

Mathematik für Informatiker

Algebraische Strukturen

Vorlesungsmanuskript Sommersemester 2017

Janko Böhm

6. Januar 2020

Inhaltsverzeichnis

0	Einleitung	1
1	Grundkonstruktionen	4
1.1	Mengen	4
1.2	Vollständige Induktion	8
1.3	Relationen	11
1.4	Abbildungen	12
1.5	Halbordnungen und Äquivalenzrelationen	18
1.6	Übungsaufgaben	21
2	Zahlen	27
2.1	Die ganzen Zahlen und Division mit Rest	27
2.2	Fundamentalsatz der Arithmetik	32
2.3	Größter gemeinsamer Teiler und Euklidischer Algorithmus	35
2.4	Primfaktorisation	37
2.5	Der chinesische Restsatz	40
2.6	Übungsaufgaben	43
3	Gruppen	47
3.1	Übersicht	47
3.2	Gruppen und Operationen	49
3.2.1	Grundbegriffe	49
3.2.2	Gruppenoperationen	62
3.2.3	Operation durch Translation	72
3.2.4	Bahnengleichung	77
3.2.5	Anwendung: Aufzählen von Graphen	82
3.3	Normalteiler	84
3.3.1	Normalteiler und Quotientengruppe	84

3.3.2	Homomorphiesatz	89
3.4	Übungsaufgaben	91
4	Ringe	99
4.1	Übersicht	99
4.2	Grundbegriffe	102
4.3	Ringerweiterungen	108
4.4	Die Einheitengruppe von \mathbb{Z}/n	110
4.5	Anwendung: RSA Kryptosystem	114
4.5.1	Übersicht	114
4.5.2	Setup	115
4.5.3	Nachrichtenübertragung	115
4.6	Anwendung: Primfaktorisierung mit dem Verfahren von Pollard	117
4.7	Anwendung: Diffie-Hellman Schlüsselaustausch	119
4.8	Ideale und Quotientenringe	120
4.9	Integritätsringe und Körper	123
4.10	Euklidische Ringe	126
4.11	Chinesischer Restsatz	130
4.12	Anwendung: Modulares Rechnen	133
4.13	Anwendung: Interpolation	134
4.14	Übungsaufgaben	138
5	Vektorräume	145
5.1	Übersicht	145
5.2	Gaußalgorithmus	146
5.3	Vektorräume und Basen	153
5.4	Dimension	165
5.5	Vektorraumhomomorphismen	172
5.6	Inhomogene lineare Gleichungssysteme	177
5.7	Darstellende Matrix eines Homomorphismus	184
5.8	Gauß mit Zeilen- und Spaltentransformationen	189
5.9	Isomorphismen	197
5.10	Basiswechsel	201
5.11	Klassifikation von Homomorphismen	203
5.12	Homomorphiesatz	205
5.13	Anwendung: Lineare Codes	207
5.13.1	Setup	207
5.13.2	Fehlererkennung	208

5.13.3 Fehlerkorrektur	213
5.14 Determinanten	217
5.15 Anwendung: Eigenvektoren und Page-Rank	227
5.15.1 Setup	227
5.15.2 Eigenwerte und Eigenvektoren	229
5.15.3 Markovmatrizen	235
5.16 Übungsaufgaben	236

Abbildungsverzeichnis

1	Knoten	1
2	Vier Punkte	2
1.1	Komplement	6
1.2	Vereinigung	6
1.3	Durchschnitt	6
1.4	Graph der Parabel	13
1.5	Hyperbel	14
1.6	Eine nicht-injektive Abbildung	14
1.7	Eine bijektive Abbildung und ihre Umkehrabbildung	16
1.8	Wurzel	16
1.9	Identische Abbildung $\mathbb{R} \rightarrow \mathbb{R}$	18
1.10	Äquivalenzklassen	21
1.11	Die Türme von Hanoi	24
1.12	Wieviele kürzeste Wege gibt es von A nach B	24
2.1	Zwei Konfigurationen von drei Zahnrädern	46
3.1	Die Platonischen Körper	48
3.2	Komposition von zwei Symmetrien des Tetraeders	48
3.3	Eine Drehsymmetrie des Tetraeders	52
3.4	Eine Spiegelsymmetrie des Tetraeders	53
3.5	Restklassen modulo 3	55
3.6	Exponentialfunktion	58
3.7	Beispiel einer Bewegung des \mathbb{R}^2	64
3.8	Tetraeder	79
3.9	Spiegelsymmetrie $(2, 3)$ des Tetraeders	80
3.10	Bahnen von Punkten des Tetraeders	81
3.11	Graph	82

3.12 Nachbarschaftsverhältnisse	83
3.13 Isomorphe Graphen	83
3.14 Tetraeder	94
3.15 Regelmäßiges 5-Eck	95
3.16 Tetraeder mit Kantenmittendiagonalen	97
3.17 Ikosaeder mit Nummerierung der Ecken	98
4.1 Polynomfunktion	108
4.2 Interpolation	137
4.3 Interpolation	138
4.4 Polynom mit vorgegebenen Funktionswerten und Ableitungen	142
5.1 Kubische Polynome mit Nullstellen bei -1 und 2 und Wendepunkt bei 0	151
5.2 Geraden im \mathbb{R}^2 , die Untervektorräume sind	157
5.3 Halbebene	158
5.4 Parabel	159
5.5 Zwei Erzeugendensysteme der Ebene $\{z = 0\} \subset \mathbb{R}^3$	161
5.6 Affine Gerade	179
5.7 Dreiecksungleichung	214
5.8 Parallelogramm	218
5.9 Subtraktion eines Vielfachen des ersten Erzeugers des Parallelogramms vom zweiten.	219
5.10 Parallelogramm nach Scherung	219
5.11 Scherung zum Rechteck	220
5.12 Zum Parallelogramm flächengleiches Rechteck	221
5.13 Gerichteter Graph von Links zwischen Internetsei- ten.	228

Symbolverzeichnis

$m \in M$	m ist Element von M	4
\mathbb{N}	Die natürlichen Zahlen	5
\mathbb{N}_0	Die natürlichen Zahlen mit 0	5
\mathbb{Z}	Die ganzen Zahlen	5
\mathbb{Q}	Die rationalen Zahlen	5
	mit	5
\Rightarrow	daraus folgt	5
\Leftrightarrow	genau dann wenn	5
$M \setminus N$	Komplement von N in M	5
$M \cup N$	Vereinigung von N und M	5
$M \cap N$	Durchschnitt von N und M	5
\forall	für alle	7
\exists	es existiert	7
$ M $	Anzahl der Elemente von M	7
$M \times N$	Kartesisches Produkt von M und N	7
2^M	Potenzmenge von M	8
$\sum_{k=1}^n a_k$	Summe	9
$\prod_{k=1}^n a_k$	Produkt	9
$f(A)$	Bild von A unter der Abbildung f	12
$\text{Bild}(f)$	Bild der Abbildung f	12
$f^{-1}(B)$	Urbild von B unter der Abbildung f	12
$\text{Graph}(f)$	Graph von f	12
f^{-1}	Umkehrabbildung der bijektiven Abb. f	15
\exists_1	es existiert genau ein	15
$\binom{n}{k}$	Binomialkoeffizient	23
$b \mid a$	b teilt a	31
$a \equiv b \pmod{m}$	a kongruent zu b modulo m	32
$\pi(x)$	Anzahl der Primzahlen kleiner gleich x	34
ggT	Größter gemeinsamer Teiler	35

kgV	Kleinstes gemeinsames Vielfaches	35
$S(X)$	Gruppe der Selbstabbildungen von X .	51
S_n	Symmetrische Gruppe	51
$G_1 \times G_2$	Kartesisches Produkt von G_1 und G_2 .	53
\mathbb{Z}/n	Restklassengruppe	54
\mathbb{Z}_n	Restklassengruppe	54
$\ker \varphi$	Kern von φ	56
Bild φ	Bild von φ	56
$\langle E \rangle$	Untergruppe erzeugt von E	60
$\text{ord}(g)$	Ordnung von g	61
$E(n)$	Gruppe der Euklidischen Bewegungen .	63
$\text{Sym}(M)$	Symmetriegruppe	63
Gm	Bahn von m unter der Operation von G	66
$\text{Stab}(N)$	Stabilisator der Menge N unter der Operation von G	66
$\text{Stab}(m)$	Stabilisator von m unter der Operation von G	67
$[G : H]$	Index der Untergruppe $H \subset G$	76
R^\times	Einheitengruppe von R	101
$R[x]$	Polynomring in x über R	105
$\deg(f)$	Grad des Polynoms f	105
$\varphi(n)$	Eulersche Phi-Funktion, $n \in \mathbb{N}$	111
$\text{char}(K)$	Charakteristik von K	125
$\dim V$	Dimension von V	168
φ_Ω	Koordinatenabbildung bezüglich Ω . . .	172
$L(A, b)$	Lösungsmenge von $A \cdot x = b$	178
$M_\Delta^\Omega(F)$	Darstellende Matrix von F bezüglich der Basen Ω und Δ	186
$K^{n \times m}$	Vektorraum der $n \times m$ -Matrizen	188
$\text{Hom}_K(V, W)$	Vektorraum der Homom. $V \rightarrow W$	188
$L_\Delta^\Omega(A)$	Zur Matrix A bezüglich der Basen Ω und Δ zugeordneter Homomorphismus	189
A^t	Transponierte von A	209
$d(a, b)$	Hammingabstand von a und b	212
$d_{\min}(U)$	Minimalabstand des Codes U	212
$\det(A)$	Determinante von A	220
$\text{Eig}(A, \lambda)$	Eigenraum von A zum Eigenwert λ . . .	229
\oplus	Direkte Summe	232

0

Einleitung

Wir wollen uns mit den Grundlagen der Zahlentheorie, Algebra und insbesondere der linearen Algebra beschäftigen. Dies sind eng verknüpfte Teilgebiete der reinen Mathematik, neben Analysis, Kombinatorik¹, Geometrie und Topologie².

Was ist Zahlentheorie? Wie der Name schon verrät befassen sich die Zahlentheoretiker mit den Eigenschaften von Zahlen $(\dots, -1, 0, 1, 2, 3, \dots)$, 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

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

¹Mit Hilfe der Kombinatorik kann man zum Beispiel berechnen, dass es beim Ziehen der Lottozahlen $\binom{49}{6} \approx 14\,000\,000$ mögliche Ergebnisse gibt.

²In der Topologie sieht man zum Beispiel, dass sich der Knoten in Abbildung 1 nicht ohne Aufschnneiden entwirren läßt.

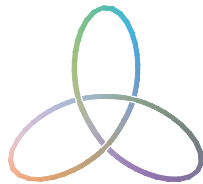


Abbildung 1: Knoten

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 weites 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. Durch Kombination der Grundlagen der Zahlentheorie und Algebra werden wir als zentrale Anwendung die Public-Key Kryptographie diskutieren. 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 Variablen³.

Der einfachste (aber in der Praxis sehr wichtige) Spezialfall sind lineare Gleichungssysteme über einem Körper K (zum Beispiel $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ der Körper der rationalen, reellen oder komplexen Zahlen), das Kernthema der linearen Algebra. Hier lösen

³Zum Beispiel besteht die gemeinsame Lösungsmenge von $x^2 + 2y^2 = 3$ und $2x^2 + y^2 = 3$, das heißt der Durchschnitt von zwei Ellipsen, aus 4 Punkten $(1, 1), (-1, 1), (1, -1), (-1, -1)$, siehe Abbildung 2.

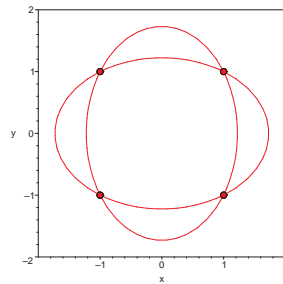


Abbildung 2: Vier Punkte

wir

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

mit $a_{ij} \in K$, $b_i \in K$ nach $x_j \in K$ (mit $i = 1, \dots, n$ und $j = 1, \dots, m$). 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.

