachte, dass dieses Polynom in dem Lösungsraum von Beispiel 6.7.10 enthalten ist (für $\lambda = -\frac{1}{2}$).

Invertierbare Matrizen verwenden wir z.B., um aus der darstellenden Matrix eines Homomorphismus eine darstellende Matrix bezüglich anderer Basen zu berechnen:

6.11 Basiswechsel

Wie in Satz 6.6.2 gezeigt, lässt sich jeder Homomorphismus $K^m \to K^n$ durch eine Matrix $A \in K^{n\times m}$ darstellen. In der i-ten Spalte von A steht die Darstellung des Bildes des i-ten Einheitsbasisvektors $e_i \in K^m$ bezüglich der Einheitsbasis von K^n. In der Praxis kann es aber oft nützlich sein, A bezüglich anderer Basen $\Omega = (v_1, ..., v_m)$ von K^m und $\Delta = (w_1, ..., w_n)$ und K^n darzustellen.

Hat z.B. die darstellende Matrix viele Nulleinträge, dann lässt sich die Matrix effizient im Computer speichern (als sogenannte **sparse matrix**, bestehend aus den Positionen und Werten der Einträge $\neq 0$) und die Matrixmultiplikation schnell berechnen.

Die darstellende Matrix kann man wie folgt bestimmen: Die Linearkombinationsabbildung

$$\mathrm{lc}_\Omega : K^m \to K^m$$

ist (mit Beispiel 6.5.2.(1)) ein Isomorphismus und wird als **Basiswechsel** bezeichnet. Da

$$\mathrm{lc}_\Omega \begin{pmatrix} c_1 \\ \vdots \\ c_m \end{pmatrix} = c_1 \cdot v_1 + ... + c_m \cdot v_m = (v_1 \mid ... \mid v_m) \cdot \begin{pmatrix} c_1 \\ \vdots \\ c_m \end{pmatrix}$$

können wir lc_Ω (nach Satz 6.6.2) mit der invertierbaren Matrix

$$\mathrm{lc}_\Omega = (v_1 \mid ... \mid v_m) \in \mathrm{GL}(m, K)$$

identifizieren, in deren Spalten die Basisvektoren v_i stehen. Genauso ist als Matrix geschrieben

$$\mathrm{lc}_\Delta = (w_1 \mid ... \mid w_n) \in \mathrm{GL}(n, K).$$

Das Diagramm aus Definition 6.6.1 wird dann zu

$$\begin{array}{ccccc} & & K^m & \xrightarrow{A} & K^n & & \\ (v_1 \mid ... \mid v_m) & & \uparrow & & \uparrow & & (w_1 \mid ... \mid w_n) \\ & & K^m & \xrightarrow[M_\Delta^\Omega(A)]{} & K^n & & \end{array}$$

(wobei alle Abbildungen durch Matrixmultiplikation gegeben sind) und es gilt (mit Satz 6.6.7):

Satz 6.11.1 (Basiswechsel) *Ist $A \in K^{n\times m}$ und $\Omega = (v_1, ..., v_m)$ von K^m und $\Delta = (w_1, ..., w_n)$ Basen von K^n, so gilt*

$$M_\Delta^\Omega(A) = (w_1 \mid ... \mid w_n)^{-1} \cdot A \cdot (v_1 \mid ... \mid v_m).$$

Beispiel 6.11.2 *Für*

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

wie in Beispiel 6.8.6 und

$$\Omega = \left(\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ -1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right)$$

$$\Delta = \left(\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right)$$

erhalten wir (mit Beispiel 6.10.4)

$$M_\Delta^\Omega(A) = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 2 & 0 \\ 1 & 1 & 1 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 2 & 2 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & -1 & 0 & -1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 0 & 0 \\ -\frac{1}{2} & \frac{1}{2} & 0 \\ -\frac{1}{2} & -\frac{1}{2} & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Bezüglich geeignet gewählter neuer Basen hat A also eine wesentlich einfachere Darstellung. Siehe auch die Aufgaben 6.24 und 6.12.

Solche Basen kann man systematisch mit dem Gaußalgorithmus finden:

6.12 Klassifikation von Homomorphismen

Satz 6.12.1 (Klassifikationssatz) *Sei $A \in K^{n\times m}$. Dann gibt es $S \in \mathrm{GL}(m,K)$ und $T \in \mathrm{GL}(n,K)$, sodass $T \cdot A \cdot S$ die* ***Normalform***

$$T \cdot A \cdot S = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}$$

hat, wobei $r = \operatorname{rk} A$ und E_r die $r \times r$ Einheitsmatrix bezeichnet.

Beweis. Durch elementare Zeilentransformationen bringen wir A auf reduzierte Zeilenstufenform. Führen wir die Transformationen parallel mit $E \in \mathrm{GL}(n,K)$ aus, so erhalten wir T. Durch elementare Spaltentransformationen bringen wir dann $T \cdot A$ in die obige Form. Führen wir die Transformationen parallel mit $E \in \mathrm{GL}(m,K)$ aus, so erhalten wir S. ∎

In der Notation von Bemerkung 6.11.1 steht in den Spalten von T^{-1} die Basis Δ, in den Spalten von S die Basis Ω.

Von der Normalform in Satz 6.12.1 können wir nochmals ganz direkt ablesen, dass

$$\dim \mathrm{Bild}(A) + \dim \mathrm{Ker}(A) = r + (m - r) = m,$$

denn $\mathrm{Bild}(F) = \langle e_1, ..., e_r \rangle \subset K^n$ und $\mathrm{Ker}(F) = \langle e_{r+1}, ..., e_m \rangle \subset K^m$.

Beispiel 6.12.2 *In Beispiel 6.8.8 erhalten wir für*

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

durch Zeilentransformationen

$$T = \begin{pmatrix} 1 & 0 & 0 \\ -\frac{1}{2} & \frac{1}{2} & 0 \\ -\frac{1}{2} & -\frac{1}{2} & 1 \end{pmatrix} \in \mathrm{GL}(3, \mathbb{Q})$$

sodass

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

reduzierte Zeilenstufenform hat. Spaltentransformationen geben dann

$$T \cdot A = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \qquad E = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \qquad \begin{pmatrix} 1 & -1 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \qquad S = \begin{pmatrix} 1 & 0 & -1 & 0 & -1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

und es gilt

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

wie schon in Beispiel gezeigt. Siehe auch die Aufgaben 6.25 und 6.26.

Wir fassen zusammen:

Elementare Transformationen auf den		Bestimmung von
Zeilen	$\longleftrightarrow$	Kern
Spalten	$\longleftrightarrow$	Bild
Zeilen und Spalten	$\longleftrightarrow$	Normalform

Elementare Zeilentransformationen ändern den Kern der Matrix nicht, elementare Spaltentransformationen das Bild nicht, beide ändern die Normalform der Matrix nicht (d.h. wenden wir elementare Zeilen- oder Spaltentransformationen auf eine Matrix an, dann hat die modifizierte Matrix dieselbe Normalform wie die Ursprungsmatrix).

6.13 Anwendung: Lineare Codes

6.13.1 Setup

Bei der Übertragung, Verarbeitung und Speicherung von Daten entstehen durch physikalische Prozesse Fehler. Digitaltechnik können wir auffassen als Algebra über $\mathbb{F}_2 = \mathbb{Z}/2$, Analogtechnik dagegen als Algebra über $\mathbb{R}$. Somit sollten Analogrechner den digitalen überlegen sein, denn diese können reelle Zahlen stets nur mit rationalen Zahlen approximieren. Dass Analogrechner[1] heute in der Computertechnik keine wesentliche Rolle mehr spielen, liegt u.a. an der Möglichkeit, Fehler in digitalen Daten zu

[1] Analogrechner können zum Beispiel sehr gut integrieren. Die einfachste Implementation wäre folgende: Zur Bestimmung des Integrals einer nichtnegativen Funktion variieren wir mit dem Funktionswert die Durchflussrate einer Wasserleitung in ein Sammelbecken und bestimmen am Ende des Integrationsintervalls die Flüssigkeitsmenge. Üblicherweise arbeitet man jedoch mit elektrischen Spannungen.

korrigieren und damit eindeutig bestimmte, reproduzierbare Ergebnisse zu erhalten.

Als Beispiel wollen wir hier lineare Codes über

$$K = \mathbb{F}_2$$

behandeln: Um m Bits in $n \geq m$ Bits zu codieren (mit $n - m$ Kontrollbits oder **Paritätsbits**) betrachten wir eine Matrix

$$G \in K^{n \times m}$$

von maximalem Rang $\operatorname{rk} G = m$. Die Matrix heißt **Generatormatrix** des Codes und definiert einen Monomorphismus

$$G : K^m \to K^n$$

denn mit Satz 6.8.4 ist

$$\dim \operatorname{Ker}(G) = m - \dim \operatorname{Bild}(G) = 0.$$

Somit ist die Abbildung

$$G : K^m \to \operatorname{Bild}(G)$$

bijektiv. Den Code können wir bis auf Wahl einer Basis (Spalten von G) mit dem Untervektorraum

$$U = \operatorname{Bild}(G) \subset K^n$$

identifizieren.

Definition 6.13.1 *Ein **linearer Code** ist ein Untervektorraum $U \subset K^n$.*

Um einen Datenvektor $v \in K^m$ in $c \in K^n$ zu codieren, verwenden wir die Abbildung G:

$$v \mapsto c = G \cdot v$$

Man beachte, dass in dem Vektor c die Kontrollbits i.A. keine ausgezeichnete Position haben.

Zum Dekodieren bestimmt der Empfänger für $c \in K^n$ die eindeutige Lösung $v \in K^n$ des linearen Gleichungssystems

$$G \cdot v = c$$

Bei der Übertragung kann allerdings der codierte Vektor c zu $c' \in K^n$ verfälscht werden. Um einen eventuellen Fehler

$$e = c' - c \in K^n$$

zu erkennen, gehen wir wie folgt vor:

6.13.2 Fehlererkennung

Wir betrachten $c' \in K^n$ als korrekt, falls

$$c' \in \text{Bild}(G)$$

d.h. falls

$$G \cdot v = c'$$

lösbar ist. Effizienter lässt sich dies durch eine Matrixmultiplikation überprüfen, indem wir $\text{Bild}(G)$ als Lösungsmenge eines homogenen linearen Gleichungssystems darstellen, d.h.

$$\text{Bild}(G) = \text{Ker}(H)$$

schreiben mit einer geeigneten Matrix H. Um diese zu bestimmen, benötigen wir folgende Definitionen und Resultate (die über jedem Körper K gelten):

Definition 6.13.2 *Für $A = (a_{i,j}) \in K^{n\times m}$ ist die **Transponierte** $A^t = (a_{j,i}) \in K^{m\times n}$.*

Beispiel 6.13.3 *Für*

$$A = \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix}$$

ist

$$A^t = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}.$$

Bemerkung 6.13.4 *Für $A \in K^{n\times m}$ und $B \in K^{m\times s}$ gilt*

$$(A \cdot B)^t = B^t \cdot A^t$$

Der Beweis ist eine leichte Übung. Siehe auch Übung 6.32.

Satz 6.13.5 *Für $A \in K^{n\times m}$ gilt*

$$\text{rk}\, A = \text{rk}\, A^t$$

Beweis. Mit der Normalform gemäß Satz 6.12.1

$$T \cdot A \cdot S = \begin{pmatrix} E_s & 0 \\ 0 & 0 \end{pmatrix} \in K^{m \times n}$$

ist

$$S^t \cdot A^t \cdot T^t = \begin{pmatrix} E_s & 0 \\ 0 & 0 \end{pmatrix} \in K^{n \times m}$$

also

$$\operatorname{rk} A = \dim \operatorname{Bild}(A) = s = \dim \operatorname{Bild}(A^t) = \operatorname{rk} A^t$$

■

Satz 6.13.6 *Sei* $A \in K^{n \times m}$ *mit* $\operatorname{rk} A = m \leq n$, *also*

$$\dim \operatorname{Ker}(A^t) = n - m.$$

Schreiben wir eine Basis von $\operatorname{Ker}(A^t)$ *in die Spalten von*

$$W \in K^{n \times (n-m)}$$

dann gilt

$$\operatorname{Ker}(A^t) = \operatorname{Bild}(W)$$

und

$$\operatorname{Bild}(A) = \operatorname{Ker}(W^t)$$

Beweis. Nach Konstruktion von W ist $\operatorname{Ker}(A^t) = \operatorname{Bild}(W)$ klar. Damit folgt

$$W^t \cdot A = (A^t \cdot W)^t = 0$$

also $\operatorname{Bild}(A) \subset \operatorname{Ker}(W^t)$. Nach Konstruktion ist

$$\dim \operatorname{Bild}(W) = \dim \operatorname{Ker}(A^t) = n - m.$$

Mit Satz 6.8.10 und Satz 6.13.5 gilt also

$$\begin{aligned} \dim \operatorname{Ker}(W^t) &= n - \dim \operatorname{Bild}(W^t) = n - \dim \operatorname{Bild}(W) \\ &= n - (n - m) = m = \dim \operatorname{Bild}(A) \end{aligned}$$

und damit $\operatorname{Bild}(A) = \operatorname{Ker}(W^t)$ nach Corollar 6.4.15. ■

Wir wenden dies nun auf die Generatormatrix G eines linearen Codes über $K = \mathbb{F}_2$ an:

Definition 6.13.7 *Für die Generatormatrix $G \in K^{n\times m}$ heißt $H \in K^{(n-m)\times n}$ mit*

$$\mathrm{Bild}(G) = \mathrm{Ker}(H)$$

die ***Kontrollmatrix*** *des Codes. Es ist*

$$c' \in \mathrm{Bild}(G) \Leftrightarrow H \cdot c' = 0$$

Beispiel 6.13.8 *Für die Generatormatrix*

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

ist

$$\mathrm{Ker}(G^t) = \mathrm{Ker}\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} = \left\langle \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \right\rangle$$

also

$$H = (1, 1, 1)$$

die Kontrollmatrix. Wir haben also Abbildungen

$$K^2 \xrightarrow{G} K^3 \xrightarrow{H} K$$

mit $\mathrm{Ker}(H) = \mathrm{Bild}(G)$*. Zum Codieren verwenden wir die Abbildung*

$$\begin{array}{rccc} G: & K^2 & \to & K^3 \\ & \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} & \mapsto & \begin{pmatrix} v_1 \\ v_2 \\ v_1 + v_2 \end{pmatrix} \end{array}$$

d.h. wir übertragen zusätzlich zu den Datenbits v_1 und v_2 das Paritätsbit

$$v_3 = v_1 + v_2.$$

Zur Fehlererkennung verwenden wir dann die Abbildung

$$\begin{array}{rccc} H: & K^3 & \to & K \\ & \begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix} & \mapsto & c_1 + c_2 + c_3 \end{array}$$

Den empfangenen Datenvektor

$$c = \begin{pmatrix} c_1 \\ c_2 \\ c_2 \end{pmatrix} \in K^3$$

halten wir für korrekt, wenn $H \cdot c = 0$, *d.h.*

$$c_1 + c_2 + c_3 = 0$$

erfüllt. Beispielsweise wird

$$v = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad \textit{codiert in} \quad c = G \cdot v = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$$

Stören wir c *in*

$$c' = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \quad \textit{so gilt} \quad H \cdot c' = 1 \neq 0$$

und wir erkennen den Fehler.