1

Grundkonstruktionen

In diesem Abschnitt behandeln wir Grundkonstruktionen mit denen wir aus gegebenen mathematischen Objekten neue konstruieren können. Ausgehend vom Mengenbegriff beschäftigen wir uns mit der Frage, wie man zwei gegebene Mengen in Beziehung setzen kann, insbesondere mit Abbildungen zwischen Mengen und Äquivalenzrelationen auf Mengen.

1.1 Mengen

Definition 1.1.1 (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, \dots als

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

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

Bemerkung 1.1.2 *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 Elemente gleich oder verschieden sind.*

Beispiel 1.1.3 Mengen sind beispielsweise die Menge der Ziffern

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

die natürlichen Zahlen

$$\begin{aligned}\mathbb{N} &= \{1, 2, 3, \dots\} \\ \mathbb{N}_0 &= \{0, 1, 2, 3, \dots\},\end{aligned}$$

die ganzen Zahlen

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

die rationalen Zahlen

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

Dabei steht das Symbol \mid für **mit**.

Definition 1.1.4 Ist jedes Element der Menge N auch Element der Menge M (also $m \in N \Rightarrow m \in M$), dann heißt N **Teilmenge** von M (geschrieben $N \subset M$ oder auch $N \subseteq M$). Dabei steht \Rightarrow für **daraus folgt**.

Zwei Mengen M_1 und M_2 heißen **gleich** (geschrieben $M_1 = M_2$), wenn $M_1 \subset M_2$ und $M_2 \subset M_1$. Dies bedeutet $m \in M_1 \Leftrightarrow m \in M_2$. Hier steht das Symbol \Leftrightarrow für **genau dann wenn**, d.h. es gilt sowohl \Rightarrow also auch \Leftarrow .

Beispiel 1.1.5 $\{0, \dots, 9\} \subset \mathbb{N}_0$.

Definition 1.1.6 Sind M, N Mengen, dann ist

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

Komplement von N in M , als sogenanntes Venn-Diagramm siehe Abbildung 1.1. Weiter heißt

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

Vereinigung von M und N , siehe Abbildung 1.2, und

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

Durchschnitt von M und N , siehe Abbildung 1.3.

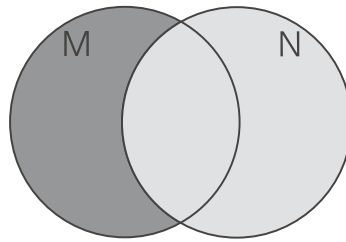


Abbildung 1.1: Komplement

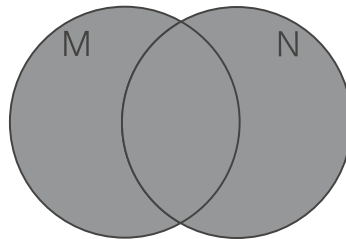


Abbildung 1.2: Vereinigung

Beispiel 1.1.7 $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

Notation 1.1.8 Für eine Indexmenge $I \neq \emptyset$ 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

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

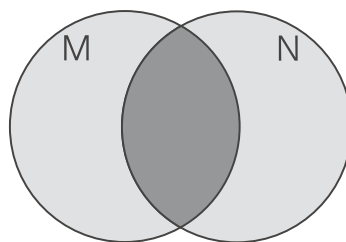


Abbildung 1.3: Durchschnitt

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

Wir kürzen **für alle** ab durch \forall und **es existiert** durch \exists .

Beispiel 1.1.9 Für $I = \{1, 2\}$ und gegebene Mengen M_1 und M_2 ist

$$\bigcap_{i \in I} M_i = M_1 \cap M_2.$$

Definition 1.1.10 Wir schreiben $|M|$ oder $\#M$ für die **Anzahl der Elemente** einer endlichen Menge M und, falls M unendlich viele Elemente hat, $|M| = \infty$.

Beispiel 1.1.11 Es ist $|\emptyset| = 0$, $|\{0, \dots, 9\}| = 10$ und $|\{0\}| = 1$.

Definition 1.1.12 Sind M_1, \dots, M_n Mengen, dann heißt die Menge der geordneten Tupel

$$M_1 \times \dots \times M_n = \{(m_1, \dots, m_n) \mid m_i \in M_i \ \forall i = 1, \dots, n\}$$

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

$$M^n = \underbrace{M \times \dots \times M}_{n\text{-mal}}$$

Die Elemente von M^n sind Listen (m_1, \dots, m_n) der Länge n mit Einträgen in M .

Beispiel 1.1.13 Es ist

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

Das Schachbrett ist das Produkt

$$\{a, \dots, h\} \times \{1, \dots, 8\} = \{(a, 1), \dots\},$$

der 3-dimensionale Raum

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

und die Menge der 8-bit Zahlen

$$\{0, 1\}^8 = \{(0, \dots, 0, 0), (0, \dots, 0, 1), \dots, (1, \dots, 1, 1)\}.$$

Definition 1.1.14 Sei M eine Menge. Die **Potenzmenge** von M ist

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

Satz 1.1.15 Sei M eine endliche Menge. Dann gilt

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

Beispiel 1.1.16 Potenzmengen:

$$2^\emptyset = \{\emptyset\}$$

$$2^{\{1\}} = \{\emptyset, \{1\}\}$$

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

Zum Beweis von Satz 1.1.15 verwenden wir das folgende allgemeine Beweisprinzip:

1.2 Vollständige Induktion

Angenommen wir haben für jedes $n \in \mathbb{N}_0$ eine beliebige Aussage $A(n)$ gegeben, und man hat gezeigt:

- 1) **Induktionsanfang:** $A(0)$ ist wahr.
- 2) **Induktionsschritt:** Es gilt für jedes $n > 0$, dass

$$A(n-1) \text{ ist wahr} \Rightarrow A(n) \text{ ist wahr.}$$

Dann ist $A(n)$ wahr für alle $n \in \mathbb{N}_0$, denn wir haben eine Kette von Schlussfolgerungen

$$A(0) \text{ wahr} \Rightarrow A(1) \text{ wahr} \Rightarrow A(2) \text{ wahr} \Rightarrow \dots$$

Bemerkung 1.2.1 Analog kann man natürlich vorgehen, um Aussagen $A(n)$ für $n \geq n_0$ mit $n_0 \in \mathbb{Z}$ zu beweisen. Man muss nur stets sicherstellen, dass man den Induktionsanfang $A(n_0)$ und alle verwendeten Folgepfeile in der Kette von Schlussfolgerungen

$$A(n_0) \text{ wahr} \Rightarrow A(n_0 + 1) \text{ wahr} \Rightarrow A(n_0 + 2) \text{ wahr} \Rightarrow \dots$$

bewiesen hat.

Mit vollständiger Induktion beweisen wir nun Satz 1.1.15:

Beweis. Durch Nummerieren der Elemente von M können wir ohne Einschränkung der Allgemeinheit (kurz geschrieben **OE**) annehmen, dass $M = \{1, \dots, n\}$, wobei wir die Konvention verwenden, dass $\{1, \dots, 0\} = \emptyset$. Wir müssen also zeigen, dass die Aussage

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

für alle $n \in \mathbb{N}_0$ gilt.

Induktionsanfang $n = 0$: Es ist $2^\emptyset = \{\emptyset\}$, also $|2^\emptyset| = 1 = 2^0$.

Induktionsschritt $n - 1$ nach n : Die Vereinigung

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

ist disjunkt, also folgt aus der **Induktionsvoraussetzung**

$$2^{\{1, \dots, n-1\}} = 2^{n-1},$$

dass

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

■

Im Folgenden diskutieren wir noch ein weiteres typisches Beispiel für einen Beweis mittels vollständiger Induktion.

Notation 1.2.2 Für Zahlen a_1, \dots, a_n schreiben wir

$$\sum_{k=1}^n a_k = a_1 + \dots + a_n$$

für deren Summe.

Genauso verwenden wir

$$\prod_{k=1}^n a_k = a_1 \cdot \dots \cdot a_n$$

für das Produkt.

Bemerkung 1.2.3 Gegeben eine Liste $a = (a_1, \dots, a_n)$ berechnet das folgende Computerprogramm diese Summe $s = \sum_{k=1}^n a_k$:

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

Wir verwenden hier die Syntax von MAPLE, siehe [18]. Siehe auch Übungsaufgabe 1.3.

Mit vollständiger Induktion können wir die folgende allgemeine Formel für $\sum_{k=1}^n k$ beweisen, die uns eine wesentlich effizientere Berechnung dieser speziellen Summe erlaubt:

Satz 1.2.4 Für alle $n \in \mathbb{N}_0$ gilt

$$\sum_{k=0}^n k = \frac{n(n+1)}{2}.$$

Beweis. *Induktionsanfang* $n = 0$: Es ist

$$\sum_{k=0}^0 k = 0 = \frac{0 \cdot (0+1)}{2}.$$

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, dass

$$\begin{aligned} \sum_{k=0}^{n+1} k &= \frac{n(n+1)}{2} + (n+1) \\ &= \frac{n(n+1) + 2(n+1)}{2} \\ &= \frac{(n+1)(n+2)}{2}. \end{aligned}$$

■

Für ein weiteres Beispiel siehe Übungsaufgabe 1.4.

Bemerkung 1.2.5 *Das Analogon zum Induktionsbeweis ist in der Informatik der rekursive Algorithmus. Beispielsweise berechnet die folgende rekursive Funktion die Summe $\sum_{k=0}^n k$:*

```
sumints:=proc(n)
  if n=0 then return(0);fi;
  return(sumints(n-1)+n);
end proc;
```

Wir können auch ausgehend vom Beweis von Satz 1.1.15 eine rekursive Funktion schreiben, die alle Teilmengen von $\{1, \dots, n\}$ bestimmt. Für die Implementierung siehe Übungsaufgabe 1.8. Einen anderen Induktionsbeweis, der einen rekursiven Algorithmus liefert, besprechen wir in den Aufgaben 1.10 und 1.11.

Für weitere Beispiele zur Induktion siehe die Übungsaufgaben 1.5, 1.6, 1.7 und 1.12.

1.3 Relationen

Auf die folgende Weise können wir Beziehungen zwischen zwei Mengen beschreiben:

Definition 1.3.1 *Eine **Relation** zwischen Mengen M und N ist gegeben durch eine Teilmenge $R \subset M \times N$.*

Beispiel 1.3.2 *Für $M = \{2, 3, 7\}$, $N = \{4, 5, 6\}$ und*

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

gilt

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

Die wichtigste Rolle spielen Relationen bei denen jedem Element von M genau ein Element von N zugeordnet wird:

1.4 Abbildungen

Definition 1.4.1 Eine **Abbildung** $f: M \rightarrow N$ 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

$$\begin{aligned} f: M &\rightarrow N \\ m &\mapsto f(m). \end{aligned}$$

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

Für eine Teilmenge $A \subset M$ heißt

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

Bild von A unter f , und

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

bezeichnen wir als 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 .

Bemerkung 1.4.2 Hat man eine Abbildung durch eine Abbildungsvorschrift $f: M \rightarrow N$, $m \mapsto f(m)$ gegeben, so ist die Darstellung von f als Relation nichts anderes als der Graph

$$R = \text{Graph}(f) = \{(m, f(m)) \mid m \in M\} \subset M \times N$$

von f .

Beispiel 1.4.3 Für

$$\begin{aligned} f: \mathbb{R} &\rightarrow \mathbb{R} \\ x &\mapsto f(x) = x^2 \end{aligned}$$

ist

$$R = \text{Graph}(f) = \{(x, x^2) \mid x \in \mathbb{R}\},$$

siehe Abbildung 1.4. Das Bild von f ist

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

und beispielsweise gilt

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

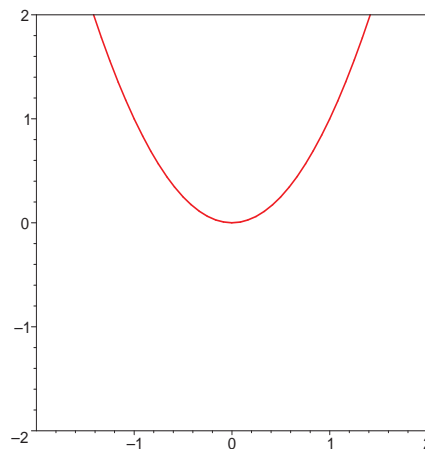


Abbildung 1.4: Graph der Parabel

Definition 1.4.4 Eine Abbildung $f : M \rightarrow N$ heißt **surjektiv**, wenn für das Bild von f gilt

$$f(M) = N.$$

Gilt für alle $m_1, m_2 \in M$, dass

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

so heißt f **injektiv**.