Wie kann man quantifizieren, vieviele Fehler ein Code erkennen kann?

Definition 6.13.9 *Der* ***Hammingabstand*** *von* $a, b \in K^n$ *ist*

$$d(a,b) = |\{i \mid a_i \neq b_i\}|$$

d.h. die Anzahl der Bits in denen sich a *und* b *unterscheiden. Der den* ***Minimalabstand*** *von zwei Punkten des Codes* $U = \mathrm{Bild}(G) \subset K^n$ *ist*

$$d_{min}(U) := \min\{d(a,b) \mid a, b \in U,\ a \neq b\}\,.$$

Wird $c = G \cdot v$ zu c' in maximal r Bits verfälscht, aber der Fehler nicht erkannt, d.h. ist $c' \in U = \mathrm{Bild}(G)$, dann gilt für den Minimalabstand des Codes $d_{min}(U) \leq d(c,c') \leq r$. Umgekehrt, ist $d_{min}(U) \leq r$, so gibt es ein c und ein c' mit r Fehlern, das nicht als falsch erkannt wird. Somit ist die folgende Bezeichung sinnvoll:

Definition 6.13.10 *Ein Code* $U = \text{Bild}(G) \subset K^n$ *heißt* r-***fehlererkennend****, wenn*

$$d_{min}(U) \geq r + 1.$$

Für einen linearen Code U gilt

$$d(a, b) = d(a + w, b + w)$$

für alle $a, b, w \in U$, und somit können wir den Minimalabstand berechnen als

$$d_{min}(U) = \min \{d(a, 0) \mid 0 \neq a \in U\}.$$

Beispiel 6.13.11 *Der Code aus Beispiel 6.13.8 ist*

$$U = \text{Bild} \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{pmatrix} = \left\{ \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} \right\}$$

Damit ist der Minimalabstand $d_{min}(U) = 2$*. Der Code ist also* 1*-fehlererkennend. Treten jedoch zwei Bitfehler auf, so fällt dies nicht auf. Wir können auch nicht feststellen, welches Bit verfälscht wurde. Allerdings lässt sich ein fehlendes Bit (bekannter Position) rekonstruieren (vorausgesetzt die restlichen sind korrekt). Ein ähnliches Verfahren wird auch bei der* ***ISBN-Nummer*** *(internationale Standardbuchnummer) im Buchhandel eingesetzt, siehe Übungsaufgabe 6.30.*

6.13.3 Fehlerkorrektur

Wir diskutieren nun, wie ein erkannter Fehler korrigiert werden kann. Zum Decodieren von $c' \in K^n$ gehen wir allgemein wie folgt vor:

Bestimme ein $c \in \text{Bild}(G)$ mit $d(c, c')$ minimal.

Inbesondere für $c' \in \text{Bild}(G)$ ist also $c = c'$. Oder ausgedrückt mit der Kontrollmatrix H und dem Fehler $e = c' - c$:

Bestimme ein $e \in K^n$ mit $d(e, 0)$ minimal und $He = Hc'$.

Beachte dabei, dass $d(e, 0) = d(c', c)$ und $Hc = 0 \Leftrightarrow He = Hc'$. Schließlich berechnen wir das eindeutige $v \in K^m$ mit $G \cdot v = c$. Dieses Verfahren bezeichnet man als **Nearest-Neighbour-Dekodierung**.

Definition 6.13.12 *Der Code U heißt r-**fehlerkorrigierend**, wenn es für alle $c' \in K^n$ maximal ein $c \in U$ gibt mit $d(c, c') \leq r$.*

Die Bezeichnung ist sinnvoll: Wird also c in höchstens r Bits zu c' gestört, dann liefert die Nearest-Neighbour-Dekodierung angewendet auf c' wieder c zurück.

Lemma 6.13.13 *Der Code U ist r-fehlerkorrigierend, falls*

$$d_{min}(U) \geq 2r + 1$$

Beweis. Gibt es ein $w \in K^n$ und $v, u \in U$, $v \neq u$ mit

$$d(w, u) \leq r \text{ und } d(w, v) \leq r$$

dann ist

$$d(u, v) \leq d(u, w) + d(w, v) = 2r,$$

ein Widerspruch zu $d_{min}(U) \geq 2r + 1$.

Dabei verwenden wir, dass der Hammingabstand die **Dreiecksungleichung**

$$d(u, w) + d(w, v) \geq d(u, v)$$

für alle $u, v, w \in K^n$ erfüllt (Übung). Diese ist ein wesentlicher Bestandteil einer vernünftigen Abstandsdefinition (neben den Eigenschaften $d(u, v) \geq 0$, $d(u, v) = d(v, u)$ und $d(u, v) = 0 \Leftrightarrow u = v$ für alle $u, v \in K^n$). Siehe Abbildung 6.7 für die Dreiecksungleichung im Fall des Euklidischen Abstands auf $\mathbb{R}^2$.

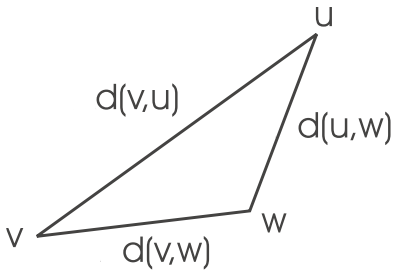


Abbildung 6.7: Dreiecksungleichung

■

Wir diskutieren nun einen Code, der einen Fehler korrigieren kann, d.h. 1-fehlerkorrigierend ist:

Definition 6.13.14 *Sei $s \geq 2$, $n = 2^s - 1$ und $H \in K^{s\times n}$ die Matrix mit allen Vektoren $0 \neq v \in K^s$ in den Spalten. Der Code $\mathrm{Ker}(H)$ mit Kontrollmatrix H heißt* ***Hamming-Code*** *mit s Kontrollbits.*

Bestimmen wir eine Basis des Kerns von H und schreiben die Basisvektoren in die Spalten einer Matrix $G \in K^{n\times m}$, dann gilt

$$\mathrm{Ker}(H) = \mathrm{Bild}(G),$$

also ist G eine Generatormatrix für den Code. Mit der Dimensionsformel folgt $m = n - s$, d.h.

$$G \in K^{n\times(n-s)}.$$

Es werden also tatsächlich $n-s$ Bits zusammen mit s Kontrollbits in einen Block von n Bits codiert.

Beispiel 6.13.15 *Für $s = 3$ erhalten wir (bis auf Umsortieren der Spalten)*

$$H = \begin{pmatrix} \mathbf{1} & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & \mathbf{1} & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & \mathbf{1} & 0 & 1 & 1 & 1 \end{pmatrix}$$

Da H schon Zeilenstufenform hat, können wir sofort eine Basis des Kerns ablesen:

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

Insbesondere gilt für den Minimalabstand des Codes $U = \mathrm{Bild}(G) = \mathrm{Ker}(H)$

$$d_{min}(U) = 3$$

und somit ist der Code 2-fehlererkennend und 1-fehlerkorrigierend.

Zum Beispiel wird die Nachricht

$$v = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad \textit{in den Vektor} \quad c = G \cdot v = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

codiert. Stören wir c zu

$$c' = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad \textit{erhalten wir} \quad H \cdot c' = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \neq 0$$

und erkennen c' somit als fehlerbehaftet.

Zur Fehlerkorrektur suchen wir ein $e \in K^7$ mit

$$H \cdot e = H \cdot (c' - c) = H \cdot c'$$

und $d(e, 0)$ minimal. Es gilt

$$H \cdot \underbrace{\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}}_{e} = H \cdot c' = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$

und für den Einheitsvektor e ist klarerweise $d(e, 0) = 1$ minimal. Somit erhalten wir

$$c = c' - e = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} - \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

und daraus wiederum das korrekt dekodierte Urbild v mit $Av = c$.

Bemerkung 6.13.16 *Bei den Hammingcodes ist e leicht zu finden, denn jeder Vektor $0 \neq v \in K^s$ tritt als Spalte von H auf, d.h. für jedes c', das als fehlerhaft erkannt worden ist, d.h. mit $H \cdot c' \neq 0$, gibt es einen Einheitsvektor e_i mit*

$$H \cdot c' = H \cdot e_i.$$

Weiter ist für einen Einheitsvektor stets $d(e_i, 0) = 1$ minimal. Wir erhalten also sofort

$$c = c' - e_i.$$

Bemerkung 6.13.17 *Ist $0 \leq p \leq 1$ die Wahrscheinlichkeit, dass ein Bit korrekt übertragen wird, so ist die Wahrscheinlichkeit von maximal 1 Fehler in einem Block von n Bits gleich*

$$p^n + n \cdot p^{n-1} \cdot (1-p)$$

(Wahrscheinlichkeit für genau 0 Fehler plus Wahrscheinlichkeit für genau 1 Fehler). Übertragen wir N Datenbits so ist beim Hamming-Code aus Definition 6.13.14 die Wahrscheinlichkeit einer mit Fehlerkorrektur richtigen Übertragung gleich

$$\left(p^n + n \cdot p^{n-1} \cdot (1-p)\right)^{\frac{N}{n-s}},$$

denn in jedem Block von n Bits sind $n - s$ Datenbits codiert.

Beispiel 6.13.18 *Gigabit-Ethernet hat eine typische Raw-Data-Fehlerrate von 10^{-10}, also ist $p = 1 - 10^{-10}$. Innerhalb eines Jahres können wir*

$$N = 10^9 \cdot 3600 \cdot 24 \cdot 365 \approx 2^{54}$$

Bits übertragen (der Dateninhalt von etwa 840000 DVD). Für den $s = 3$ Hammnig-Code ist die Wahrscheinlichkeit einen Block von $n - s = 4$ Bits mit Fehlerkorrektur richtig zu übertragen

$$99.99999999999999979\ \%,$$

und somit für alle N Bits

$$99.83\ \%.$$

Ohne Fehlerkorrektur erreichen wir dieselbe Wahrscheinlichkeit schon nach

$$\frac{\ln(0.9983)}{\ln(p)} \approx 1.7 \cdot 10^7 \text{ Bits}$$

(diese Zahl B ist die Lösung von $p^B = 0.9983$), entsprechend einer Betriebszeit von 0.017 *Sekunden.*

6.14 Determinanten

Die Determinante ordnet einer quadratischen Matrix $A \in K^{n\times n}$ ein Körperelement $\det(A) \in K$ zu. Wir betrachten zunächst den Fall $A \in \mathbb{R}^{2\times 2}$. Für

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

ist die Determinante definiert als

$$\det(A) = a_{11}a_{22} - a_{12}a_{21}.$$

Geometrisch können wir $\det(A)$ (bis auf Vorzeichen) interpretieren als Fläche des **Parallelogramms** aufgespannt von den Zeilen von A (siehe Abbildung 6.8):

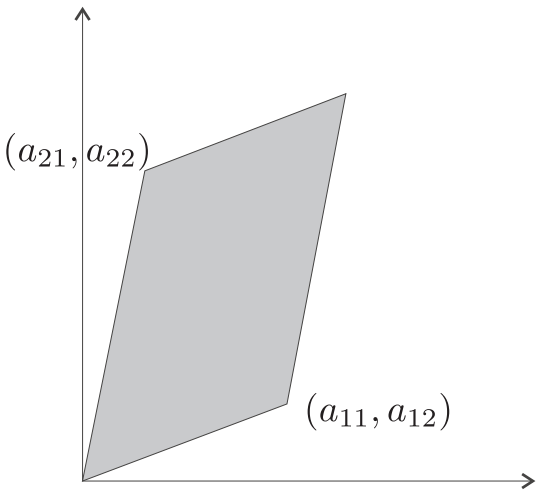


Abbildung 6.8: Parallelogramm

Zunächst bemerken wir, dass das Quadrat mit Seitenlänge 1 die Fläche

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

hat. Sei $a_{11} \neq 0$ (sonst analog). Subtraktion des $\frac{a_{21}}{a_{11}}$-fachen der ersten Zeile von der zweiten Zeile (d.h. **Scherung**) ändert die Fläche nicht, siehe Abbildung 6.9. Damit erhalten wir