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

Beispiel 1.4.5 Die Parabelfunktion

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

aus Beispiel 1.4.3 ist weder injektiv noch surjektiv. Als Abbildung auf ihr Bild

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

wird sie surjektiv. Die Abbildung

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

bei der wir auch die Quelle einschränken ist bijektiv. Die Hyperbel

$$\mathbb{R} \setminus \{0\} \rightarrow \mathbb{R}, x \mapsto \frac{1}{x}$$

ist injektiv, aber nicht surjektiv (siehe Abbildung 1.5).

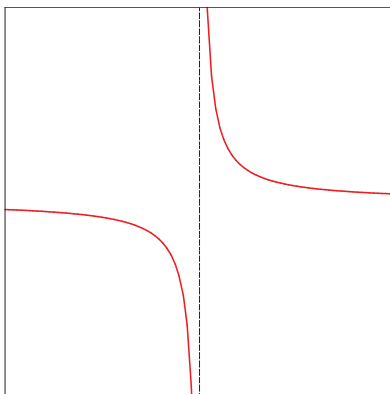


Abbildung 1.5: Hyperbel

Satz 1.4.6 (Schubfachprinzip) Sind M, N endliche Mengen und ist $f : M \rightarrow N$ eine injektive Abbildung, dann gilt $|M| \leq |N|$.

Beispiel 1.4.7 Sei $M = \{1, 2, 3\}$ und $N = \{1, 2\}$. Wegen $|M| > |N|$ gibt es keine injektive Abbildung $f : M \rightarrow N$.

Abbildung 1.6 zeigt ein Beispiel einer Abbildung $f : M \rightarrow N$. Es ist $f(1) = f(3)$, also f nicht injektiv.

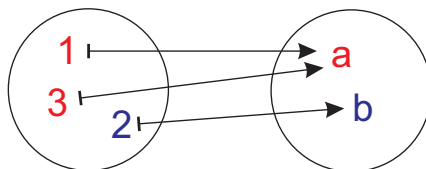


Abbildung 1.6: Eine nicht-injektive Abbildung

Wir zeigen nun Satz 1.4.6:

Beweis. Es gilt

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

denn $f^{-1}(\{n\})$ hat genau 1 Element, wenn n im Bild von f liegt (da f injektiv), und ist leer sonst. ■

Da eine Abbildung jedem Element der Quelle genau ein Bildelement zuordnet, folgt die entsprechende Aussage für surjektiv:

Satz 1.4.8 Sind M, N endliche Mengen und $f : M \rightarrow N$ eine surjektive Abbildung, dann gilt $|M| \geq |N|$.

Kombinieren wir Satz 1.4.6 und Satz 1.4.8, so erhalten wir:

Corollar 1.4.9 Sind M, N endliche Mengen und $f : M \rightarrow N$ eine bijektive Abbildung, dann gilt $|M| = |N|$.

Definition und Satz 1.4.10 Ist $f : M \rightarrow N$ bijektiv, dann gibt es eine eindeutig bestimmte **Umkehrabbildung**

$$f^{-1} : N \rightarrow M, y \mapsto x \text{ falls } f(x) = y.$$

Es gilt

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

für alle $x \in M$ bzw. $y \in N$. Weiter ist f^{-1} bijektiv.

Beweis. Die Umkehrabbildung ist **wohldefiniert** (d.h. die Definition ordnet jedem Element der Quelle ein eindeutiges Element des Ziels zu): Zu jedem $y \in N$ gibt es genau ein $x \in M$ mit $f(x) = y$. Wegen f surjektiv existiert ein solches x , und wegen f injektiv, ist dieses x eindeutig bestimmt.

Die beiden Gleichungen sind klar nach Definition. Zur Bijektivität von f^{-1} : Da für jedes $x \in M$ gilt $f^{-1}(f(x)) = x$, ist f^{-1} surjektiv. Bei der Injektivität verwenden wir insbesondere, dass f eine Abbildung ist: Sind $y_1, y_2 \in N$ und $x_i \in M$ mit $y_i = f(x_i)$, dann folgt aus

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

dass $y_1 = f(x_1) = f(x_2) = y_2$. ■

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

Bemerkung 1.4.11 Die Umkehrabbildung f^{-1} ist die Relation

$$\{(f(x), x) \mid x \in M\} \subset N \times M.$$

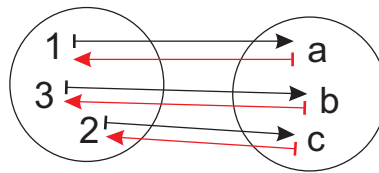


Abbildung 1.7: Eine bijektive Abbildung und ihre Umkehrabbildung

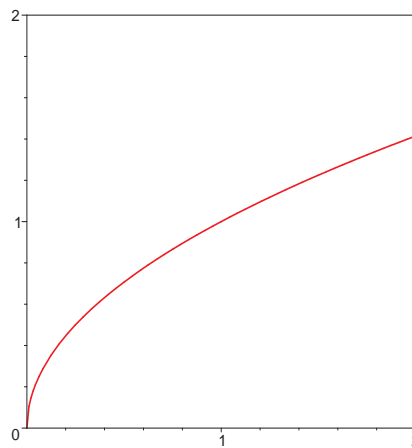


Abbildung 1.8: Wurzel

Beispiel 1.4.12 *Abbildung 1.7 zeigt eine bijektive Abbildung $f : \{1, 2, 3\} \rightarrow \{a, b, c\}$ und ihre Umkehrabbildung f^{-1} . Die Umkehrabbildung der bijektiven Abbildung*

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

ist

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

wie in Abbildung 1.8 dargestellt.

Siehe auch die Übungsaufgaben [1.14](#), [1.17](#), [1.18](#) und [1.19](#).

Definition 1.4.13 *Seien $f : M \rightarrow N$ und $g : N \rightarrow L$ Abbildungen, dann ist die Komposition von f und g definiert als*

$$\begin{aligned} g \circ f : M &\rightarrow L \\ m &\mapsto g(f(m)) \end{aligned}$$

Lemma 1.4.14 *Die Komposition von Abbildungen ist assoziativ, das heißt für Abbildungen*

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

gilt

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

Zum Beweis siehe Übungsaufgabe 1.15.

Beispiel 1.4.15 *Selbst wenn $f : M \rightarrow M$ und $g : M \rightarrow M$ ist im Allgemeinen $f \circ g \neq g \circ f$. Zum Beispiel für*

$$\begin{aligned} f : \mathbb{R}^2 &\rightarrow \mathbb{R}^2, (x, y) \mapsto (x + y, y) \\ g : \mathbb{R}^2 &\rightarrow \mathbb{R}^2, (x, y) \mapsto (x, x + y) \end{aligned}$$

erhalten wir

$$\begin{aligned} f \circ g : \mathbb{R}^2 &\rightarrow \mathbb{R}^2, (x, y) \mapsto (2x + y, x + y) \\ g \circ f : \mathbb{R}^2 &\rightarrow \mathbb{R}^2, (x, y) \mapsto (x + y, x + 2y). \end{aligned}$$

Definition 1.4.16 *Sei M eine Menge. Die **identische Abbildung** auf M ist*

$$\begin{aligned} \text{id}_M : M &\rightarrow M \\ m &\mapsto m \end{aligned}$$

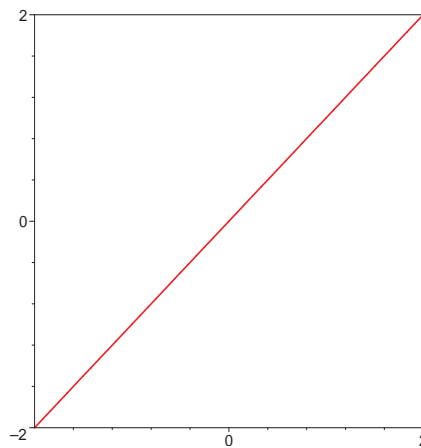
Beispiel 1.4.17 *Abbildung 1.9 zeigt den Graphen von $\text{id}_{\mathbb{R}}$.*

Die beiden Gleichungen in Definition und Satz 1.4.10 schreiben sich dann wie folgt:

Satz 1.4.18 *Ist $f : M \rightarrow N$ eine bijektive Abbildung, so gilt*

$$f^{-1} \circ f = \text{id}_M \quad f \circ f^{-1} = \text{id}_N$$

Tatsächlich liefern diese beiden Gleichungen eine Charakterisierung von bijektiv und legen die Umkehrabbildung eindeutig fest. Siehe dazu Übungsaufgabe 1.16.

Abbildung 1.9: Identische Abbildung $\mathbb{R} \rightarrow \mathbb{R}$

1.5 Halbordnungen und Äquivalenzrelationen

Definition 1.5.1 Eine Relation $R \subset M \times M$ auf einer Menge M heißt

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

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

- *antisymmetrisch*, wenn

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

Ist R reflexiv, transitiv und antisymmetrisch, so spricht man von einer **Halbordnung**. Gilt außerdem für alle $m, n \in M$, dass $(m, n) \in R$ oder $(n, m) \in R$, so heißt R **Totalordnung**.

Beispiel 1.5.2 1) Die Inklusion \subset zwischen Teilmengen einer Menge 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 $B \subset C \implies A \subset C$ (transitiv)
- $A \subset B$ und $B \subset A \implies A = B$ (antisymmetrisch).

Im Allgemeinen ist \subset keine Totalordnung, z.B. ist für $M = \{1, 2\}$ weder $\{1\} \subset \{2\}$ noch $\{2\} \subset \{1\}$.

2) Dagegen ist \leq auf \mathbb{R} eine Totalordnung.

Der Begriff der Äquivalenzrelation schwächt den Begriff der Gleichheit ab.

Definition 1.5.3 Sei M eine Menge und $R \subset M \times M$ eine reflexive und transitive Relation. Ist R außerdem **symmetrisch**, das heißt

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

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

Beispiel 1.5.4 Gleichheit ist eine Äquivalenzrelation.

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

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

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

eine Äquivalenzrelation auf M definiert.

Definition 1.5.5 Ist M eine Menge, \sim eine Äquivalenzrelation und $m \in M$, dann heißt

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

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

$$\begin{aligned} \pi: M &\rightarrow M/\sim \\ m &\mapsto [m] \end{aligned}$$

für die **kanonische Abbildung**.

Satz 1.5.6 *Je zwei Äquivalenzklassen sind gleich oder disjunkt.*

Beweis. Sei $[m] \cap [n] \neq \emptyset$. 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. ■

Eine Äquivalenzrelation partitioniert (unterteilt) also M in die Äquivalenzklassen.

Bemerkung 1.5.7 *Es gilt*

$$m_1 \sim m_2 \iff [m_1] = [m_2]$$

d.h. Äquivalenz übersetzt sich in Gleichheit von Äquivalenzklassen.

Beispiel 1.5.8 *Die Äquivalenzklassen unter der Äquivalenzrelation gleich groß sein auf einer Menge M von Menschen (siehe Beispiel 1.5.4) sind die Teilmengen der Menschen, die jeweils dieselbe Körpergröße haben. Somit steht die Menge der Äquivalenzklassen M/\sim in Bijektion zu der Menge aller vorkommenden Körpergrößen. Ein Kleiderverkäufer interessiert sich nicht für m sondern für $[m]$.*

Beispiel 1.5.9 *Betrachte die Äquivalenzrelation \sim auf \mathbb{R}^2 gegeben durch*

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

mit

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

Die Äquivalenzklassen sind die konzentrischen Kreise (und der Punkt $(0, 0)$)

$$K_s = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = s\}$$

für $s \in \mathbb{R}_{\geq 0}$. Beispielsweise ist

$$[(1, 2)] = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 5\}.$$

Es ist also

$$M / \sim = \{K_s \mid s \in \mathbb{R}_{\geq 0}\},$$

und die Abbildung $\mathbb{R}_{\geq 0} \rightarrow M / \sim$, $s \mapsto K_s$ ist bijektiv. Siehe Abbildung 1.10.

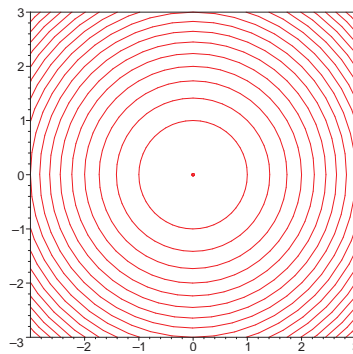


Abbildung 1.10: Äquivalenzklassen

1.6 Übungsaufgaben

Übung 1.1 Sei M eine Menge. Zeigen Sie für Teilmengen $A, B, C \subset M$, zum Beispiel mit Hilfe von Venn-Diagrammen:

1) Für \cap gilt:

(a) Kommutativität $A \cap B = B \cap A$,

(b) Identität $A \cap M = A$,

(c) Assoziativität $A \cap (B \cap C) = (A \cap B) \cap C$.

2) Für \cup gilt:

(a) Kommutativität $A \cup B = B \cup A$,

(b) Identität $A \cup \emptyset = A$,

(c) Assoziativität $A \cup (B \cup C) = (A \cup B) \cup C$.

3) Für \cap und \cup gelten die Distributivgesetze

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

4) Vergleichen Sie mit den Rechenregeln für ganze Zahlen.

Übung 1.2 Zeigen Sie für endliche Mengen M und N , dass

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

und

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

Übung 1.3 Schreiben Sie ein Programm, das für eine Liste $a = (a_1, \dots, a_n) \in \mathbb{Z}^n$ die Summe

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

berechnet.

Übung 1.4 Zeigen Sie mit vollständiger Induktion, dass

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

für alle $n \in \mathbb{N}$.

Übung 1.5 Stellen Sie eine Formel für

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

auf und beweisen Sie diese.

Übung 1.6 Stellen Sie eine Formel für

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

auf und beweisen Sie diese.

Übung 1.7 Zeigen Sie für $q \in \mathbb{R}$, $q \neq 1$ mit vollständiger Induktion

$$\sum_{k=0}^n q^k = \frac{1 - q^{n+1}}{1 - q}$$

Übung 1.8 Schreiben Sie eine Funktion, die rekursiv alle Teilmengen von $\{1, \dots, n\}$ bestimmt.

Übung 1.9 Sei $0 \leq k \leq n$. Zeigen Sie: Für die Anzahl $\binom{n}{k}$ der k -elementigen Teilmengen einer n -elementigen Menge gilt

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

wobei $n! = 1 \cdot 2 \cdot \dots \cdot n$.

Übung 1.10 Das Spiel "Die Türme von Hanoi" besteht aus 3 Spielfeldern, auf denen n Scheiben paarweise verschiedener Größe gestapelt werden können (siehe Abbildung 1.11). 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.

Übung 1.11 Schreiben Sie ein rekursives Programm, das das Spiel "Die Türme von Hanoi" löst.

Übung 1.12 In einem amerikanischen Stadtplan mit n Avenues und m Streets (siehe Abbildung 1.12) wollen wir von Punkt A nach Punkt B gehen. Wieviele kürzeste Wege gibt es?

Beweisen Sie die Formel mit vollständiger Induktion nach $n + m$.

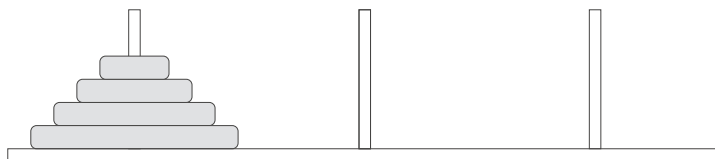
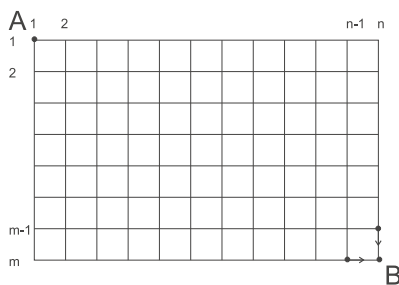


Abbildung 1.11: Die Türme von Hanoi

Abbildung 1.12: Wieviele kürzeste Wege gibt es von A nach B .

Übung 1.13 Geben Sie je ein Beispiel für eine Abbildung $\mathbb{N} \rightarrow \mathbb{N}$, die

- 1) injektiv aber nicht surjektiv ist,
- 2) surjektiv aber nicht injektiv ist.

Übung 1.14 Auf einem Fest treffen sich n Personen. Zeigen Sie, dass zwei von diesen mit derselben Anzahl von Anwesenden bekannt sind.

Übung 1.15 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 1.16 Sei $f : M \rightarrow N$ eine Abbildung. Zeigen Sie:

- 1) f ist injektiv genau dann, wenn es eine Abbildung $g : f(M) \rightarrow M$ gibt mit $g \circ f = \text{id}_M$.

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

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

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

Übung 1.17 Seien M, N endliche Mengen mit $|M| = |N|$ und $f: M \rightarrow N$ eine Abbildung. Zeigen Sie, dass folgende Aussagen äquivalent sind:

1) f ist bijektiv,

2) f ist injektiv,

3) f ist surjektiv.

Übung 1.18 Seien die Zahlen $1, \dots, 101$ 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 1.19 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.

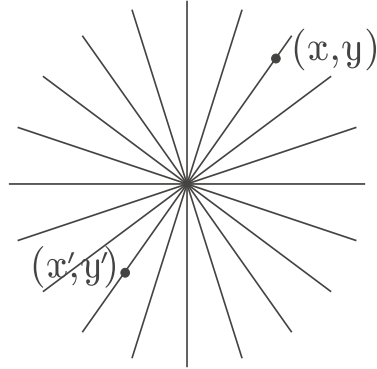
Übung 1.20 Sei M eine *unendliche* Menge. Zeigen Sie:

1) Es gibt keine surjektive Abbildung $\varphi: M \rightarrow 2^M$.

2) Es gibt keine injektive Abbildung $\psi: 2^M \rightarrow M$.

Übung 1.21 Sei $M := \mathbb{R}^2 \setminus \{(0, 0)\}$ die Menge der Punkte der reellen Ebene ohne den 0-Punkt. Auf M definiere $(x, y) \sim (x', y')$

genau dann, wenn es eine Gerade durch $(0,0) \in \mathbb{R}^2$ gibt, auf der sowohl der Punkt (x,y) als auch der Punkt (x',y') liegen.



- 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.

2

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.

2.1 Die ganzen Zahlen und Division mit Rest

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

$$\begin{aligned}a + (b + c) &= (a + b) + c \\ a \cdot (b \cdot c) &= (a \cdot b) \cdot c\end{aligned}$$

Kommutativgesetz

$$\begin{aligned}a + b &= b + a \\ a \cdot b &= b \cdot a\end{aligned}$$

und Distributivgesetz

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

gehörten 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 $\mathbb{Z} = \{0, 1, -1, 2, -2, \dots\}$ wie folgt:

Bemerkung 2.1.1 *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 2.2). 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

$$\begin{aligned} [(0, 0)] + [(a, b)] &= [(a, b)] \\ [(1, 0)] \cdot [(a, b)] &= [(a, b)]. \end{aligned}$$

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 Konto mit keinem Guthaben oder keinen Schulden: Für $a \geq b$ sei $c \in \mathbb{N}_0$ mit $a = b + c$. Dann gilt $(a, b) \sim (c, 0)$ und wir schreiben

$$c := [(a, b)].$$

Für $a < b$ sei $c \in \mathbb{N}$ mit $b = a + c$. Dann gilt $(a, b) \sim (0, c)$ und wir setzen

$$-c := [(a, b)].$$

Es gilt dann

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

für alle $c \in \mathbb{Z} \setminus \{0\}$ und $0 + 0 = 0$.

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

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

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 2.1.2 (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 2.1.3 *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 2.1.2:

Beweis. Existenz: Ohne Einschränkung ist $b > 0$. Die Menge

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

hat ein kleinstes Element w . Setze dann

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

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

$$0 \leq r_1 - r_2 = b \cdot (q_2 - q_1) < |b|,$$

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

Beispiel 2.1.5 *Für $a = 2225$ und $b = 7$ schreiben wir*

$$\begin{array}{r} 2225 = 7 \cdot 300 + 7 \cdot 10 + 7 \cdot 7 + 6 = 7 \cdot 317 + 6 \\ \underline{-2100} \\ 125 \\ \underline{-70} \\ 55 \\ \underline{-49} \\ 6 \end{array}$$

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

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

Definition 2.1.6 *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

$$a \equiv b \pmod{m}$$

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

Beispiel 2.1.7 $1 \equiv 7 \pmod{3}$.

Kongruent modulo m zu sein ist eine Äquivalenzrelation, siehe dazu Übungsaufgabe 2.3. 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

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

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

Beispiel 2.1.8 *Kongruenz modulo 3 partitioniert \mathbb{Z} in die 3 Restklassen*

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

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.

2.2 Fundamentalsatz der Arithmetik

Definition 2.2.1 Ein Element $p \in \mathbb{Z}_{>1}$ heißt **Primzahl**, wenn aus $p = a \cdot b$, $a, b \in \mathbb{Z}_{\geq 1}$ folgt $a = 1$ oder $b = 1$.

Beispiel 2.2.2 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 2.2.3 (Fundamentalsatz der Arithmetik) Jede Zahl $n \in \mathbb{Z} \setminus \{0, 1, -1\}$ hat eine eindeutige Darstellung

$$n = \pm 1 \cdot p_1^{r_1} \cdot \dots \cdot p_s^{r_s}$$

mit Primzahlen $p_1 < \dots < p_s$ 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

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

mit $p_1 \leq \dots \leq p_s$ und $q_1 \leq \dots \leq q_t$. 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

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

nach Induktionsvoraussetzung eine eindeutige Primfaktorzerlegung und die Behauptung folgt.

Angenommen es wäre $p_1 < q_1$. Dann gilt

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

also hat $N_1 = N_2$ nach Induktionsvoraussetzung eine eindeutige Primfaktorzerlegung. Wegen $p_1 < q_1 \leq \dots \leq q_t$ 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 2.2.4 $24 = 2^3 \cdot 3$.

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 2.2.5 (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 2.2.6 (Euklids zweiter Satz) *Es gibt unendlich viele Primzahlen.*

Beweis. Sei $M = \{p_1, \dots, p_r\}$ eine endliche Menge von Primzahlen. Wir zeigen, dass es eine Primzahl gibt, die nicht in M enthalten ist. Die Zahl $N = p_1 \cdot \dots \cdot p_r + 1$ 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 2.2.7 (Primzahlsatz) *Sei für $x \in \mathbb{R}_{>0}$*

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

dann gilt

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

Beispiel 2.2.8 *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 2.5.

2.3 Größter gemeinsamer Teiler und Euklidischer Algorithmus

Definition 2.3.1 Sind $a_1, \dots, a_t \in \mathbb{Z}$, dann heißt $d \in \mathbb{N}$ **größter gemeinsamer Teiler** von a_1, \dots, a_t , geschrieben $d = \text{ggT}(a_1, \dots, a_t)$, wenn gilt

- 1) $d \mid a_j$ für alle $j = 1, \dots, t$, 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 $j = 1, \dots, t$, dann gilt $\tilde{d} \mid d$.

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

- 1) $a_j \mid m$ für alle $j = 1, \dots, t$, 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 $j = 1, \dots, t$, dann gilt $m \mid \tilde{m}$.