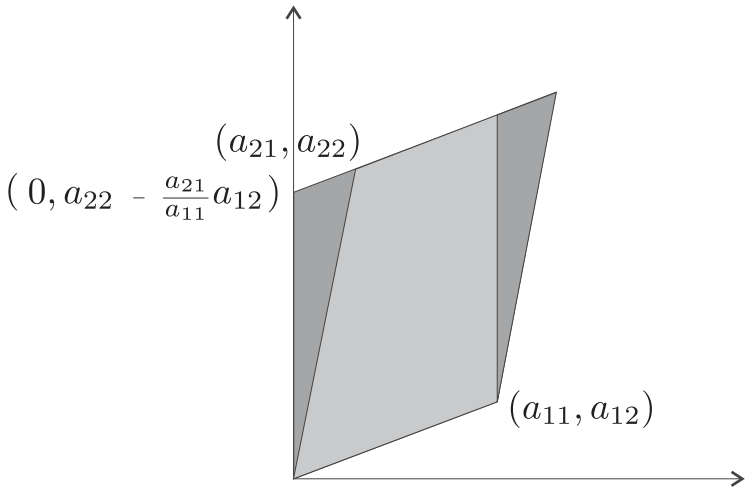


Abbildung 6.9: Subtraktion eines Vielfachen des ersten Erzeugers des Parallelogramms vom zweiten.

$$\begin{pmatrix} a_{11} & a_{12} \\ 0 & a_{22} - \frac{a_{21}}{a_{11}}a_{12} \end{pmatrix}$$

siehe Abbildung 6.10. Es ist $a_{22} - \frac{a_{21}}{a_{11}}a_{12} = 0$ genau dann, wenn die Zeilen von A linear abhängig waren. In diesem Fall ist die Fläche des Parallelogramms 0 und auch $\det(A) = 0$. Anderenfalls erhalten wir durch Subtraktion eines Vielfachen der zweiten von der ersten Zeile

$$\begin{pmatrix} a_{11} & 0 \\ 0 & a_{22} - \frac{a_{21}}{a_{11}}a_{12} \end{pmatrix}$$

siehe Abbildung 6.11. Die Zeilen dieser Matrix spannen ein Rechteck auf mit Fläche

$$a_{11} \cdot \left(a_{22} - \frac{a_{21}}{a_{11}}a_{12}\right) = \det(A)$$

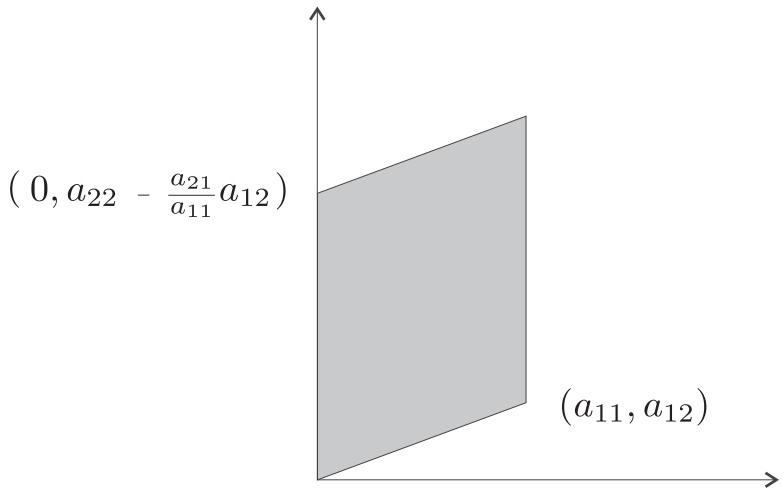


Abbildung 6.10: Parallelogramm nach Scherung

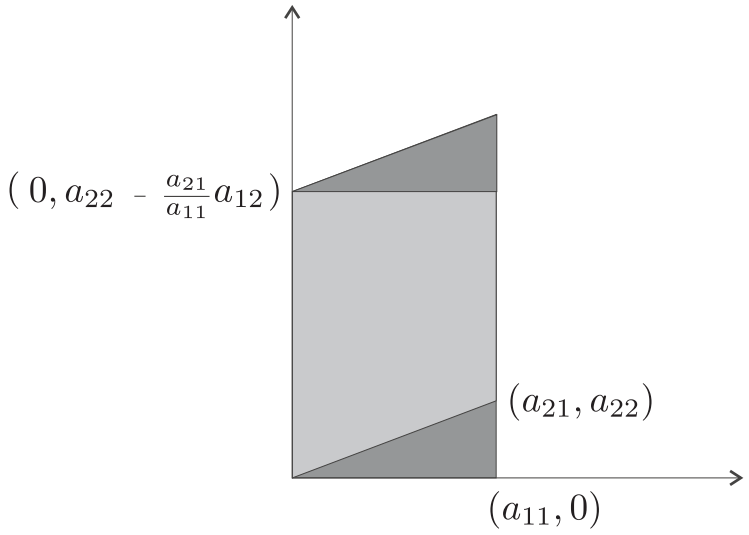


Abbildung 6.11: Scherung zum Rechteck

was die Behauptung zeigt, siehe Abbildung 6.12.

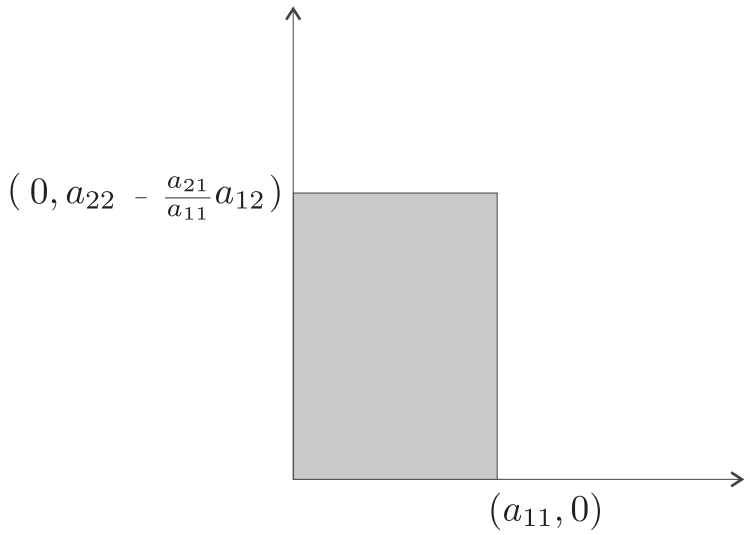


Abbildung 6.12: Zum Parallelogramm flächengleiches Rechteck

Weiter gilt

$$\text{Zeilen von } A \text{ sind linear abhängig } \Leftrightarrow \det(A) = 0$$

oder äquivalent

$$A \text{ invertierbar } \Leftrightarrow \det(A) \neq 0.$$

Wir wollen nun in analoger Weise für beliebiges n eine Volumenfunktion für das von den Zeilen von A aufgespannte **Parallelepiped** definieren:

Definition 6.14.1 *Sei K ein Körper. Die **Determinantenabbildung** ist definiert als*

$$\begin{aligned} \det &: K^{n\times n} \to K \\ \det(A) &= \sum_{\sigma\in S_n} \operatorname{sign}(\sigma) \cdot a_{1,\sigma(1)} \cdot \ldots \cdot a_{n,\sigma(n)} \end{aligned}$$

Lemma 6.14.2 *Wir bezeichnen mit $a_i, b_i \in K^n$ die Zeilen der jeweiligen Matrix und mit E die $n \times n$ Einheitsmatrix. Es gilt:*

(D1) det *ist* ***multilinear****, d.h. für jedes* $i = 1, ..., n$ *und jedes* $\lambda \in K$ *gilt*

$$\det\begin{pmatrix} a_1 \\ \vdots \\ a_{i-1} \\ \boldsymbol{a_i + b_i} \\ a_{i+1} \\ \vdots \\ a_n \end{pmatrix} = \det\begin{pmatrix} a_1 \\ \vdots \\ a_{i-1} \\ \boldsymbol{a_i} \\ a_{i+1} \\ \vdots \\ a_n \end{pmatrix} + \det\begin{pmatrix} a_1 \\ \vdots \\ a_{i-1} \\ \boldsymbol{b_i} \\ a_{i+1} \\ \vdots \\ a_n \end{pmatrix}$$

und

$$\det\begin{pmatrix} a_1 \\ \vdots \\ a_{i-1} \\ \boldsymbol{\lambda \cdot a_i} \\ a_{i+1} \\ \vdots \\ a_n \end{pmatrix} = \boldsymbol{\lambda} \cdot \det\begin{pmatrix} a_1 \\ \vdots \\ a_{i-1} \\ \boldsymbol{a_i} \\ a_{i+1} \\ \vdots \\ a_n \end{pmatrix}$$

(D2) det *ist alternierend, d.h. sind zwei Zeilen von* A *gleich, so gilt*

$$\det(A) = 0.$$

(D3) det *ist normiert, d.h.*

$$\det(E) = 1.$$

Beweis. Schreiben wir $a_i = (a_{i,j})$ und $b_i = (b_{i,j})$ dann gilt

$$\begin{aligned} &\sum_{\sigma \in S_n} \operatorname{sign}(\sigma) \cdot a_{1,\sigma(1)} \cdot \ldots \cdot \left(\mathbf{a}_{i,\sigma(i)} + \mathbf{b}_{i,\sigma(i)}\right) \cdot \ldots \cdot a_{n,\sigma(n)} \\ &= \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) \cdot a_{1,\sigma(1)} \cdot \ldots \cdot \mathbf{a}_{i,\sigma(i)} \cdot \ldots \cdot a_{n,\sigma(n)} \\ &+ \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) \cdot a_{1,\sigma(1)} \cdot \ldots \cdot \mathbf{b}_{i,\sigma(i)} \cdot \ldots \cdot a_{n,\sigma(n)} \end{aligned}$$

und

$$\begin{aligned} &\sum_{\sigma \in S_n} \operatorname{sign}(\sigma) \cdot a_{1,\sigma(1)} \cdot \ldots \cdot \left(\boldsymbol{\lambda} \cdot \mathbf{a}_{i,\sigma(i)}\right) \cdot \ldots \cdot a_{n,\sigma(n)} \\ &= \boldsymbol{\lambda} \cdot \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) \cdot a_{1,\sigma(1)} \cdot \ldots \cdot \mathbf{a}_{i,\sigma(i)} \cdot \ldots \cdot a_{n,\sigma(n)} \end{aligned}$$

und damit (D1).

Zu (D2): Sei $i \neq j$. Mit der Transposition $\tau = (i, j)$ gilt

$$S_n = A_n \dot{\cup} A_n \tau$$

(denn $S_n/A_n = \{\mathrm{id},\ A_n \cdot \tau\}$), also

$$\begin{aligned} \det(A) = &\sum_{\sigma \in A_n} a_{1,\sigma(1)} \cdot \ldots \cdot a_{n,\sigma(n)} \\ &- \sum_{\sigma \in A_n} a_{1,\sigma(\tau(1))} \cdot \ldots \cdot a_{n,\sigma(\tau(n))} \end{aligned}$$

wobei wir verwenden, dass sign ein Gruppenhomomorphismus ist, also

$$\mathrm{sign}(\sigma \circ \tau) = \mathrm{sign}(\sigma) \cdot \mathrm{sign}(\tau) = -\mathrm{sign}(\sigma).$$

Angenommen die i-te und j-te Zeile sind gleich, d.h. $a_i = a_j$. Dann ist

$$\begin{aligned} &a_{1,\sigma(\tau(1))} \cdot \ldots \cdot a_{i,\sigma(\tau(i))} \cdot \ldots \cdot a_{j,\sigma(\tau(j))} \cdot \ldots \cdot a_{n,\sigma(\tau(n))} \\ &= a_{1,\sigma(1)} \cdot \ldots \cdot a_{i,\sigma(j)} \cdot \ldots \cdot a_{j,\sigma(i)} \cdot \ldots \cdot a_{n,\sigma(n)} \\ &= a_{1,\sigma(1)} \cdot \ldots \cdot a_{i,\sigma(i)} \cdot \ldots \cdot a_{j,\sigma(j)} \cdot \ldots \cdot a_{n,\sigma(n)}. \end{aligned}$$

In der Formel für $\det(A)$ tritt also jeder Summand einmal mit positivem und einmal mit negativem Vorzeichen auf.

(D3) folgt sofort aus der Definition. ■

Man kann zeigen, dass det durch diese Eigenschaften schon eindeutig bestimmt ist (Übung).

Corollar 6.14.3 *Sei $A \in K^{n \times n}$.*

1) *Entsteht B aus A durch Vertauschen von zwei Zeilen, so gilt*
$$\det(A) = -\det(B)$$

2) *Addition eines Vielfachen einer Zeile zu einer anderen Zeile ändert den Wert der Determinante nicht.*

3) *Ist A eine obere Dreiecksmatrix*
$$A = \begin{pmatrix} \lambda_1 & & * \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$$

dann ist die Determinante das Produkt der Diagonalelemente:

$$\det(A) = \lambda_1 \cdot \ldots \cdot \lambda_n$$

4) Es gilt

$$A \text{ invertierbar} \Longleftrightarrow \det(A) \neq 0$$

Beweis.