Bemerkung 2.3.2 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

$$\text{ggT}(a_1, \dots, a_t) = \prod_{i=1}^s p_i^{\min\{r_{ji} \mid j\}} \quad (2.1)$$

(und für kgV analog mit dem Maximum). Zwei Zahlen $a, b \in \mathbb{Z}$ sind teilerfremd genau dann, wenn

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

Beispiel 2.3.3 Die gemeinsamen Teiler von $18 = 2 \cdot 3^2$ und $66 = 2 \cdot 3 \cdot 11$ sind 1, 2, 3 und 6, also gilt

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

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

Satz 2.3.4 (Euklidischer Algorithmus) *Seien $a_1, a_2 \in \mathbb{Z} \setminus \{0\}$. 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

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

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

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

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}, \dots, 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, \dots, a_n . ■

Beispiel 2.3.5 *Wir bestimmen den ggT von 66 und 18 mit Hilfe des Euklidischen Algorithmus, d.h. durch sukzessive Division mit Rest:*

$$\begin{aligned} 66 &= 3 \cdot 18 + 12 \\ 18 &= 1 \cdot 12 + 6 \\ 12 &= 2 \cdot 6 + 0 \end{aligned}$$

Somit ist $\text{ggT}(66, 18) = 6$, 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

$$t \mid 12 \text{ und } t \mid 6 \text{ also } t \mid 6 \text{ also } t \mid 3.$$

Weiter erhalten wir eine Darstellung von $\text{ggT}(36, 15)$ 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 übernächsten Abschnitt über den Chinesischen Restsatz diskutieren.

2.4 Primfaktorisierung

Zunächst behandeln wir folgendes offensichtliche Primfaktorisierungsverfahren:

Algorithmus 2.4.1 (Probedivision) Sei $n \in \mathbb{N}$ zusammengesetzt (nicht prim). Für den kleinsten Primteiler p von n gilt

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

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 $p \leq \lfloor \sqrt{n} \rfloor$. ■

Beispiel 2.4.2 Zum Faktorisieren von 234 mittels Probedivision testen wir zunächst, ob n durch eine Primzahl $p \leq \lfloor \sqrt{234} \rfloor = 15$ teilbar ist. Wir finden

$$234 = 2 \cdot 117.$$

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

$$117 = 3 \cdot 39.$$

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

$$39 = 3 \cdot 13.$$

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

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

Beispiel 2.4.3 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 2.4.4 (Sieb des Eratosthenes) *Wir erhalten eine Liste aller Primzahlen kleiner gleich $N \in \mathbb{N}$, $N \geq 4$ wie folgt:*

- 1) *Erstelle eine boolesche Liste L mit einem Eintrag zu jeder Zahl $2, \dots, N$. 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. Induktiv sehen wir, dass q in Schritt (3) stets prim ist, da p die größte Primzahl $< q$ ist, und somit schon alle Vielfachen $j \cdot x$ von allen Primzahlen $x < q$ als *false* markiert sind. Der Algorithmus terminiert also, wenn alle Zahlen als *false* markiert wurden, die eine Primzahl $p \leq \sqrt{N}$ als echten Teiler haben, d.h. nicht prim sind. ■

Beispiel 2.4.5 *Wir bestimmen alle Primzahlen ≤ 15 und geben in jedem Durchlauf die Liste aller j mit $L_j = \text{true}$ 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.

2.5 Der chinesische Restsatz

Satz 2.5.1 (Chinesischer Restsatz in \mathbb{Z}) Sind $n_1, \dots, n_r \in \mathbb{N}$ paarweise teilerfremd und $a_1, \dots, a_r \in \mathbb{Z}$, dann ist die **simultane Kongruenz**

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

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

Beweis. Sei

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

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

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

Dann ist

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

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 $\text{kgV}(n_1, \dots, n_r) \mid (x - x')$. Da die n_i paarweise teilerfremd sind, ist $\text{kgV}(n_1, \dots, n_r) = n_1 \cdot \dots \cdot n_r$, 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 2.5.2 Gegeben $n_1, n_2 \in \mathbb{N}$ teilerfremd und $a_1, a_2 \in \mathbb{Z}$, bestimmen wir eine Lösung der simultanen Kongruenzen

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

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

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

Wegen

$$\begin{aligned}un_1 &\equiv 0 \pmod{n_1} \\un_1 &\equiv 1 \pmod{n_2} \\vn_2 &\equiv 1 \pmod{n_1} \\vn_2 &\equiv 0 \pmod{n_2}\end{aligned}$$

gilt dann für

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

dass

$$\begin{aligned}z &\equiv a_1 \pmod{n_1} \\z &\equiv a_2 \pmod{n_2}\end{aligned}$$

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

$$\left. \begin{aligned}x &\equiv a_1 \pmod{n_1} \\x &\equiv a_2 \pmod{n_2}\end{aligned} \right\} \iff x \equiv z \pmod{n_1 n_2}$$

Iteratives Anwenden liefert einen weiteren Beweis von Satz 2.5.1.

Den Chinesischen Restsatz werden wir später wesentlich allgemeiner formulieren.

Beispiel 2.5.3 Wir lösen die simultane Kongruenz

$$\begin{aligned}x &\equiv -28 \pmod{30} \\x &\equiv 5 \pmod{7}\end{aligned}$$

Es ist $\text{ggT}(30, 7) = 1$, 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. $u = -3$, $v = 13$. Die Lösungsformel aus dem Beweis des Chinesischen Restsatzes liefert

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

Der Chinesische Restsatz erlaubt uns also zwei Kongruenzen durch eine einzelne Kongruenz zu ersetzen:

$$\left. \begin{array}{l} x \equiv -28 \pmod{30} \\ x \equiv 5 \pmod{7} \end{array} \right\} \Leftrightarrow x \equiv -2998 \equiv 152 \pmod{210}.$$

Für letztere können wir die Lösungsmenge direkt angeben, sie ist

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

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

$$\begin{array}{l} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \end{array}$$

genau dann lösbar, wenn

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

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

Dies zeigen wir in Übungsaufgabe 2.12, indem wir die entsprechende Lösungsformel herleiten.

2.6 Übungsaufgaben

Übung 2.1 Sei $n \in \mathbb{N}$ und $M \subset \{1, \dots, 2n\}$ 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 2.2 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

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

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

$$a \equiv b \pmod{m}$$

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

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

3) Zeigen Sie, dass $\frac{56249121391}{123259} \in \mathbb{Z}$.

Übung 2.4 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 2.5 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 2.6 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 2.7 Implementieren Sie den erweiterten Euklidischen Algorithmus. Testen Sie Ihre Implementierung an Beispielen.

Übung 2.8 Kürzen Sie

$$\frac{93497059597}{18856392791}$$

Übung 2.9 Auf ein ursprünglich leeres Konto werden regelmäßig 2809 € gutgeschrieben, und gelegentlich 10403 € abgebucht. Ist es möglich, dass das Konto irgendwann einen Kontostand von genau 1 € hat?

Übung 2.10 *Implementieren Sie*

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

114365889060301309.

Übung 2.11 *Bestimmen Sie die Menge $L \subset \mathbb{Z}$ aller Lösungen x der simultanen Kongruenzen*

$$x \equiv 1 \pmod{3}$$

$$x \equiv 2 \pmod{5}$$

$$x \equiv 1 \pmod{7}$$

Übung 2.12 *Seien $a_1, a_2 \in \mathbb{Z}$ und $n_1, n_2 \in \mathbb{Z}_{>0}$. Zeigen Sie: Die simultanen Kongruenzen*

$$x \equiv a_1 \pmod{n_1}$$

$$x \equiv a_2 \pmod{n_2}$$

sind genau dann lösbar, wenn

$$a_1 - a_2 \equiv 0 \pmod{\text{ggT}(n_1, n_2)}$$

Die Lösung ist eindeutig modulo dem kgV (n_1, n_2) .

Übung 2.13 *Lassen sich die beiden Konfigurationen von Zahnrädern in Abbildung 2.1 durch Drehung ineinander überführen? Falls ja, um wieviele Schritte muss man dafür drehen?***Übung 2.14** *Bestimmen Sie die Menge $L \subset \mathbb{Z}$ aller Lösungen x der simultanen Kongruenzen*

$$x \equiv 1 \pmod{108}$$

$$x \equiv 25 \pmod{80}$$

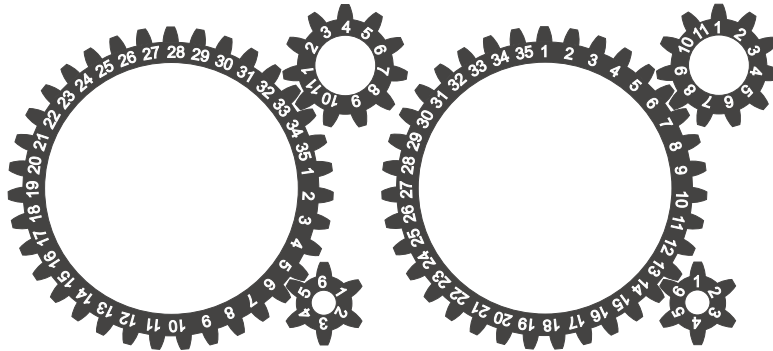


Abbildung 2.1: Zwei Konfigurationen von drei Zahnrädern

Übung 2.15 Schreiben Sie mit Hilfe Ihrer Implementierung des erweiterten Euklidischen Algorithmus (oder der MAPLE-Funktion `igcdex`) eine Prozedur, die die Lösungsmenge der simultanen Kongruenzen

$$x \equiv a_1 \pmod{n_1}$$

$$x \equiv a_2 \pmod{n_2}$$

für $a_1, a_2 \in \mathbb{Z}$ und $n_1, n_2 \in \mathbb{Z}_{>0}$ mit $\text{ggT}(n_1, n_2) = 1$ 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.

3

Gruppen

3.1 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 3.1) 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 3.2.

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

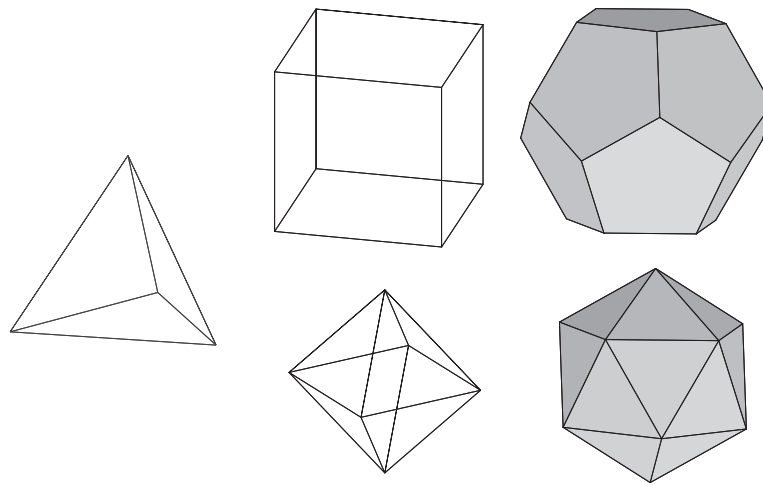


Abbildung 3.1: Die Platonischen Körper

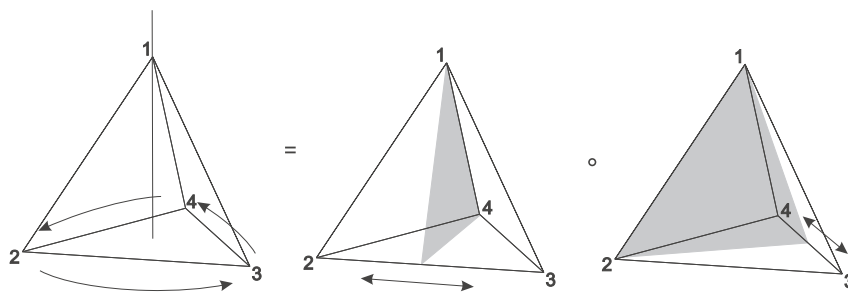


Abbildung 3.2: Komposition von zwei Symmetrien des Tetraeders

einigen offensichtlichen Zusatzbedingungen)

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

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

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

und von G auf sich selbst durch Konjugation

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

Die Translation werden wir im Detail diskutieren und auf die Konjugation in Übung 3.12 zurückkommen.

3.2 Gruppen und Operationen

3.2.1 Grundbegriffe

Definition 3.2.1 Eine **Gruppe** (G, \circ) ist eine Menge G zusammen mit einer **Verknüpfung**

$$\begin{aligned} \circ: G \times G &\longrightarrow G \\ (a, b) &\longmapsto a \circ b \end{aligned}$$

die folgende Axiome erfüllt:

(G1) *Assoziativität*

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

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

$$e \in G$$

mit

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

(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

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

dann heißt G **abelsch**.

Eine Menge G zusammen mit einer Verknüpfung

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

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

- 1) Für $a, b \in G$ gilt: Ist $ab = e$, dann ist auch $ba = e$.
- 2) Es ist $a \circ e = a$ für alle $a \in G$.

Bemerkung 3.2.3 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 $(ab)^{-1} = b^{-1}a^{-1}$.
- 4) Für $a \in G$ ist $(a^{-1})^{-1} = a$.

Diese Aussagen zeigen wir in Übung 3.2.

Neben den in Abschnitt 3.1 angesprochenen Symmetriegruppen wollen wir noch die folgenden zentralen Beispiele von Gruppen diskutieren:

Beispiel 3.2.4 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

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

bildet eine Gruppe.

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

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

zusammen mit der Komposition ist eine Gruppe.

Speziell für

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

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

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

die **symmetrische Gruppe**. Offenbar gilt

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

Für $\sigma \in S_n$ schreiben wir auch

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

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 3.3 mit der Permutation

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

und die Spiegelung in Abbildung 3.4 mit der Transposition

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

identifizieren.

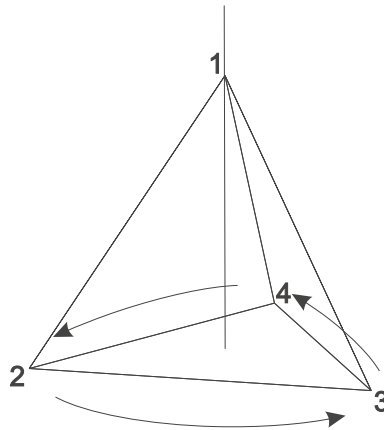


Abbildung 3.3: Eine Drehsymmetrie des Tetraeders

5) Sei

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

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

$$w = b_1 b_2 \dots b_n$$

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

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

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 $\alpha^{-1}, \beta^{-1}, \dots$ mit der Rechenregel

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

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

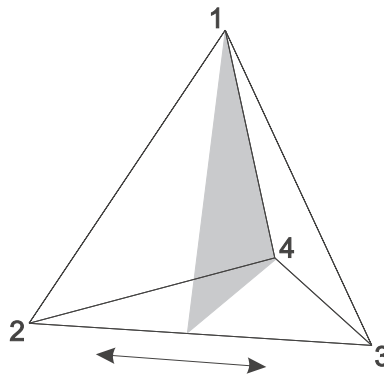


Abbildung 3.4: Eine Spiegelsymmetrie des Tetraeders

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 3.2.5 (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 $a, b \in H \implies a \circ b \in H, b^{-1} \in H$)

2) $H \neq \emptyset$, und $a, b \in H \implies a \circ b^{-1} \in H$.

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

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

■

Beispiel 3.2.6 Sei G die Symmetriegruppe des Tetraeders, r_{120} die Drehung in Abbildung 3.3 und s_{23} die Spiegelung in Abbildung 3.4. Dann sind

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

jeweils Untergruppen.

Beispiel 3.2.7 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 3.2.8 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

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

(siehe auch Übungsaufgabe 2.3).

Die Menge der Restklassen

$$\mathbb{Z}_n := \mathbb{Z}/n := \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$$

wird mit der Verknüpfung

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

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

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

Ist $\bar{a}_1 = \bar{a}_2$ und $\bar{b}_1 = \bar{b}_2$, also $n \mid (a_1 - a_2)$ und $n \mid (b_1 - b_2)$, so gilt

$$\bar{a}_1 + \bar{b}_1 = \overline{a_1 + b_1} = \overline{a_2 + b_2} = \bar{a}_2 + \bar{b}_2$$

denn $n \mid (a_1 - a_2 + b_1 - b_2)$.

Beispiel 3.2.9 Für $n = 3$ ist $\mathbb{Z}/3 = \{\bar{0}, \bar{1}, \bar{2}\}$ mit

$$\bar{0} = \{\dots, -3, 0, 3, 6, \dots\} = 3\mathbb{Z}$$

$$\bar{1} = \{\dots, -2, 1, 4, 7, \dots\} = 1 + 3\mathbb{Z}$$

$$\bar{2} = \{\dots, -1, 2, 5, 8, \dots\} = 2 + 3\mathbb{Z}$$

siehe auch Abbildung 3.5.

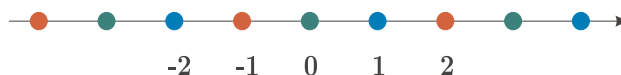


Abbildung 3.5: Restklassen modulo 3

Die Verknüpfung kann man durch die **Gruppentafel**

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

beschreiben, beispielsweise gilt $\bar{2} + \bar{2} = \overline{2+2} = \bar{4} = \bar{1}$.

Beispiel 3.2.10 Für jeden Teiler a von n und $d = \frac{n}{a}$ ist

$$\{\bar{0}, \bar{a}, \bar{2a}, \dots, \overline{(d-1)a}\} \subset \mathbb{Z}/n$$

eine Untergruppe (Übung).

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

$$\{\bar{0}, \bar{2}, \bar{4}\} \subset \mathbb{Z}/6.$$

Vergleichen wir die Gruppentafel

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

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 $\{\bar{0}, \bar{2}, \bar{4}\} \subset \mathbb{Z}/6$ mit $\mathbb{Z}/3$ ist ein Beispiel eines Gruppenisomorphismus, d.h. einer bijektiven Abbildung, die die Gruppenstruktur erhält. Der Gruppenisomorphismus

$$\begin{aligned} \varphi: \quad \mathbb{Z}/3 &\longrightarrow \{\bar{0}, \bar{2}, \bar{4}\} \\ 0 + 3\mathbb{Z} &\longmapsto 0 + 6\mathbb{Z} \\ 1 + 3\mathbb{Z} &\longmapsto 2 + 6\mathbb{Z} \\ 2 + 3\mathbb{Z} &\longmapsto 4 + 6\mathbb{Z} \end{aligned}$$

erfüllt zum Beispiel

$$\varphi(\bar{1} + \bar{1}) = \varphi(\bar{2}) = \bar{4} = \bar{2} + \bar{2} = \varphi(\bar{1}) + \varphi(\bar{1}).$$

Wir schreiben dann

$$\mathbb{Z}/3 \cong \{\bar{0}, \bar{2}, \bar{4}\}$$

und allgemeiner gilt

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

Definition 3.2.11 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 3.2.12 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

$$\text{Ker } \varphi = \{a \in G_1 \mid \varphi(a) = e_2\}$$

und das **Bild** von φ

$$\text{Bild } \varphi = \varphi(G_1)$$

sind Untergruppen von G_1 bzw. G_2 .

Für den Beweis der Aussagen siehe Übung 3.4.

Zum Beispiel für den Gruppenhomomorphismus $\varphi : \mathbb{Z}/3 \rightarrow \mathbb{Z}/6$, gegeben durch $\bar{1} \mapsto \bar{2}$ wie oben, erhalten wir

$$\text{Bild } \varphi = \{\bar{0}, \bar{2}, \bar{4}\}$$

$$\text{Ker } \varphi = \{\bar{0}\}.$$

Lemma 3.2.13 *Ein Gruppenhomomorphismus $\varphi : G_1 \rightarrow G_2$ ist injektiv genau dann, wenn*

$$\text{Ker } \varphi = \{e_1\},$$

d.h. der Kern nur das neutrale Element e_1 von G_1 enthält.

Beweis. Wir bemerken zunächst, dass für $b \in G_1$

$$(\varphi(b))^{-1} = \varphi(b^{-1})$$

da

$$\varphi(b) \circ \varphi(b^{-1}) = \varphi(b \circ b^{-1}) = \varphi(e_1) = e_2,$$

und das Inverse eindeutig bestimmt ist. Für $a, b \in G_1$ gilt damit

$$\varphi(a) = \varphi(b) \iff \varphi(a \circ b^{-1}) = e_2 \iff a \circ b^{-1} \in \text{Ker } \varphi.$$

denn

$$\varphi(a) \circ (\varphi(b))^{-1} = \varphi(a) \circ \varphi(b^{-1}) = \varphi(a \circ b^{-1})$$

Ist also $\text{Ker } \varphi = \{e_1\}$, 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 3.2.14 *Injektive Gruppenhomomorphismen nennt man auch (Gruppen-) **Monomorphismen**, surjektive Gruppenhomomorphismen (Gruppen-) **Epimorphismen**.*

*Ein (Gruppen-) **Isomorphismus***

$$\varphi : G_1 \rightarrow G_2$$

ist ein bijektiver Homomorphismus. Die Umkehrabbildung

$$\varphi^{-1} : G_2 \rightarrow G_1$$

ist dann ebenfalls ein Homomorphismus. Wir schreiben auch $G_1 \cong G_2$.

Siehe auch Übung 3.4.

Beispiel 3.2.15 1) Die Inklusion einer Untergruppe $H \hookrightarrow G$ ist ein Monomorphismus.

2) Die Abbildung

$$\begin{aligned} \mathbb{Z} &\longrightarrow n\mathbb{Z} \\ k &\longmapsto n \cdot k \end{aligned}$$

ist für $n \geq 1$ ein Isomorphismus.

3) Die **Exponentialfunktion**

$$\begin{aligned} (\mathbb{R}, +) &\longrightarrow (\mathbb{R}_{>0}, \cdot) \\ x &\longmapsto \exp(x) = e^x \end{aligned}$$

in Abbildung 3.6 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 $\lim_{x \rightarrow \infty} e^x = \infty$ und $\lim_{x \rightarrow -\infty} e^x = 0$, definiert sie sogar einen Isomorphismus.

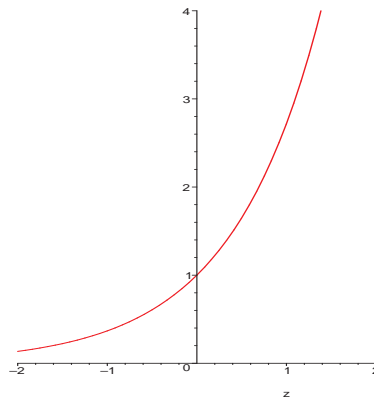


Abbildung 3.6: Exponentialfunktion

4) Im Gegensatz dazu ist mit $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ die Abbildung

$$\begin{aligned} (\mathbb{C}, +) &\longrightarrow (\mathbb{C}^*, \cdot) \\ z &\longmapsto \exp(z) = e^z \end{aligned}$$

zwar ein Epimorphismus, aber kein Isomorphismus. Sie hat den Kern

$$\text{Ker}(\exp : \mathbb{C} \longrightarrow \mathbb{C}^*) = 2\pi i\mathbb{Z} := \{2\pi in \mid n \in \mathbb{Z}\}.$$

5) Sei $n \geq 2$. Die **Signatur** oder das **Signum**

$$\begin{aligned} \text{sign} : S_n &\longrightarrow (\{\pm 1\}, \cdot) \\ \sigma &\longmapsto \text{sign}(\sigma) = \prod_{\substack{i,j=1 \\ i < j}}^n \frac{\sigma(i) - \sigma(j)}{i - j} \end{aligned}$$

ist ein Epimorphismus und

$$\text{Ker}(\text{sign}) = A_n$$

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 $(\sigma(1), \dots, \sigma(n))$ repräsentieren.

Als Beispiel betrachten wir die Permutationen aus Abbildung 3.2. Für die Drehung

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

berechnet man mit obiger Formel, dass

$$\begin{aligned} \text{sign}(\sigma) &= \frac{1-3}{1-2} \cdot \frac{1-4}{1-3} \cdot \frac{1-2}{1-4} \cdot \frac{3-4}{2-3} \cdot \frac{3-2}{2-4} \cdot \frac{4-2}{3-4} \\ &= \frac{3-2}{2-3} \cdot \frac{4-2}{2-4} = (-1)^2 = 1 \end{aligned}$$

und für die beiden Spiegelungen

$$\tau_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} \quad \tau_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$$

dass $\text{sign}(\tau_i) = -1$. Tatsächlich gilt für jede Transposition τ , dass $\text{sign}(\tau) = -1$. Dies beweisen wir in Kürze.