1) Mit (D1) und (D2) gilt für $i \neq j$

$$\underbrace{\det\begin{pmatrix}\vdots\\ \boldsymbol{a_i}+\boldsymbol{a_j}\\ \vdots\\ \boldsymbol{a_i}+\boldsymbol{a_j}\\ \vdots\end{pmatrix}}_{0} = \underbrace{\det\begin{pmatrix}\vdots\\ \boldsymbol{a_i}\\ \vdots\\ \boldsymbol{a_i}\\ \vdots\end{pmatrix}}_{0} + \underbrace{\det\begin{pmatrix}\vdots\\ \boldsymbol{a_j}\\ \vdots\\ \boldsymbol{a_j}\\ \vdots\end{pmatrix}}_{0} + \det\begin{pmatrix}\vdots\\ \boldsymbol{a_i}\\ \vdots\\ \boldsymbol{a_j}\\ \vdots\end{pmatrix} + \det\begin{pmatrix}\vdots\\ \boldsymbol{a_j}\\ \vdots\\ \boldsymbol{a_i}\\ \vdots\end{pmatrix}$$

2) Mit (D1) und (D2) gilt für $i \neq j$

$$\det\begin{pmatrix}a_1\\ \vdots\\ a_{i-1}\\ \boldsymbol{a_i}+\boldsymbol{\lambda}\cdot\boldsymbol{a_j}\\ a_{i+1}\\ \vdots\\ a_n\end{pmatrix} = \det\begin{pmatrix}a_1\\ \vdots\\ a_{i-1}\\ \boldsymbol{a_i}\\ a_{i+1}\\ \vdots\\ a_n\end{pmatrix} + \boldsymbol{\lambda}\cdot \underbrace{\det\begin{pmatrix}a_1\\ \vdots\\ a_{i-1}\\ \boldsymbol{a_j}\\ a_{i+1}\\ \vdots\\ a_n\end{pmatrix}}_{0}$$

3) Angenommen alle $\lambda_i \neq 0$. Durch Addition von Vielfachen von Zeilen zu darüberliegenden Zeilen können wir A in die **Diagonalmatrix**

$$\begin{pmatrix}\lambda_1 & & 0\\ & \ddots & \\ 0 & & \lambda_n\end{pmatrix}$$

transformieren. Für diese erhalten wir in der Definition der Determinanten nur den Summanden $\lambda_1 \cdot \ldots \cdot \lambda_n$ entsprechend $\sigma = () \in S_n$.

Sei anderenfalls i maximal mit $\lambda_i = 0$. Durch Addition von Vielfachen der $(i+1)$-ten bis n-ten Zeile können wir die i-te Zeile komplett zu Null machen

$$\begin{pmatrix} \lambda_1 & & & & * \\ & \ddots & & & \\ & & \lambda_{i-1} & & \\ & & 0 & \cdots \cdots & 0 \\ & & & \lambda_{i+1} & * \\ & & & & \ddots \\ 0 & & & & \lambda_n \end{pmatrix}$$

Aus der Definition der Determinante folgt, dass $\det(A) = 0$, denn jeder Summand enthält einen Faktor aus der i-ten Zeile.

4) Mit Bemerkung 6.5.9 und Satz 6.8.4 gilt: A invertierbar $\Leftrightarrow$ $\operatorname{rk} A = \dim \operatorname{Bild} A = n \Leftrightarrow$ Zeilenstufenform von A ist

$$\begin{pmatrix} \lambda_1 & & * \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$$

mit $\lambda_1, \ldots, \lambda_n \neq 0$.

■

Das Corollar gibt uns Algorithmus 6.6 zur Bestimmung der Determinanten.

Man beachte, dass auch Diagonalelemente $\lambda_i = 0$ sein können, und zwar genau dann, wenn D weniger als n Stufen hat. In diesem Fall ist $\det(A) = 0$.

Beispiel 6.14.4 *Für die Determinante von*

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

Algorithmus 6.6 Determinante

Input: $A \in K^{n\times n}$

Output: $\det(A)$

1: Durch Addition von Vielfachen von Zeilen zu anderen Zeilen und Zeilenvertauschungen bringe A auf die Form einer oberen Dreiecksmatrix

$$D = \begin{pmatrix} \boxed{\lambda_1} & & * \\ & \ddots & \\ 0 & & \boxed{\lambda_n} \end{pmatrix}$$

2: $v :=$ Anzahl der Zeilenvertauschungen

3: **return** $\det(A) = (-1)^v \det(D) = (-1)^v \cdot \lambda_1 \cdot \ldots \cdot \lambda_n$.

erhalten wir als

$$\det(A) = \det\begin{pmatrix} 1 & -1 & -1 \\ 0 & 0 & 2 \\ 0 & 1 & 2 \end{pmatrix} = -\det\begin{pmatrix} 1 & -1 & -1 \\ 0 & 1 & 2 \\ 0 & 0 & 2 \end{pmatrix} = -2$$

Vorsicht: Nach (D1) ändert die Multiplikation einer Zeile mit einer Konstanten den Wert der Determinanten. Lassen wir auch diese Operation zu, so könnten wir fortfahren:

$$\det(A) = -\det\begin{pmatrix} 1 & -1 & -1 \\ 0 & 1 & 2 \\ 0 & 0 & 2 \end{pmatrix} = -2 \cdot \det\begin{pmatrix} 1 & -1 & -1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} = -2$$

In MAPLE *lässt sich die Determinante berechnen mit:*

```
with(LinearAlgebra):
A := <<1,1,2>|<-1,-1,-1>|<-1,1,0>>:
Determinant(A);
-2
```

Satz 6.14.5 *Sind $A, B \in K^{n\times n}$, so gilt*

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

Beweis. Da $\text{Bild}(A \cdot B) \subset \text{Bild}(A)$ gilt $\text{rk}(A \cdot B) \leq \text{rk}(A)$. Für $\det(A) = 0$ ist also auch $\det(A \cdot B) = 0$.

Sei nun $\det(A) \neq 0$. Nach Corollar 6.14.3 und (D1) gilt

$$\det(T \cdot B) = \det(T) \cdot \det(B)$$

falls $T \in \mathrm{GL}(n, K)$ eine elementare Zeilenoperation darstellt. Mit Algorithmus 6.5 ist $A = T_1 \cdot \ldots \cdot T_s$ das Produkt solcher Matrizen, also

$$\det(A \cdot B) = \det(T_1) \cdot \ldots \cdot \det(T_s) \cdot \det(B)$$

Insbesondere für $B = E$ folgt

$$\det(A) = \det(T_1) \cdot \ldots \cdot \det(T_s)$$

und damit die Behauptung. ■

Mit $\det(E) = 1$ erhalten wir:

Corollar 6.14.6 *Für $A \in \mathrm{GL}(n, K)$ ist*

$$\det(A^{-1}) = \frac{1}{\det(A)}.$$

Beispiel 6.14.7 *Als Illustration des Corollars bestimmen wir die Inverse für A aus Beispiel 6.14.4 und beobachten wie sich in jedem Schritt die Determinante ändert*

$$\begin{aligned}
\det(A) &= \det\begin{pmatrix} 1 & -1 & -1 \\ 1 & -1 & 1 \\ 2 & -1 & 0 \end{pmatrix} \\
&= \det\begin{pmatrix} 1 & -1 & -1 \\ 0 & 0 & 2 \\ 0 & 1 & 2 \end{pmatrix} \\
&= -\det\begin{pmatrix} 1 & -1 & -1 \\ 0 & 1 & 2 \\ 0 & 0 & 2 \end{pmatrix} \\
&= -2 \cdot \det\begin{pmatrix} 1 & -1 & -1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}
\end{aligned}
\qquad
\begin{aligned}
1 &= \det\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\
&= \det\begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ -2 & 0 & 1 \end{pmatrix} \\
&= -\det\begin{pmatrix} 1 & 0 & 0 \\ -2 & 0 & 1 \\ -1 & 1 & 0 \end{pmatrix} \\
&= -2 \cdot \det\begin{pmatrix} 1 & 0 & 0 \\ -2 & 0 & 1 \\ -\frac{1}{2} & \frac{1}{2} & 0 \end{pmatrix}
\end{aligned}$$

$$
\begin{array}{rl|rl}
= & -2 \cdot \det \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} & = & -2 \cdot \det \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 0 \\ -1 & -1 & 1 \\ -\frac{1}{2} & \frac{1}{2} & 0 \end{pmatrix} \\
= & -2 \cdot \det \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} & = & -2 \cdot \det \begin{pmatrix} -\frac{1}{2} & -\frac{1}{2} & 1 \\ -1 & -1 & 1 \\ -\frac{1}{2} & \frac{1}{2} & 0 \end{pmatrix} \\
= & -2 & = & -2 \cdot \det(A^{-1})
\end{array}
$$

6.15 Anwendung: Eigenvektoren und PageRank

6.15.1 Setup

Die Grundidee des Page-Rank-Algorithmus ist Internetseiten nach Wichtigkeit zu sortieren. Wir betrachten eine Seite als umso bedeutender je mehr Seiten sie verlinken. Dabei werden wiederum Links von bedeutenden Seiten stärker gewichtet. Das Internet können wir als gerichteten Graphen auffassen.

Beispiel 6.15.1 *Als Beispiel betrachten wir den Graphen in Abbildung 6.13.*

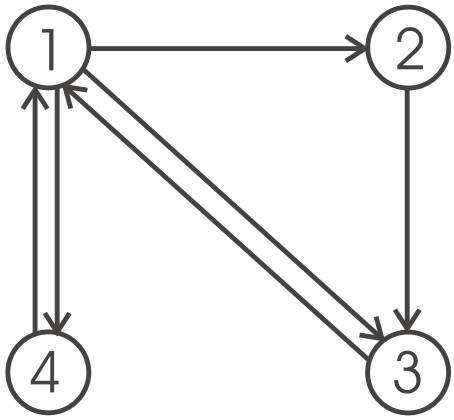


Abbildung 6.13: Gerichteter Graph von Links zwischen Internetseiten.

Sei n die Anzahl der Seiten. Dann codieren wir die Information des Graphen in einer Matrix $A = (a_{i,j}) \in \mathbb{R}^{n\times n}$ wobei

$$a_{i,j} = \begin{cases} \frac{1}{N_j} & \text{wenn Seite } j \text{ die Seite } i \text{ verlinkt} \\ 0 & \text{sonst} \end{cases}$$

und N_j die Anzahl der Links von j auf eine andere Seite ist. Wir können also $a_{i,j}$ interpretieren als die Wahrscheinlichkeit von Seite j auf Seite i zu gelangen, wenn wir einen zufälligen Link anklicken. Ein Problem haben wir bei der Definition, wenn $N_j = 0$, es also eine Seite ohne Links gibt. Deshalb ersetzt man in der Praxis A durch die gewichtete Summe $\alpha \cdot A + (1-\alpha) \cdot B$, wobei $0 < \alpha < 1$ und

$$B = \begin{pmatrix} \frac{1}{n} & \cdots & \frac{1}{n} \\ \vdots & \ddots & \vdots \\ \frac{1}{n} & \cdots & \frac{1}{n} \end{pmatrix}.$$

Dies modelliert, dass ein Surfer mit einer gewissen Wahrscheinlichkeit eine beliebige Seite im Internet direkt anspringt (deren Adresse ihm z.B. bekannt ist, weil er sie in seinen Bookmarks gespeichert hat). Die Konstante α wird empirisch durch Nutzerstudien bestimmt.

Die Matrix A ist gerade so konstruiert, dass alle Spaltensummen gleich 1 sind. Allgemein definiert man:

Definition 6.15.2 *Eine Matrix $A = (a_{i,j}) \in \mathbb{R}^{n\times n}$ heißt **Markovmatrix**, falls $a_{ij} \geq 0$ für alle i, j und*

$$\sum_{i=1}^{n} a_{i,j} = 1$$

für alle i.

Beispiel 6.15.3 *Für den obigen Graphen erhalten wir*

$$A = \begin{pmatrix} 0 & 0 & 1 & 1 \\ \frac{1}{3} & 0 & 0 & 0 \\ \frac{1}{3} & 1 & 0 & 0 \\ \frac{1}{3} & 0 & 0 & 0 \end{pmatrix}$$

Sei x_j die Wichtigkeit der Seite j, d.h. die Wahrscheinlichkeit, dass sich ein Zufallssurfer auf der Seite j aufhält. Dann berechnen wir die Wichtigkeit der Seite i als

$$x_i = \sum_{j=1}^{n} a_{i,j} x_j.$$

Um die Wichtigkeit aller Seiten zu bestimmen, muss man also schon die Wichtigkeit aller Seiten kennen. Dies ist ein sogenanntes Eigenwertproblem: Wir suchen einen Vektor $0 \neq x \in \mathbb{R}^n$ mit

$$A \cdot x = x,$$

äquivalent mit

$$(E - A) \cdot x = 0$$

Allgemein definiert man:

6.15.2 Eigenwerte und Eigenvektoren

Definition 6.15.4 *Sei K ein Körper. Ist $A \in K^{n\times n}$ eine quadratische Matrix, dann heißt $\lambda \in K$ **Eigenwert** von A, wenn es ein $0 \neq x \in K^n$ gibt mit*

$$Ax = \lambda x$$

*und x heißt **Eigenvektor** von A zum Eigenwert λ.*

Weiter heißt

$$\mathrm{Eig}(A, \lambda) = \mathrm{Ker}(\lambda E - A) \subset K^n$$

*der **Eigenraum** von A zum Eigenwert λ.*

Als Kern ist $\mathrm{Eig}(A, \lambda)$ ein Untervektorraum. Bis auf den 0-Vektor sind die Elemente von $\mathrm{Eig}(A, \lambda)$ genau die Eigenvektoren von A zum Eigenwert λ.

Satz 6.15.5 *Für $A \in K^{n\times n}$ gilt*

$$\mathrm{Eig}(A, \lambda) \neq \{0\} \iff \det(\lambda E - A) = 0$$

Beweis. Mit Satz 6.8.4 und Corollar 6.14.3.(4) gilt

$$\begin{aligned} \mathrm{Eig}(A,\lambda) \neq \{0\} &\iff \dim \mathrm{Ker}(\lambda E - A) > 0 \\ &\iff \lambda E - A \text{ ist nicht invertierbar} \\ &\iff \det(\lambda E - A) = 0 \end{aligned}$$

■

Eine quadratische Matrix $A \in K^{n\times n}$ können wir als **Endomorphismus** auffassen, d.h. als Homomorphismus mit Ziel gleich Quelle. Bei der Bestimmung einer Normalform D wollen wir also in Ziel und Quelle denselben Basiswechsel durchführen:

$$\begin{array}{ccc} K^n & \overset{A}{\to} & K^n \\ T\uparrow & & \uparrow T \\ K^n & \underset{D}{\to} & K^n \end{array}$$

das heißt

$$D = T^{-1} \cdot A \cdot T.$$

Ist es möglich T so zu wählen, dass D eine Diagonalmatrix ist

$$D = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$$

(das ist nicht klar, denn für die Normalform hatten wir ja verschiedene Basiswechsel in Ziel und Quelle zugelassen), dann können wir damit leicht Potenzen von A bestimmen: Es gilt

$$A^j = (T \cdot D \cdot T^{-1})^j = T \cdot D^j \cdot T^{-1}$$

und

$$D^j = \begin{pmatrix} \lambda_1^j & & 0 \\ & \ddots & \\ 0 & & \lambda_n^j \end{pmatrix}.$$

Siehe dazu auch Übungsaufgabe 6.36.

Definition und Satz 6.15.6 *Sei $A \in K^{n\times n}$. Dann gilt: K^n hat eine Basis aus Eigenvektoren von A, genau dann, wenn A* ***diagonalisierbar*** *ist, d.h. wenn es ein $T \in \mathrm{GL}(n,K)$ gibt mit*

$$T^{-1} \cdot A \cdot T = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} =: D$$

und die λ_i sind Eigenwerte von A.

Beweis. Zu $\Leftarrow$: In den Spalten von $T \in \mathrm{GL}(n, K)$ steht eine Basis. Ist t_i die i-te Spalte von T, dann gilt wegen $A \cdot T = T \cdot D$, dass

$$A \cdot t_i = t_i \cdot \lambda_i.$$

Zu $\Rightarrow$: Sei $t_1, ..., t_n$ die Basis aus Eigenvektoren und $T = (t_1 \mid ... \mid t_n)$. Dann gilt $A \cdot t_i = t_i \cdot \lambda_i$, also

$$A \cdot T = T \cdot D.$$

■

Definition und Satz 6.15.7 *Sei $A \in K^{n \times n}$. Die Nullstellen des* ***charakteristischen Polynoms***

$$\chi_A(t) = \det(t \cdot E - A) \in K[t]$$

in K sind genau die Eigenwerte von A.

Beweis. Mit Satz 5.7.6 (Einsetzen in Polynome ist ein Ringhomomorphismus) und Satz 6.15.5 gilt

$$\chi_A(\lambda) = 0 \Leftrightarrow \det(\lambda \cdot E - A) = 0 \Leftrightarrow \mathrm{Eig}(A, \lambda) \neq \{0\}$$

■

Bemerkung 6.15.8 *Ist A diagonalisierbar, dann gilt mit Satz 6.14.5 und Corollar 6.14.6, dass*

$$\begin{aligned} \chi_A(t) &= \det(t \cdot E - A) = \det(T \cdot (t \cdot E - D) \cdot T^{-1}) \\ &= \det(T) \cdot \det(t \cdot E - D) \cdot \det(T)^{-1} \\ &= \chi_D(t) = \textstyle\prod_{i=1}^{s} (t - \mu_i)^{n_i} \end{aligned}$$

mit den paarweise verschiedenen Eigenwerten $\mu_1, ..., \mu_s \in K$ von A und den ***algebraischen Vielfachheiten*** *$n_i > 0$ von μ_i. Das heißt:*

Vielfachheit der Nullstelle μ_i von $\chi_A(t)$	=	*Häufigkeit mit der μ_i auf der Diagonalen von D vorkommt*

Satz 6.15.9 *Eine Matrix $A \in K^{n\times n}$ ist diagonalisierbar genau dann, wenn $\chi_A(t) \in K[t]$ in Linearfaktoren zerfällt, d.h.*

$$\chi_A(t) = \prod_{i=1}^{s}(t-\mu_i)^{n_i} \text{ mit } \mu_i \in K$$

und die ***geometrischen Vielfachheiten*** $\dim \mathrm{Eig}(A,\mu_i)$ *mit den algebraischen Vielfachheiten n_i übereinstimmen, d.h.*

$$\dim \mathrm{Ker}(\mu_i E - A) = n_i \ \forall i = 1,...,s.$$

Beweis. Wir beweisen, dass Vektoren ungleich 0 aus verschiedenen Eigenräumen nicht linear abhängig sein können. Die Basen der Eigenräume fügen sich also zu einer Basis des K^n aus Eigenvektoren zusammen.

Zur linearen Unabhängigkeit: Für $v_i \in \mathrm{Eig}(A,\mu_i)$ zeigen wir mit Induktion nach s

$$v_1 + ... + v_s = 0 \implies v_1 = ... = v_s = 0.$$

Der Induktionsanfang $s = 1$ ist klar.
Induktionsschritt $s-1 \mapsto s$: Ist $\sum_{i=1}^{s} v_i = 0$, dann

$$0 = (\mu_s E - A)\left(\sum_{i=1}^{s} v_i\right) = \sum_{i=1}^{s-1}(\mu_s - \mu_i)v_i$$

Nach Induktionsvoraussetzung gilt $(\mu_s - \mu_i)v_i = 0$ und somit $v_i = 0$ $\forall i = 1,...,s-1$, also auch $v_s = 0$. ■

Man sagt dann auch: Die Summe der Eigenräume

$$\sum_{i=1}^{s} \mathrm{Eig}(A,\mu_i) = \left\{\sum_{i=1}^{s} v_i \mid v_i \in \mathrm{Eig}(A,\mu_i)\right\} = K^n$$

ist eine **direkte Summe** und schreibt $\bigoplus_{i=1}^{s} \mathrm{Eig}(A,\mu_i)$.

Bemerkung: Es gilt stets $\dim \mathrm{Eig}(A,\mu_i) \le n_i$ (Übung).

Beispiel 6.15.10 *Für*

$$A = \begin{pmatrix} 4 & 0 & 2 \\ -2 & 2 & -2 \\ -4 & 0 & -2 \end{pmatrix}$$

ist

$$\begin{aligned}\chi_A(t) = \det(tE - A) &= \det\begin{pmatrix} t-4 & 0 & -2 \\ 2 & t-2 & 2 \\ 4 & 0 & t+2 \end{pmatrix} \\ &= \det\begin{pmatrix} t-4 & 0 & -2 \\ 0 & t-2 & 2+\frac{2}{t-4}2 \\ 0 & 0 & t+2+\frac{4}{t-4}2 \end{pmatrix} \\ &= t^3 - 4t^2 + 4t \\ &= t(t-2)^2\end{aligned}$$

Man beachte, dass wir hier mit rationalen Funktionen in $\mathbb{Q}(t) = Q(\mathbb{Q}[t])$ *rechnen, das Ergebnis nach Definition der Determinanten aber in* $\mathbb{Q}[t]$ *sein muss.*
Somit hat A *die Eigenwerte* 0 *und* 2 *mit den Eigenräumen*

$$\mathrm{Eig}(A,0) = \mathrm{Ker}(A) = \left\langle \begin{pmatrix} -\frac{1}{2} \\ \frac{1}{2} \\ 1 \end{pmatrix} \right\rangle$$

$$\mathrm{Eig}(A,2) = \mathrm{Ker}(2E - A) = \left\langle \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix} \right\rangle$$

die wir mit dem Gaußalgorithmus bestimmen. Schreiben wir die Basen der Eigenräume in die Matrix T *(die Basiswahl in den einzelnen Eigenräumen spielt keine Rolle, die Reihenfolge der Spalten bestimmt die Reihenfolge der Diagonaleinträge von* D*), so erhalten wir*

$$T = \begin{pmatrix} 0 & -1 & -\frac{1}{2} \\ 1 & 0 & \frac{1}{2} \\ 0 & 1 & 1 \end{pmatrix} \quad \textit{und} \quad T^{-1} = \begin{pmatrix} -1 & 1 & -1 \\ -2 & 0 & -1 \\ 2 & 0 & 2 \end{pmatrix}$$

und es gilt

$$T^{-1} \cdot A \cdot T = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

In MAPLE *berechnet folgender Code die Eigenwerte und Eigenräume von* A*:*

```
with(LinearAlgebra):
A := <<4,-2,-4>|<0,2,0>|<2,-2,-2>>:
Eigenvectors(A);
```

$$\begin{bmatrix} 2 \\ 2 \\ 0 \end{bmatrix}, \begin{bmatrix} -1 & 0 & -\frac{1}{2} \\ 0 & 1 & \frac{1}{2} \\ 1 & 0 & 1 \end{bmatrix}$$

Direkt diagonalisieren können wir A mit:

```
T:=JordanForm(A, output='Q');
```

$$T := \begin{bmatrix} -1 & 1 & -1 \\ 1 & -1 & 0 \\ 2 & -1 & 1 \end{bmatrix}$$

```
T^(-1) . A . T;
```

$$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{bmatrix}$$

Man beachte, dass die Diagonalform eindeutig durch A festgelegt ist bis auf die Reihenfolge der Eigenwerte. Die Matrix T dagegen ist nicht eindeutig bestimmt, da die Eigenräume jeweils viele verschiedene Basen besitzen.

Siehe dazu auch Aufgabe 6.34.

Bemerkung 6.15.11 *Nicht jede quadratische Matrix ist diagonalisierbar, z.B.*

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in K^{2\times 2}$$

hat nur den Eigenwert 1 *und*

$$\mathrm{Eig}(A, 1) = \left\langle \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\rangle,$$

es gibt also keine Basis von K^2 *aus Eigenvektoren. In diesem Fall kann man die* ***Jordansche Normalform*** *berechnen, die für A gleich A wäre.*

Ein anders geartetes Problem zeigt folgendes Beispiel: Für

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in \mathbb{R}^{2\times 2}$$

gilt

$$\chi_A(t) = t^2 + 1$$

und somit hat A in $\mathbb{R}$ *keine Eigenwerte, ist also nicht diagonalisierbar. Aufgefasst als Matrix in* $\mathbb{C}^{2\times 2}$ *dagegen schon, denn über* $\mathbb{C}$ *hat A die Eigenwerte* $\pm i$.

Siehe dazu auch Aufgabe 6.35.

6.15.3 Markovmatrizen

Satz 6.15.12 *Jede Markovmatrix hat den Eigenwert* 1.

Beweis. Sei A eine Markovmatrix. Mit Übung 6.32 hat eine Matrix und ihre Transponierte dieselbe Determinante, also

$$\chi_A(t) = \det(t \cdot E - A) = \det((t \cdot E - A)^t) = \chi_{A^t}(t).$$

Weiter hat A^t den Eigenwert 1, denn

$$A^t \cdot \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$$

Die Behauptung folgt dann weil mit Satz 6.15.7 die Nullstellen des charakteristischen Polynoms gerade die Eigenwerte sind. ■

Man kann zeigen, dass es einen Eigenvektor zum Eigenwert 1 mit nicht-negativen Einträgen gibt. Klar ist, dass wir ihn auf Spaltensumme 1 normieren und somit die Einträge als Wahrscheinlichkeiten interpretieren können.

Beispiel 6.15.13 *Für die Matrix A in Beispiel 6.15.3 erhalten wir mit dem Gaußalgorithmus*

$$E - A = \begin{pmatrix} 1 & 0 & -1 & -1 \\ -\frac{1}{3} & 1 & 0 & 0 \\ -\frac{1}{3} & -1 & 1 & 0 \\ -\frac{1}{3} & 0 & 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & -1 & -1 \\ 0 & 1 & -\frac{1}{3} & -\frac{1}{3} \\ 0 & -1 & \frac{2}{3} & -\frac{1}{3} \\ 0 & 0 & -\frac{1}{3} & \frac{2}{3} \end{pmatrix}$$
$$\mapsto \begin{pmatrix} 1 & 0 & -1 & -1 \\ 0 & 1 & -\frac{1}{3} & -\frac{1}{3} \\ 0 & 0 & \frac{1}{3} & -\frac{2}{3} \\ 0 & 0 & -\frac{1}{3} & \frac{2}{3} \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & -1 & -1 \\ 0 & 1 & -\frac{1}{3} & -\frac{1}{3} \\ 0 & 0 & 1 & -2 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$
$$\mapsto \begin{pmatrix} 1 & 0 & -1 & -1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -2 \\ 0 & 0 & 0 & 0 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 & -3 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -2 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

also

$$\mathrm{Eig}(A, 1) = \mathrm{Ker}(E - A) = \left\langle \begin{pmatrix} 3 \\ 1 \\ 2 \\ 1 \end{pmatrix} \right\rangle$$

Das Ranking der Internetseiten mit dem Linkgraphen aus Abbildung 6.13 ist also gegeben durch die Aufenthaltswahrscheinlichkeiten

$$(x_1, x_2, x_3, x_4) = \left(\frac{3}{7}, \frac{1}{7}, \frac{2}{7}, \frac{1}{7}\right),$$

d.h. Seite 1 ist wichtiger als Seite 3, und diese ist wiederum wichtiger als die Seiten 2 und 4.