Da sign ein Gruppenhomomorphismus ist, folgt aus $\sigma = \tau_1 \cdot \tau_2$ direkt

$$\text{sign}(\sigma) = \text{sign}(\tau_1) \cdot \text{sign}(\tau_2) = 1.$$

Wie wir in Satz 3.2.34 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 3.5.

6) Sind $a, b \in \mathbb{N}$ und $\text{ggT}(a, b) = 1$. Dann gilt

$$\mathbb{Z}/ab \cong \mathbb{Z}/a \times \mathbb{Z}/b$$

Dies ist eine Umformulierung des Chinesischen Restsatzes. Zum Beweis siehe Übung 3.8.

Praktisch werden Gruppen oft durch Erzeuger gegeben:

Definition 3.2.16 Sei E eine Teilmenge einer Gruppe G . Dann ist $\langle E \rangle$ die kleinste Untergruppe von G , die 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

$$g^r = \underbrace{g \circ \dots \circ g}_r$$

$g^r = (g^{-1})^{-r}$ für $r < 0$. Bei einer additiven Verknüpfung $+$ schreiben wir intuitiver $r \cdot g$ statt g^r .

Beispiel 3.2.17 1) Die Restklassengruppe \mathbb{Z}/n wird zyklisch von $\bar{1}$ 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 $n\mathbb{Z} = \langle n \rangle$. Nach Beispiel 3.2.15 gilt $n\mathbb{Z} \cong \mathbb{Z}$.

Wir werden später zeigen, dass alle zyklischen Gruppen bis auf Isomorphie von der Form \mathbb{Z} oder \mathbb{Z}/n sind (siehe Beispiel 3.3.13).

Definition 3.2.18 Sei $g \in G$ ein Element einer Gruppe. Dann heißt

$$\text{ord}(g) = |\langle g \rangle|$$

die **Ordnung** von g .

Siehe auch Übungsaufgabe 3.9.

Beispiel 3.2.19 Für die Drehung des Tetraeders um 120°

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

erhalten wir

$$\langle \sigma \rangle = \{\text{id} = \sigma^0, \sigma^1, \sigma^2\} \cong \mathbb{Z}/3$$

und somit $\text{ord}(\sigma) = 3$.

3.2.2 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 3.2.20 Sei (G, \circ) eine Gruppe und M eine Menge. Eine **Operation** von G auf M (von links) ist eine Abbildung

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

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 3.2.21 Analog kann man auch Operationen von rechts

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

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 $H \times G \rightarrow G$, $(h, g) \mapsto h \circ g$ von links und $G \times H \rightarrow G$, $(g, h) \mapsto g \circ h$ von rechts, auf die wir später noch ausführlich zurückkommen.

Bemerkung 3.2.22 Anders formuliert ist eine Operation von G auf M ein Gruppenhomomorphismus

$$\begin{aligned} \varphi : G &\longrightarrow S(M) \\ g &\longmapsto \varphi(g) := \begin{pmatrix} M &\longrightarrow & M \\ m &\longmapsto & g \cdot m \end{pmatrix} \end{aligned}$$

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

$$\begin{aligned} m_1 &= e \cdot m_1 = (g^{-1} \circ g) \cdot m_1 = g^{-1} \cdot (g \cdot m_1) \\ &= g^{-1} \cdot (g \cdot m_2) = (g^{-1} \circ g) \cdot m_2 = e \cdot m_2 = m_2. \end{aligned}$$

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 3.2.23 S_n operiert auf $\{1, \dots, n\}$ durch

$$\begin{array}{ccc} S_n \times \{1, \dots, n\} & \longrightarrow & \{1, \dots, n\} \\ (\sigma, j) & \longmapsto & \sigma(j) \end{array}$$

Ein anderes zentrales Beispiel ist die Operation der Gruppe der Bewegungen auf dem \mathbb{R}^n :

Definition 3.2.24 Eine Euklidische **Bewegung** $f: \mathbb{R}^n \rightarrow \mathbb{R}^n$ ist eine Abbildung, die den Euklidischen Abstand

$$\|x\| := \sqrt{\sum_{i=1}^n x_i^2}$$

erhält, d.h. mit

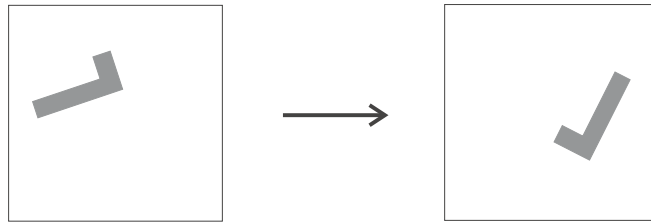
$$\|x - y\| = \|f(x) - f(y)\|$$

für alle $x, y \in \mathbb{R}^n$. Abbildung 3.7 zeigt eine Bewegung, die sich aus einer Translation und einer Drehspiegelung zusammensetzt. Die Menge $E(n)$ der Euklidischen Bewegungen des \mathbb{R}^n ist mit der Komposition eine Gruppe, die **Bewegungsgruppe**.

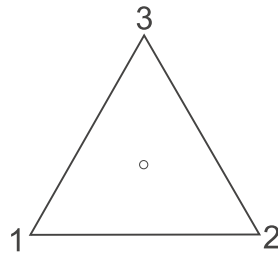
Sei $M \subset \mathbb{R}^n$ eine Teilmenge. Die Gruppe

$$\text{Sym}(M) = \{A \in E(n) \mid A(M) = M\}$$

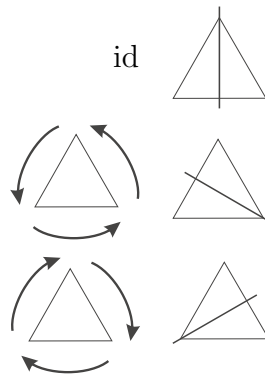
heißt **Symmetriegruppe** von M .

Abbildung 3.7: Beispiel einer Bewegung des \mathbb{R}^2 .

Beispiel 3.2.25 (Symmetriegruppe) Wir beschreiben die Symmetriegruppe $\text{Sym}(D)$ des gleichseitigen Dreiecks D .

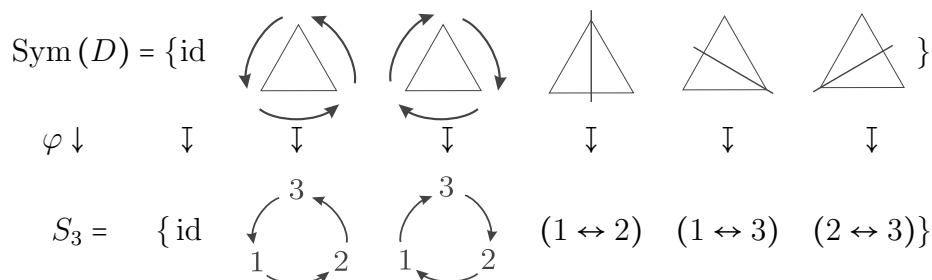


Jede Symmetrie ist eine Drehung oder Spiegelung



Jede Symmetrie ist eindeutig durch ihre Wirkung auf den Ecken festgelegt. Durch Nummerieren der Ecken können wir also jedes Element als eine bijektive Abbildung $\{1, 2, 3\} \rightarrow \{1, 2, 3\}$ auffas-

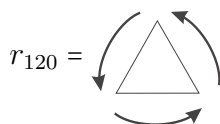
sen. Genauer haben wir einen Gruppenisomorphismus φ



Dieser wird induziert durch die Operation von $\text{Sym}(D)$ auf den Ecken des Dreiecks

$$\text{Sym}(D) \times \{1, 2, 3\} \longrightarrow \{1, 2, 3\}.$$

Bezeichnet etwa



die Drehung um 120° , dann gibt die Operation die Zuordnung

$$(r_{120}, 1) \mapsto 2, (r_{120}, 2) \mapsto 3, (r_{120}, 3) \mapsto 1$$

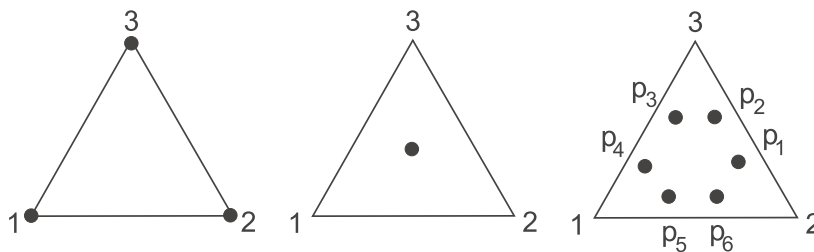
also

$$\varphi(r_{120}) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Beispiel 3.2.26 (Bahn und Stabilisator) Gegeben ein Punkt des gleichseitigen Dreiecks D , wollen wir untersuchen, auf welche anderen Punkte dieser unter der Operation

$$\text{Sym}(D) \times D \longrightarrow D$$

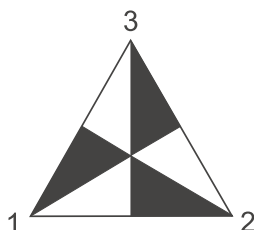
abgebildet werden kann. Diese Menge nennt man die Bahn, die Anzahl der Elemente die Länge der Bahn. Beispiele von Bahnen sind



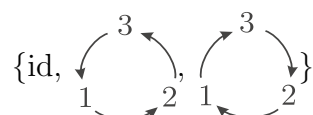
Die Operation auf D induziert eine Operation

$$\text{Sym}(D) \times 2^D \longrightarrow 2^D$$

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 $\text{Sym}(D)$ betrachten, die einen gegebenen Punkt (oder eine Teilmenge) festhalten. Die Ecke 1 wird festgehalten von $\{\text{id}, (2 \leftrightarrow 3)\}$, der Mittelpunkt m von $\text{Sym}(D)$ und der Punkt p_1 nur von der Identität. Die schwarze Teilmenge wird festgehalten von



Wir beobachten, dass diese Mengen stets Untergruppen von $\text{Sym}(D)$ sind, und das Produkt der Gruppenordnung mit der Länge der jeweiligen Bahn stets $|\text{Sym}(D)| = 6$ ergibt

	Bahn	festgehalten von	
1	$\{1, 2, 3\}$	$\{\text{id}, (2 \leftrightarrow 3)\}$	$3 \cdot 2 = 6$
m	$\{m\}$	$\text{Sym}(D)$	$1 \cdot 6 = 6$
p_1	$\{p_1, \dots, p_6\}$	$\{\text{id}\}$	$6 \cdot 1 = 6$

Dies werden wir in Abschnitt 3.2.4 zeigen.

Zunächst formalisieren wir aber diese Ideen:

Definition 3.2.27 Sei $G \times M \rightarrow M$ eine Operation. Für $m \in M$ nennt man

$$Gm = \{gm \mid g \in G\} \subset M$$

die **Bahn** (oder den **Orbit**) von m . Ist $N \subset M$ eine Teilmenge, dann heißt

$$\text{Stab}(N) = \{g \in G \mid gN = N\}$$

der **Stabilisator** der Menge N . Für ein Element $m \in M$ sei

$$\text{Stab}(m) = \{g \in G \mid gm = m\} = \text{Stab}(\{m\}).$$

Bemerkung 3.2.28 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

$$m_3 = g_1m_1 = g_2m_2$$

also

$$m_2 = g_2^{-1}g_1m_1.$$

Damit ist $m_2 \in Gm_1$, und somit $Gm_2 \subset Gm_1$, ebenso gilt die andere Inklusion, also $Gm_2 = Gm_1$. ■

Definition 3.2.29 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

$$\begin{aligned} \pi: M &\longrightarrow M/G \\ m &\longmapsto Gm \end{aligned}$$

Quotientenabbildung.