6.16 Übungsaufgaben

Übung 6.1 *Sei V ein K-Vektorraum und $U \subset V$ ein Untervektorraum. Zeigen Sie:*

1) *$(-1) \cdot v = -v$ für alle $v \in V$.*

2) *U ist mit der von V induzierten Addition und Skalarmultiplikation ein K-Vektorraum.*

Beispiel 6.16.1 *Bestimmen Sie jeweils die Lösungsmenge $V \subset \mathbb{Q}^5$ für folgende Gleichungssysteme und eine Basis von V:*

1)

$$\begin{array}{rcrcrcrcrcl} x_1 & + & 2x_2 & + & 2x_3 & - & 2x_4 & - & x_5 & = & 0 \\ -2x_1 & - & 3x_2 & - & x_3 & + & 8x_4 & + & x_5 & = & 0 \\ x_1 & + & 4x_2 & + & 8x_3 & + & 8x_4 & - & 4x_5 & = & 0 \\ 2x_1 & + & 5x_2 & + & 7x_3 & + & 2x_4 & - & 4x_5 & = & 0 \end{array}$$

2)

$$\begin{array}{rcrcrcrcrcl} x_1 & + & x_2 & + & x_3 & + & x_4 & - & x_5 & = & 0 \\ x_1 & + & 2x_2 & + & 3x_3 & + & 4x_4 & - & 5x_5 & = & 0 \\ x_1 & + & 4x_2 & + & 9x_3 & + & 16x_4 & - & 25x_5 & = & 0 \\ x_1 & + & 8x_2 & + & 27x_3 & + & 64x_4 & - & 125x_5 & = & 0 \end{array}$$

Beispiel 6.16.2 *Bestimmen Sie für jedes $t \in \mathbb{Q}$ eine Basis des Lösungsraums $V_t \subset \mathbb{Q}^3$ des homogenen linearen Gleichungssystems*

$$\begin{array}{rcrcrcl} -x_1 & + & x_2 & - & 2x_3 & = & 0 \\ x_1 & + & (t-1) \cdot x_2 & + & 2x_3 & = & 0 \\ 2x_1 & + & (t-2) \cdot x_2 & + & (t^2 - t + 4) \cdot x_3 & = & 0 \end{array}$$

Übung 6.2 *Sei*

$$\begin{aligned} l_1 &= a_{1,1}x_1 + \ldots + a_{1,n}x_n = 0 \\ &\vdots \\ l_r &= a_{r,1}x_1 + \ldots + a_{r,n}x_n = 0 \end{aligned}$$

mit $a_{i,j} \in \mathbb{Q}$ ein homogenes lineares Gleichungssystem. Schreiben Sie jeweils eine Funktion, die

1) *das System in Zeilenstufenform bringt.*
2) *das System in reduzierte Zeilenstufenform bringt.*
3) *eine Basis des Lösungsraums bestimmt.*

Übung 6.3 *Sei $d \geq 2$ und*

$$\mathbb{R}[x]_{\leq d} = \{f \in \mathbb{R}[x] \mid \deg f \leq d\}$$

der Vektorraum der Polynome vom Grad $\leq d$.

1) *Prüfen Sie, ob die folgenden Teilmengen Untervektorräume von $\mathbb{R}[x]_{\leq d}$ sind:*

$$\begin{aligned} U_1 &= \left\{f \in \mathbb{R}[x]_{\leq d} \mid f(0) = 0\right\} \\ U_2 &= \left\{f \in \mathbb{R}[x]_{\leq d} \mid f(0) = 1\right\} \\ U_3 &= \left\{f \in \mathbb{R}[x]_{\leq d} \mid f(1) = 0\right\} \\ U_4 &= \left\{f \in \mathbb{R}[x]_{\leq d} \mid \int_0^1 f(x)\,dx = 0\right\} \\ U_5 &= \left\{f \in \mathbb{R}[x]_{\leq d} \mid f'(0) + f''(0) = 0\right\} \\ U_6 &= \left\{f \in \mathbb{R}[x]_{\leq d} \mid f'(0) \cdot f''(0) = 0\right\} \end{aligned}$$

2) *Bestimmen Sie bei den Untervektorräumen U_i jeweils eine Basis.*

Übung 6.4 *Bilden die Vektoren*

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

eine Basis von $\mathbb{R}^4$? Beweisen Sie Ihre Behauptung.

Übung 6.5 *Zeigen Sie: Für jedes $b \in \mathbb{R}$ bilden die $d+1$ Polynome*

$$1, (x-b), (x-b)^2, ..., (x-b)^d \in \mathbb{R}[x]_{\leq d}$$

eine Basis von $\mathbb{R}[x]_{\leq d}$.

Übung 6.6 *Sei p eine Primzahl und $\mathbb{F}_p = \mathbb{Z}/p$ der endliche Körper mit p Elementen.*

1) *Zeigen Sie: Jeder d-dimensionale $\mathbb{F}_p$-Vektorraum V hat genau p^d Elemente.*

2) *Sei $V = (\mathbb{F}_2)^3$ und*

$$v_1 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \quad v_2 = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$$

   Bestimmen Sie alle Elemente des Untervektorraums $\langle v_1, v_2 \rangle \subset V$ und alle Vektoren $v_3 \in V$, sodass v_1, v_2, v_3 eine Basis von V bilden.

3) *Wieviele verschiedene Basen von $(\mathbb{F}_p)^d$ gibt es? Geben Sie eine Formel an.*

Übung 6.7 *Bestimmen Sie welche Teilmengen von*

$$\left\{x^3 + x,\ \ x^2,\ \ x^3,\ \ x^2 + 1,\ \ x,\ \ 1\right\}$$

Basen von $\mathbb{R}[x]_{\leq 3}$ bilden.

Übung 6.8 *Sei K ein Körper, und seien $U, V \subset K^n$ Untervektorräume gegeben durch Basen $u_1, ..., u_s$ von U und $v_1, ..., v_t$ von V.*

1) *Zeigen Sie, dass $U \cap V \subset K^n$ ein Untervektorraum ist.*

2) *Beschreiben Sie einen Algorithmus zur Bestimmung einer Basis von $U \cap V$.*

3) Wenden Sie Ihr Verfahren auf die Untervektorräume

$$U = \left\langle \begin{pmatrix} 4 \\ 0 \\ 2 \\ 4 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ 1 \\ 1 \end{pmatrix} \right\rangle \qquad V = \left\langle \begin{pmatrix} 2 \\ 0 \\ 3 \\ 1 \end{pmatrix}, \begin{pmatrix} 4 \\ 3 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 2 \\ 2 \\ 3 \\ 1 \end{pmatrix} \right\rangle$$

von $\mathbb{Q}^4$ an.

Übung 6.9 *Sei*

$$A = \begin{pmatrix} 1 & -2 & 3 & -4 \\ -3 & 2 & -1 & 0 \end{pmatrix} \quad \textit{und} \quad B = \begin{pmatrix} 0 & -2 \\ 1 & -1 \\ 2 & 0 \\ 3 & 1 \end{pmatrix}$$

Berechnen Sie AB und BA. Wie können Sie $AB \neq BA$ auch ohne Rechnung sofort sehen? Bestimmen Sie den Rang von BA.

Übung 6.10 *1) Berechnen Sie jeweils eine Basis des Kerns von*

$$A = \begin{pmatrix} 1 & 2 & 2 & -2 & -1 \\ -2 & -3 & -1 & 8 & 1 \\ 1 & 4 & 8 & 8 & -4 \end{pmatrix} \in \mathbb{Q}^{3\times 5} \quad B = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \\ 3 & 4 & 0 \end{pmatrix} \in (\mathbb{Z}/5)^{3\times 3}$$

2) Bestimmen Sie jeweils die Lösungsmenge für die linearen Gleichungssysteme

$$A \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_5 \end{pmatrix} = \begin{pmatrix} 2 \\ -7 \\ -7 \end{pmatrix} \qquad B \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$$

Übung 6.11 *Für welche $t \in \mathbb{R}$ ist das lineare Gleichungssystem*

$$\begin{pmatrix} 4 & 1 & 2 & 2 \\ 1 & 1 & 1 & 1 \\ 5 & -1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} t^2 + t \\ t \\ t \end{pmatrix}$$

lösbar? Bestimmen Sie für alle $t \in \mathbb{R}$ die Lösungsmenge.

Übung 6.12 *Sei*

$$\frac{d}{dx} : \mathbb{Q}[x]_{\leq 3} \longrightarrow \mathbb{Q}[x]_{\leq 2}$$

der durch die Ableitung gegebene $\mathbb{Q}$-Vektorraumhomomorphismus.

1) Bestimmen Sie bezüglich der Basen

$$\Omega = \left(1,\ x-1,\ (x-1)^2,\ (x-1)^3\right)$$

von $\mathbb{Q}[x]_{\leq 3}$ und

$$\Delta = (1, x, x^2)$$

von $\mathbb{Q}[x]_{\leq 2}$ die darstellende Matrix

$$A = M_{\Delta}^{\Omega}\left(\frac{d}{dx}\right) \in \mathbb{Q}^{3\times 4}$$

2) Berechnen Sie die Ableitung des Polynoms

$$p = 2(x-1)^3 + 3(x-1) + 7$$

direkt und mittels der Formel

$$\frac{d}{dx} = \mathrm{lc}_{\Delta} \circ A \circ \mathrm{co}_{\Omega}\,.$$

3) Berechnen Sie die Inverse von $T = (w_1 \mid w_2 \mid w_3) \in \mathbb{Q}^{3\times 3}$ für

$$w_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix},\ w_2 = \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix},\ w_3 = \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix}$$

4) Bestimmen Sie die darstellende Matrix

$$M_{\omega}^{\varepsilon}(A) \in \mathbb{Q}^{3\times 4}$$

bezüglich der Basis $\omega = (w_1, w_2, w_3)$ von $\mathbb{Q}^3$ und der Einheitsbasis $\varepsilon = (e_1, ..., e_4)$ von $\mathbb{Q}^4$. Können Sie die Matrix im Sinne von Ableitungen interpretieren?

Übung 6.13 *Sei $d \in \mathbb{N}$, $t_1, ..., t_{d+1} \in \mathbb{R}$ und*

$$\begin{array}{rccc} F: & \mathbb{R}[x]_{\leq d} & \to & \mathbb{R}^{d+1} \\ & p & \mapsto & \begin{pmatrix} p(t_1) \\ \vdots \\ p(t_{d+1}) \end{pmatrix} \end{array}$$

1) Zeigen Sie, dass F ein Homomorphismus von $\mathbb{R}$-Vektorräumen ist.

2) Bestimmen Sie die darstellende Matrix $M_\Delta^\Omega(F)$ von F bezüglich der Basis $\Omega = (1, x, ..., x^d)$ von $\mathbb{R}[x]_{\leq d}$ und der Standardbasis $\Delta = (e_1, ..., e_{d+1})$ von $\mathbb{R}^{d+1}$.

3) Sei $d = 3$ und $t_1 = -4$, $t_2 = 0$, $t_3 = 1$, $t_4 = 4$. Zeigen Sie, dass $M_\Delta^\Omega(F)$ ein Isomorphismus ist und bestimmen Sie das Urbild von

$$\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \in \mathbb{R}^4.$$

Vergleichen Sie mit Aufgabe 5.19.

Übung 6.14 *Seien V und W zwei K-Vektorräume mit Basen $\Omega = (v_1, ..., v_n)$ und $\Delta = (w_1, ..., w_m)$. Zeigen Sie: Die Menge $\mathrm{Hom}_K(V, W)$ der Homomorphismen $V \to W$ und die Menge $K^{n\times m}$ der $n \times m$-Matrizen sind K-Vektorräume und die Abbildung*

$$\begin{array}{rcl} \mathrm{Hom}_K(V, W) & \to & K^{n\times m} \\ F & \mapsto & M_\Delta^\Omega(F) \end{array}$$

ist ein Isomorphismus.

Übung 6.15 *Für Matrizen $A, B \in K^{n\times m}$ und $C \in K^{m\times r}$ gilt*

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

für $A \in K^{n\times m}$ und $B, C \in K^{m\times r}$

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

und für $A \in K^{n\times m}$, $B \in K^{m\times r}$, $C \in K^{r\times s}$, dass

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

Übung 6.16 *Bestimmen Sie jeweils eine Basis von* $\operatorname{Ker} A$ *und* $\operatorname{Bild} A$ *für folgende Matrizen:*

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \\ 3 & 4 & 5 \end{pmatrix} \in \mathbb{Q}^{3\times 3} \qquad A = \begin{pmatrix} 1 & 2 \\ 2 & 1 \\ 0 & 0 \\ 1 & 2 \end{pmatrix} \in (\mathbb{F}_3)^{4\times 2}$$

$$A = \begin{pmatrix} 1 & 2 & 2 & -2 & -1 \\ -2 & -3 & -1 & 8 & 1 \\ 1 & 4 & 8 & 8 & -4 \\ 2 & 5 & 7 & 2 & -4 \end{pmatrix} \in \mathbb{Q}^{4\times 5}$$

Dabei bezeichnet $\mathbb{F}_3 = \mathbb{Z}/3$ *den Körper mit* 3 *Elementen.*

Übung 6.17 *Bestimmen Sie die Lösungsmenge des folgenden linearen Gleichungssystems:*

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 \\ 1 & 4 & 9 & 16 \\ 1 & 8 & 27 & 64 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 1 \\ 5 \\ 25 \\ 125 \end{pmatrix}$$

Übung 6.18 *Sei*

$$A = \begin{pmatrix} 1 & 2 & 2 & -2 \\ -2 & -3 & -1 & 8 \\ 1 & 4 & 8 & 8 \\ 2 & 5 & 7 & 2 \end{pmatrix} \quad \textit{und} \quad b = \begin{pmatrix} 1 \\ -1 \\ 4 \\ 4 \end{pmatrix}$$

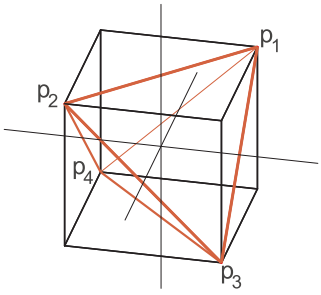
1) *Berechnen Sie eine Basis von Kern und Bild von* A.

2) *Berechnen Sie die Lösungsmenge* $L(A, b) \subset \mathbb{Q}^4$ *des inhomogenen linearen Gleichungssystems* $A \cdot x = b$ *für* $x \in \mathbb{Q}^4$.

3) *Bestimmen Sie das Urbild von* b *unter dem Isomorphismus*

$$\begin{aligned} \mathbb{Q}^4/\operatorname{Ker}(A) &\longrightarrow \operatorname{Bild}(A) \\ \overline{x} &\longmapsto A \cdot x. \end{aligned}$$

Übung 6.19 *Betrachten Sie den Tetraeder T*



mit den Ecken

$$p_2 = \begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix} \quad p_1 = \begin{pmatrix} -1 \\ 1 \\ 1 \end{pmatrix}$$
$$p_4 = \begin{pmatrix} -1 \\ -1 \\ -1 \end{pmatrix} \quad p_3 = \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix}$$

Jede Bewegung des $\mathbb{R}^3$, die 0 festhält, ist ein Homomorphismus $\mathbb{R}^3 \to \mathbb{R}^3$. Geben Sie für die Drehung mit Wirkung $(1,2,3) \in S_4$ auf den Ecken und für die Drehspiegelung $(1,2,3,4)$ jeweils die darstellende Matrix in $\mathbb{R}^{3\times 3}$ an.

Hinweis: Stellen Sie ein lineares Gleichungssystem zur Bestimmung der Einträge der Matrix auf.

Übung 6.20 *Für welche $t \in \mathbb{R}$ hat das lineare Gleichungssystem*

$$\underbrace{\begin{pmatrix} -1 & 1 & 1 \\ 2 & t & 1 \\ t+1 & 1 & -1 \end{pmatrix}}_{A_t} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}$$

eine Lösung, für welche t ist sie eindeutig bestimmt. Stellen Sie in diesem Fall die Lösung durch Funktionen $x_i = x_i(t)$ dar.

Übung 6.21 *Berechnen Sie jeweils die Inverse A^{-1} für folgende Matrizen:*

1)

$$A = \begin{pmatrix} 0 & 0 & 3 & -4 \\ 2 & 6 & 0 & 10 \\ 3 & 3 & 3 & 3 \\ 4 & -4 & 0 & 0 \end{pmatrix} \in \mathbb{Q}^{4\times 4}$$

2)

$$A = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 0 \\ 0 & 1 & 2 \end{pmatrix} \in (\mathbb{F}_3)^{3\times 3}$$

Übung 6.22 *Sei $K = \mathbb{Q}$. Schreiben Sie eine Funktion, die für eine Matrix $T \in K^{n\times n}$*

1) *prüft, ob $T \in \mathrm{GL}(n, K)$, und*

2) *in diesem Fall die Inverse T^{-1} berechnet.*

3) *Wenden Sie Ihre Funktion an auf die Matrix $T \in \mathbb{Q}^{3\times 3}$ aus Aufgabe 6.12, die Matrix $A \in \mathbb{Q}^{4\times 4}$ aus Aufgabe 6.21.(1) und*

$$T = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \\ 3 & 4 & 5 \end{pmatrix} \in \mathbb{Q}^{3\times 3}$$

an.

4) *Erweitern Sie Ihre Implementierung, sodass sie auch für $K = \mathbb{Z}/p$ mit p prim funktioniert. Erproben Sie Ihre Funktion an der Matrix A aus Aufgabe 6.21.(2).*

Übung 6.23 *Implementieren Sie für eine Matrix $A \in \mathbb{Q}^{n\times m}$ eine Funktion zur Bestimmung von $T \in \mathrm{GL}(n, \mathbb{Q})$, sodass $T \cdot A$ Zeilenstufenform hat. Schreiben Sie auch eine Funktion, die aus $T \cdot A$ eine Basis von $\operatorname{Ker} A$ berechnet.*

Hinweis: Verwenden Sie z.B. die Funktion `RowOperation` *der* MAPLE*-Bibliothek* `LinearAlgebra`*. Vergleichen Sie mit den Funktionen* `GaussianElimination` *und* `NullSpace`*.*

Übung 6.24 *Sei*

$$A = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & \frac{1}{2} & 0 \\ 0 & 0 & \frac{1}{3} \end{pmatrix} \in \mathbb{Q}^{4\times 3}$$

Bestimmen Sie die darstellende Matrix von $M_\Delta^\Omega(A)$ bezüglich der Basen

$$\Delta = \left(\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ -2 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 3 \\ -3 \\ 1 \end{pmatrix} \right) \quad \Omega = \left(\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix} \right)$$

Kennen Sie den Homomorphismus $L^{(1,x,x^2)}_{(1,x,x^2,x^3)}(A) : \mathbb{Q}[x]_{\leq 2} \to \mathbb{Q}[x]_{\leq 3}$*?*

Übung 6.25 *Bestimmen Sie für*

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

Matrizen $T \in \mathrm{GL}(4, \mathbb{Q})$ *und* $S \in \mathrm{GL}(5, \mathbb{Q})$*, sodass* $T \cdot A \cdot S$ *die Normalform*

$$T \cdot A \cdot S = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}$$

hat, wobei $r = \operatorname{rang} A$ *und* E_r *die* $r \times r$ *Einheitsmatrix ist.*

Übung 6.26 *Sei*

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

Bestimmen Sie $T \in \mathrm{GL}(3, \mathbb{Q})$ *und* $S \in \mathrm{GL}(4, \mathbb{Q})$ *sodass* $T \cdot A \cdot S$ *Normalform hat.*

Übung 6.27 *Berechnen Sie für die Matrizen in Aufgabe 6.17 jeweils die Determinante.*

Übung 6.28 *Seien* $a_1, \ldots, a_{d+1}$ *Elemente eines Körpers* K*. Die Matrix*

$$A = \begin{pmatrix} 1 & a_1 & a_1^2 & \cdots & a_1^d \\ 1 & a_2 & a_2^2 & \cdots & a_2^d \\ \vdots & & & & \vdots \\ 1 & a_{d+1} & a_{d+1}^2 & \cdots & a_{d+1}^d \end{pmatrix}$$

nennt man eine Vandermondsche Matrix. Zeigen Sie

$$\det A = \prod_{1 \leq i < j \leq d+1} (a_j - a_i)$$

Übung 6.29 *Schreiben Sie eine Funktion, die für* $A \in \mathbb{Q}^{n\times n}$ *die Determinante* $\det(A)$ *berechnet. Erproben Sie Ihre Funktion an der Vandermondschen Matrix für* $d = 4$ *und* $a_1 = -2$*,* $a_2 = -1$*,* $a_3 = 0$*,* $a_4 = 1$*,* $a_5 = 2$*.*

Übung 6.30 *Der ISBN-Code ist gegeben durch eine Identifikationsnummer aus* 9 *nichtnegativen ganzen Zahlen* $a_1, ..., a_9$ *und einer zehnten Zahl* $a_{10} \in \{1, ..., 9, X\}$*, wobei* X *für* 10 *steht, mit*

$$\sum_{j=1}^{10} j a_j \equiv 0 \bmod 11$$

Zeigen Sie:

1) *Sind* 9 *der* 10 *Ziffern einer ISBN-Nummer gegeben, dann kann man die fehlende Ziffer berechnen, wenn man weiß, an welcher Position* j *sie steht.*

2) *Werden in einer ISBN-Nummer zwei ungleiche Ziffern vertauscht, dann ist die Prüfsummenkongruenz nicht mehr erfüllt.*

3) *Es gibt Beispiele von zwei gültigen ISBN-Nummern, aus denen man durch Vertauschen von jeweils zwei Ziffern dieselbe ungültige ISBN-Nummer erhält. Insbesondere kann man zwar noch feststellen, dass die Nummer ungültig ist, jedoch nicht mehr die korrekte Nummer rekonstruieren.*

Übung 6.31 *Sei* $s \geq 2$*. Implementieren Sie Codierung, Fehlererkennung und Dekodierung für den Hamming-Code mit* s *Kontrollbits, z.B. in* MAPLE.

Übung 6.32 *Zeigen Sie:*

1) *Für* $A \in K^{n \times n}$ *gilt*

$$\det(A) = \det(A^t)$$

2) *Für* $A \in K^{n \times m}$ *und* $B \in K^{m \times r}$ *gilt*

$$(A \cdot B)^t = B^t \cdot A^t$$

3) *Für* $A \in \mathrm{GL}(n, K)$ *gilt*

$$(A^t)^{-1} = \left(A^{-1}\right)^t$$

4) Sei R ein kommutativer Ring. Überprüfen Sie, dass obige Aussagen auch für Matrizen mit Koeffizienten in R sinnvoll sind.

Übung 6.33 *Bestimmen Sie die Eigenwerte und Eigenräume von*

$$A = \begin{pmatrix} 2 & 6 & -8 \\ 1 & -2 & 1 \\ 1 & 0 & -1 \end{pmatrix} \in \mathbb{Q}^{3\times 3}$$

Übung 6.34 *Diagonalisieren Sie*

$$A = \begin{pmatrix} 5 & -5 & -5 \\ 1 & -1 & -1 \\ 3 & -3 & -3 \end{pmatrix} \in \mathbb{Q}^{3\times 3} \quad \textit{und} \quad B = \begin{pmatrix} 2 & 1 & 1 \\ 2 & 2 & 1 \\ -2 & 1 & 2 \end{pmatrix} \in \mathbb{Q}^{3\times 3}$$

Übung 6.35 *Welche der folgenden Matrizen ist über $\mathbb{R}$ diagonalisierbar, welche über $\mathbb{C}$, welche ist nicht diagonalisierbar?*

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

Übung 6.36 *Für $a_{d-1}, \ldots, a_0 \in \mathbb{R}$ sei V der Vektorraum der Folgen (b_n), die der linearen Rekursionsgleichung*

$$b_{n+d} = a_{d-1}b_{n+d-1} + \ldots + a_0 b_n \ \forall n \geq 0$$

genügen. Zeigen Sie:

1) V ist ein d-dimensionaler $\mathbb{R}$-Vektorraum.

2) Die Indexshift-Abbildung $T : V \to V$, $(b_0, b_1, \ldots) \mapsto (b_1, b_2, \ldots)$ ist ein Endomorphismus. Bestimmen Sie die Matrixdarstellung von T bezüglich einer geeigneten Basis von V.

3) Das charakteristische Polynom von T ist

$$\chi_T(t) = t^d - \left(a_{d-1}t^{d-1} + \ldots + a_1 t + a_0\right)$$

Sei nun

$$V = \{(b_n) \mid b_n \in \mathbb{R},\ b_{n+2} = b_{n+1} + b_n\ \forall n \geq 0\}$$

die Menge der Folgen vom Fibonacci-Typ.

4) *Bestimmen Sie die Eigenwerte und Eigenräume der Indexshift-Abbildung T.*

5) *Stellen Sie die Fibonacci-Folge $(f_n) \in V$, gegeben durch die Anfangswerte $f_0 = 0$, $f_1 = 1$, als Linearkombination der Eigenvektoren von T dar.*

6) *Leiten Sie damit eine geschlossene Formel für die Fibonaccizahlen her.*

7

Anhang: Computeralgebra

Für die Algebra, Zahlentheorie und elementares Programmieren ist ein Computeralgebrasystem mit allgemeiner Funktionalität am besten geeignet, da es alle drei Themengebiete gemeinsam abdeckt. Im kommerziellen Bereich sind MAPLE [21], und MATHEMATICA [23] verfügbar, ebenso die Open-Source-Systeme MAXIMA [22], REDUCE [25], und AXIOM [1], die allerdings einen deutlich kleineren Funktionsumfang besitzen.

Speziell für die Anwendung in der Algebra (exaktes Rechnen) gibt es deutlich leistungsfähigere Systeme, wie z.B. die Open-Source-Systeme SINGULAR [10], MACAULAY2 [14] (beide zum Rechnen mit Polynomen) und GAP [13] (zum Rechnen mit Permutationen), und das kommerzielle System MAGMA [20]. Dasselbe gilt für die Numerik (Rechnen mit floating point Zahlen), in der das kommerzielle System MATLAB [24] den Standard darstellt.

Im Folgenden wollen zunächst ausgehend von einfachen Fragestellungen einen kurzen Überblick über MAPLE geben, das sowohl in der Zahlentheorie, der Algebra, der Analysis, der Kombinatorik, der Stochastik und der Statistik eine umfangreiche Funktionalität bereitstellt.

7.1 Maple

MAPLE kann sowohl in der Kommandozeile als auch in einem graphischen Frontend verwendet werden. Die Ausgabe von Graphik ist natürlich nur in letzterem möglich, wobei die Komman-

dozeilenversion Graphiken in Dateien schreiben kann. In beiden Benutzeroberflächen folgt Output auf Input. Eine neue Zeile für mehrzeiligen Input erhält man durch `Shift-Return`, ein neues Eingabefeld durch `Strg-j`. Jeder Befehl wird mit einem Strichpunkt abgeschlossen und durch `Return` ausgewertet. Ersetzt man den Strichpunkt durch einen Doppelpunkt wird der Output unterdrückt. Durch `quit;` verlassen wir MAPLE.
Zuweisungen erfolgen mit:

```
i:=0;
0
```

Bedingte Anweisungen haben folgende Syntax:

```
if i=0 then print(null");fi;
null"
```

Mengen erzeugt man durch geschweifte Klammern:

```
M:={1,1,2,3,2};
M:={1,2,3}
```

und Listen durch eckige Klammern:

```
L:=[1,1,2,3,-1];
L:=[1,1,2,3,-1]
```

An eine Liste hängt man an durch

```
L:=[op(L),2];
L:=[1,1,2,3,-1,2]
```

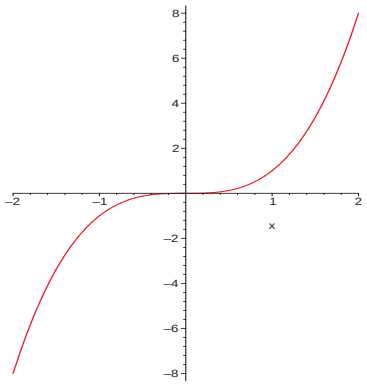
und genauso für Mengen.

Abbildungen (oder Prozeduren) werden auf die Elemente einer Menge oder die Einträge einer Liste angewendet durch:

```
map(x->x^2,L);
[1, 1, 4, 9, 1, 4]
```

Abbildungen $f : \mathbb{R} \to \mathbb{R}$ lassen sich plotten mit:

```
plot(x^3, x=-2..2);
```



Die Ausgabe wird nach dem Befehl

```
plotsetup(jpeg, plotoutput=‘plot.jpg‘, plotoptions
                          =‘portrait,noborder,color‘);
```

in eine Datei umgeleitet. Für eine Postscript-Ausgabe kann man jpeg durch ps ersetzen. Auf dem Bildschirm werden Plots wieder ausgegeben nach:

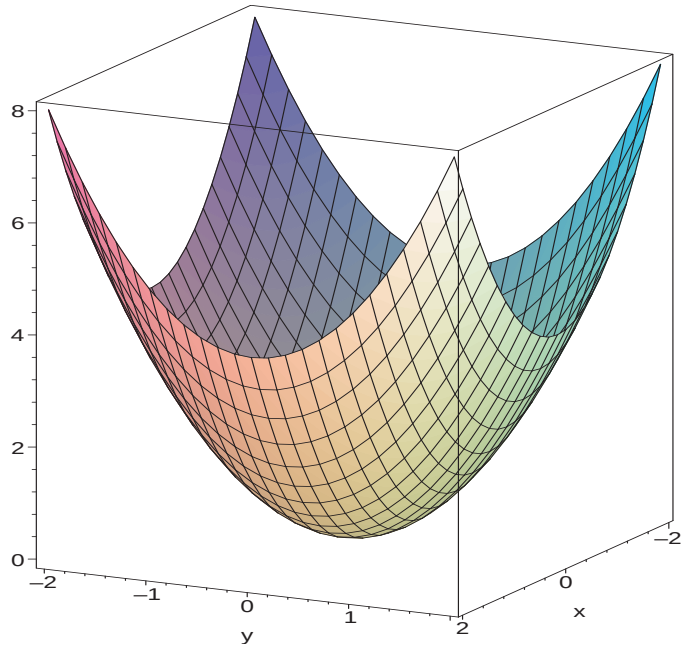
```
plotsetup(default);
```

Den Graphen der Abbildung

$$f : \mathbb{R}^2 \to \mathbb{R},\ (x, y) \mapsto x^2 + y^2$$

erhalten wir mit:

```
plot3d(x^2+y^2, x=-2..2,y=-2..2);
```



Bei der graphischen Ausgabe sind viele Optionen verfügbar, siehe dazu die Hilfe-Funktion unter `plot,options`.

Ein Beispiel für eine Prozedur, die

$$\sum_{k=1}^{n} k$$

berechnet ist (lokale Variablen werden mit `local` deklariert):

```
summe:=proc(n)
  local k,s;
  s:=0;
  for k from 1 to n do
      s:=s+k;
  od;
  return(s);
end proc:
```

Damit erhalten wir:

```
summe(5);
15
```

Tatsächlich gibt es eine Funktion die Summen und Produkte direkt auswertet:

```
sum(k,k=1..5);
```
15

gibt

$$\sum_{k=1}^{5} k = 1+2+3+4+5 = 15$$

und

```
product(k,k=1..5);
```
120

liefert

$$\prod_{k=1}^{5} k = 1\cdot 2\cdot 3\cdot 4\cdot 5 = 120$$

Dies funktioniert (in vielen Fällen) auch für unbestimmte Grenzen:

```
sum(k,k=1..n);
```
$\frac{(n+1)^2}{2} - \frac{n}{2} - \frac{1}{2}$

Durch Vereinfachen mit der sehr mächtigen Funktion `simplify` sieht man, dass die Formel mit der in Satz 1.3.4 bewiesenen übereinstimmt (wobei sich `%` auf die letzte Ausgabe bezieht):

```
simplify(%);
```
$\frac{1}{2}n^2 + \frac{1}{2}n$

Man kann auch Summenformeln eingeben, ohne sie auszuwerten

```
s:=Sum(k,k=1..n);
```
$s := \sum_{k=1}^{n} k$

damit weiterrechnen, z.B. n durch einen konkreten Wert ersetzen

```
s:=subs(n=5,s);
```
$s := \sum_{k=1}^{5} k$

und schließlich die Formel auswerten:

```
value(s);
```
15

In der Division mit Rest von a durch b mit Rest r

$$a = q\cdot b + r$$

erhalten wir q und r in MAPLE wie folgt, z.B. für $a = 36$ und $b = 15$:

```
iquo(36,15);
```
2
```
irem(36,15);
```
6

Diese Funktionen können Sie verwenden, um eine Prozedur zur Berechnung der Binärdarstellung zu schreiben. Vergleichen Sie auch mit der schon vorhandenen Funktion:

```
convert(23,binary);
10111
```

Weitere Anwendungsbeispiele werden wir jeweils in Zusammenhang mit den theoretischen Resultaten diskutieren.

7.2 Singular

Beispielhaft für spezialisierte Systeme in der Algebra stellen wir das Computeralgebrasystem SINGULAR [10] vor, das sich mit dem Rechnen mit polynomialen Gleichungssystemen befasst. Sie können Singular ohne Installation in dem Webinterface auf

http://www.singular.uni-kl.de

ausprobieren. Ein Beispiel für ein solches Gleichungssystem ist

$$\begin{aligned} 2x^2 - xy + 2y^2 - 2 &= 0 \\ 2x^2 - 3xy + 3y^2 - 2 &= 0 \end{aligned}$$

das den Durchschnitt von zwei Ellipsen beschreibt. Mathematisch wird ein polynomiales Gleichungssystem durch ein Ideal in einem Polynomring dargestellt, hier etwa das Ideal

$$I = \left\langle 2x^2 - xy + 2y^2 - 2,\ 2x^2 - 3xy + 3y^2 - 2 \right\rangle \subset \mathbb{Q}[x, y].$$

Der Grund hierfür ist der folgende: Wenn (x, y) eine Nullstelle von $f(x, y)$ und $g(x, y)$ ist, dann auch von

$$a(x, y) \cdot f(x, y) + b(x, y) \cdot g(x, y)$$

für alle $a, b \in \mathbb{Q}[x, y]$. Ein solches Ideal hat viele verschiedene Erzeugendensysteme. Der in SINGULAR implementierte Gröbnerbasen-Algorithmus findet ein äquivalentes leichter lösbares System (eine sogenannte Gröbnerbasis von I). Dabei geht er analog zum Gauß-Algorithmus für lineare Gleichungssysteme vor, indem er Variablen eliminiert:

```
ring R=0,(y,x),lp;
```

```
ideal I = 2x2-xy+2y2-2, 2x2-3xy+3y2-2;
std(I);
_[1]=4x4-5x2+1
_[2]=3y+8x3-8x
```

Dies zeigt, dass

$$\begin{array}{r} 2x^2 - xy + 2y^2 - 2 = 0 \\ 2x^2 - 3xy + 3y^2 - 2 = 0 \end{array} \quad \Longleftrightarrow \quad \begin{array}{r} 3y + 8x^3 - 8x = 0 \\ 4x^4 - 5x^2 + 1 = 0 \end{array}$$

In dem äquivalenten System können wir die zweite Gleichung nach x lösen und dann in die erste Gleichung einsetzen und erhalten die Lösungsmenge

$$V(I) = \{(1,0), (-1,0), (\frac{1}{2}, 1), (-\frac{1}{2}, -1)\}.$$

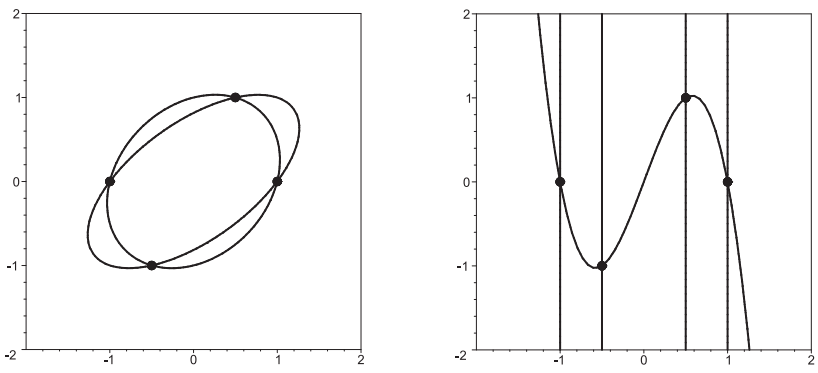


Abbildung 7.1: Gröbnerbasen-Algorithmus für den Schnitt von zwei Ellipsen

Neben dem Buchberger-Algorithmus sind in SINGULAR noch viele weitere Algorithmen zum Lösen und Analysieren von polynomialen Gleichungssystemen implementiert. Insgesamt umfasst das System über 150 spezialisierte Bibliotheken.

Index

Literaturverzeichnis

[1] The Axiom Group: *Axiom*, http://www.axiom-developer.org/ (2012).

[2] M. Artin: Algebra, Birkhäuser (2003).

[3] J. Böhm: Grundlagen der Algebra und Zahlentheorie, Springer (2016).

[4] J. Böhm, M. Marais: Introduction to algebraic structures, Lecture Notes (2019).

[5] J. Böhm: Mathematik für Informatiker: Kombinatorik und Analysis, Lecture Notes (2018).

[6] J. Böhm: Mathematik für Informatiker: Analysis, Lecture Notes (2019).

[7] J. Böhm: Mathematik für Informatiker: Kombinatorik, Stochastik und Statistik, Lecture Notes (2019).

[8] S. Bosch: Algebra, Springer (1993).

[9] P. Bundschuh: Einführung in die Zahlentheorie, Springer (1998).

[10] Decker, W.; Greuel, G.-M.; Pfister, G.; Schönemann, H.: SINGULAR *4-1-1 — A computer algebra system for polynomial computations*. http://www.singular.uni-kl.de (2018).

[11] G. Fischer: Lineare Algebra, Vieweg (2010).

[12] G. Fischer, R. Sacher: Einführung in die Algebra, Teubner (1983).

[13] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.8.10*; http://www.gap-system.org, (2018).

[14] Grayson, D. R.; Stillman, M. E.: *Macaulay2, a software system for research in algebraic geometry*, available at http://www.math.uiuc.edu/Macaulay2/ (2019).

[15] G.H. Hardy, E.M. Wright: An introduction to the theory of numbers, Oxford (1956).

[16] J. C. Jantzen, J. Schwermer: Algebra, Springer (2006).

[17] C. Karpfinger, K. Meyberg: Algebra, Spektrum Akademischer Verlag (2008).

[18] E. Kunz: Algebra, Vieweg (1994).

[19] B. Kreußler, G. Pfister: Mathematik für Informatiker: Algebra, Analysis, Diskrete Strukturen, Springer (2009).

[20] Bosma, W.; Cannon J.; Playoust C.: *The Magma algebra system. I. The user language*, J. Symbolic Comput., 24 (1997), 235–265.

[21] Maple (Waterloo Maple Inc.): Maple 2018, http://www.maplesoft.com/ (2018).

[22] Maxima: *Maxima, a Computer Algebra System.* Version 5.25.1, available at http://maxima.sourceforge.net/ (2011).

[23] Wolfram Research, Inc.: *Mathematica Edition: Version 11* (2018).

[24] MATLAB. Natick, Massachusetts: The MathWorks Inc., http://www.mathworks.de/products/matlab/ (2018).

[25] Hearn, A. C.: *REDUCE 3.8*, available at http://reduce-algebra.com/ (2009).

[26] R. Remmert, P. Ullrich: Elementare Zahlentheorie, Birkhäuser (1987).

[27] P. Ribenboim: Die Welt der Primzahlen, Springer (2006).

[28] R. Schulze-Pillot: Einführung in die Algebra und Zahlentheorie, Springer (2008).

[29] V. Shoup: A Computational Introduction to Number Theory and Algebra, Cambridge University Press (2005).

[30] W. Willems: Codierungstheorie und Kryptographie, Birkhäuser (2008).

[31] J. Wolfart: Einführung in die Algebra und Zahlentheorie, Vieweg (1996).

[32] G. Wüstholz: Algebra, Vieweg (2004).