Mit obigen Bemerkungen sieht man:

Definition und Satz 3.2.30 Sei $G \times M \rightarrow M$ 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

$$M = \dot{\bigcup}_{r \in R} G \cdot r$$

Definition 3.2.31 Ist $\sigma \in S_n$, dann zerlegt die Operation von $\langle \sigma \rangle$ die Menge $\{1, \dots, n\}$ in Bahnen der Form

$$\langle \sigma \rangle x = \{x, \sigma(x), \sigma^2(x), \dots, \sigma^{t-1}(x)\}$$

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

$$\sigma = (x, \sigma(x), \sigma^2(x), \dots, \sigma^{t-1}(x)).$$

Transpositionen sind Zyklen der Länge 2. Für das neutrale Element schreiben wir $()$.

Bemerkung 3.2.32 Der Zykel

$$\sigma = (a_1, \dots, a_t) \in S_n$$

ist also die Abbildung

$$\begin{aligned} \{1, \dots, n\} &\longrightarrow \{1, \dots, n\} \\ a_1 &\longmapsto a_2 \\ a_2 &\longmapsto a_3 \\ &\vdots \\ a_{t-1} &\longmapsto a_t \\ a_t &\longmapsto a_1 \\ a &\longmapsto a \quad \text{sonst.} \end{aligned}$$

Es gilt $\text{ord}(\sigma) = t$.

Beispiel 3.2.33 Für die Drehung

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

des Tetraeders um 120° (siehe auch [Beispiel 3.2.19](#)) 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. $2 \mapsto 3, 3 \mapsto 4, 4 \mapsto 2$.

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

$$\sigma^2 = (2, 4, 3).$$

Satz 3.2.34 *Es gilt:*

- 1) Jedes Element der S_n ist ein Produkt elementfremder Zykkel.
- 2) Jedes Element der S_n ist ein Produkt von Transpositionen.

Beweis. Sei $\sigma \in S_n$.

- 1) Sei $\{x_1, \dots, x_r\}$ ein vollständiges Repräsentantensystem der Bahnen der Operation von $\langle \sigma \rangle$ auf $\{1, \dots, n\}$. Schränken wir σ als Abbildung auf die Bahn $\langle \sigma \rangle x_i$ ein, erhalten wir einen Zykel σ_i und

$$\sigma = \sigma_1 \cdot \dots \cdot \sigma_r$$

- 2) Mit 1) können wir annehmen, dass σ ein Zykel (y_0, \dots, y_{t-1}) ist. Dann gilt

$$(y_0, \dots, y_{t-1}) = (y_0, y_1) \cdot \dots \cdot (y_{t-2}, y_{t-1}).$$

■

Beispiel 3.2.35 *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

$$\{1, \dots, 9\} = \{1, 2, 3, 4\} \dot{\cup} \{5, 9\} \dot{\cup} \{6, 8\} \dot{\cup} \{7\}$$

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 3.7.

Bemerkung 3.2.36 Ist $\sigma = \tau_1 \cdot \dots \cdot \tau_r$ mit Transpositionen τ_i , dann können wir das Signum von σ sofort berechnen als

$$\text{sign}(\sigma) = (-1)^r,$$

denn sign ist ein Gruppenhomomorphismus und $\text{sign} \tau = -1$ für jede Transposition τ .

Beweis. Angenommen $\tau = (k, l)$ und $k < l$. Dann ist

$$\frac{\tau(i) - \tau(j)}{i - j} = \begin{cases} -1 & \text{für } i = k \text{ und } j = l \\ 1 & \text{für } i, j \notin \{k, l\} \\ \frac{l-j}{k-j} & \text{für } i = k \text{ und } j \neq l \\ \frac{i-k}{i-l} & \text{für } i \neq k \text{ und } j = l \end{cases}$$

also

$$\text{sign}(\tau) = - \underbrace{\prod_{\substack{j \text{ mit} \\ l < j}} \frac{l-j}{k-j}}_{>0} \cdot \underbrace{\prod_{\substack{j \text{ mit} \\ k < j < l}} \frac{l-j}{k-j}}_1 \cdot \underbrace{\prod_{\substack{i \text{ mit} \\ k < i < l}} \frac{i-k}{i-l}}_1 \cdot \underbrace{\prod_{\substack{i \text{ mit} \\ i < k}} \frac{i-k}{i-l}}_{>0}$$

denn die beiden mittleren Summen kürzen sich weg, und alle Zähler und Nenner des ersten und letzten Produktes sind negativ. Somit ist $\text{sign} \tau < 0$ also $\text{sign} \tau = -1$. ■

Beispiel 3.2.37 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

$$\text{sign}(\sigma) = (-1)^5 = -1.$$

Bemerkung 3.2.38 Aus der Darstellung einer Permutation $\sigma = c_1 \circ \dots \circ c_r$ als Produkt disjunkter Zyklen c_i der Länge m_i lässt sich die Ordnung von σ bestimmen als

$$\text{ord}(\sigma) = \text{kgV}(m_1, \dots, m_r).$$

Für den Beweis siehe Übungsaufgabe 3.9.

Beispiel 3.2.39 Für $\sigma = (1, 4, 3, 2)(5, 9)(6, 8)$ erhalten wir

$$\text{ord}(\sigma) = \text{kgV}(4, 2, 2) = 4.$$

Wir können dies auch direkt nachrechnen

$$\sigma^2 = (1, 4, 3, 2)^2(5, 9)^2(6, 8)^2 = (1, 3)(2, 4)$$

$$\sigma^3 = (1, 2, 3, 4)(5, 9)(6, 8)$$

$$\sigma^4 = \text{id}.$$

Für Untergruppen der S_n implementiert das Computeralgebrasystem GAP, siehe [12], Algorithmen zur Berechnung im Wesentlichen aller in diesem Kapitel eingeführten Objekte.

Beispiel 3.2.40 Wir bestimmen $\text{ord}(\sigma)$ 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 $\text{ord}(\sigma) = 4$. Dies berechnet GAP auch (mittels Bemerkung 3.2.38) 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 3.2.41 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

$$S_n = \langle (1, 2), (2, 3), \dots, (n-1, n) \rangle,$$

siehe auch die Übungsaufgaben 3.21 und 3.22.

Beispiel 3.2.42 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)]
```

3.2.3 Operation durch Translation

Bisher haben wir als Gruppenoperationen die Operation von $\text{Sym}(M)$ auf einer Menge M und von S_n auf $\{1, \dots, n\}$ 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 3.2.43 (Cayley) *Jede Gruppe G ist isomorph zu einer Untergruppe der Gruppe der Selbstabbildungen $S(G)$.*

Inbesondere für $n := |G| < \infty$ können wir G als Untergruppe von $S_n \cong S(G)$ auffassen.

Beweis. Die Abbildung

$$\begin{aligned} \varphi: G &\rightarrow S(G) \\ g &\mapsto \left(\begin{array}{l} G \rightarrow G \\ h \mapsto gh \end{array} \right) \end{aligned}$$

ist ein Gruppenhomomorphismus und

$$\text{Ker } \varphi = \{g \in G \mid gh = h \ \forall h \in G\} = \{e\}$$

(mit der Eindeutigkeit des neutralen Elements) also φ injektiv. Somit gilt

$$G \cong \text{Bild}(\varphi) \subset S(G).$$

■

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, der **Verknüpfungstafel**.

Beispiel 3.2.44 *Die Gruppe*

$$G = \mathbb{Z}/4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$$

hat die Verknüpfungstafel

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

In jeder Zeile und Spalte steht jedes Element genau einmal. Die Zeilen der Verknüpfungstafel spezifizieren $\varphi(g)$, in dem Beispiel ist etwa

$$\varphi(\bar{1}) = \begin{pmatrix} \bar{0} & \bar{1} & \bar{2} & \bar{3} \\ \bar{1} & \bar{2} & \bar{3} & \bar{0} \end{pmatrix} \in S(G) \cong S_4.$$

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 3.2.45 Wie in Beispiel 3.2.7 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

$$\begin{aligned} \mathbb{Z} \times n\mathbb{Z} &\rightarrow \mathbb{Z} \\ (a, n \cdot k) &\mapsto a + n \cdot k \end{aligned}$$

Die Bahnen sind genau die Restklassen modulo n

$$\bar{a} = a + n\mathbb{Z} = \{a + n \cdot k \mid k \in \mathbb{Z}\}.$$

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.

Wir haben in Beispiel 3.2.8 schon gesehen, dass die Menge dieser Bahnen mit der Addition

$$\bar{a} + \bar{b} = (a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a + b) + n\mathbb{Z} = \overline{a + b}$$

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 3.2.46 (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

$$G \times H \longrightarrow G, (h, g) \longmapsto g \circ h.$$

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 .

Satz 3.2.47 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

$$\begin{array}{ccc} g & \longmapsto & ba^{-1}g \\ G & \xrightarrow{1:1} & G \\ \cup & & \cup \\ aH & \longrightarrow & bH \\ ah & \longmapsto & ba^{-1}ah = bh \end{array}$$

(was ist die Umkehrabbildung?). Die rechten und linken Nebenklassen aH und Ha stehen in Bijektion vermöge **Konjugation** mit a

$$\begin{array}{ccc} g & \longmapsto & a^{-1}ga \\ G & \xrightarrow{1:1} & G \\ \cup & & \cup \\ aH & \longrightarrow & Ha \\ ah & \longmapsto & a^{-1}aha = ha \end{array}$$

(was ist die Umkehrabbildung?). Die Operation durch Konjugation diskutieren wir auch in Aufgabe 3.12. ■

Corollar 3.2.48 (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 3.2.49 Ist $H \subset G$ eine Untergruppe, so heißt

$$[G : H] := |G/H|$$

Index von H in G .

Wir bemerken zunächst, dass

$$\begin{aligned} H &\rightarrow aH \\ h &\mapsto ah \end{aligned}$$

eine Bijektion ist (siehe den Beweis von Satz 3.2.47), also

$$|aH| = |H|.$$

Wir beweisen nun die Indexformel:

Beweis. Nach Definition und Satz 3.2.30 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 3.2.47). Ist $|G| = \infty$, dann auch $|G/H| = \infty$ oder $|H| = \infty$. ■

Beispiel 3.2.50 Die Gruppe $G = \mathbb{Z}/6$ der Ordnung 6 hat die Untergruppen

$$\begin{array}{ccc} & \{0, \dots, 5\} & \\ & / \quad \backslash & \\ \{0, \bar{2}, \bar{4}\} & & \{0, \bar{3}\} \\ & \backslash \quad / & \\ & \{0\} & \end{array}$$

mit den Ordnungen 1, 2, 3 und 6.

Bemerkung 3.2.51 *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 3.2.48) erhalten wir mit $H = \langle g \rangle$:

Corollar 3.2.52 *In einer endlichen Gruppe G ist die Ordnung eines Elements $g \in G$ ein Teiler der Gruppenordnung $|G|$, d.h. $\text{ord}(g) \mid |G|$.*

Corollar 3.2.53 *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

$$\{e\} \neq \langle g \rangle = G$$

■

3.2.4 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 3.2.54 *Sei*

$$G \times M \longrightarrow M$$

eine Operation, $m \in M$ und

$$H := \text{Stab}(m).$$

Dann gibt es eine natürliche Bijektion

$$\begin{aligned} G/H &\longrightarrow Gm \\ gH &\longmapsto gm \end{aligned}$$

Beweis. Die Abbildung ist wohldefiniert: Ist $gH = g'H$, dann $g' \in gH$, also $g' = gh$ mit $h \in H$. Es folgt

$$g'm = ghm = gm,$$

da m von h stabilisiert wird. Die Abbildung ist offenbar surjektiv. Sie ist auch injektiv, denn

$$\begin{aligned} g_1m = g_2m &\Rightarrow g_1^{-1}g_2 \in H \Rightarrow \\ g_2 = g_1g_1^{-1}g_2 &\in g_1H \Rightarrow g_1H = g_2H. \end{aligned}$$

■

Corollar 3.2.55 (Bahnformel) Sei $G \times M \rightarrow M$ eine Operation und $m \in M$. Dann gilt

$$|Gm| \cdot |\text{Stab}(m)| = |G|.$$

Beweis. Es ist

$$|Gm| = |G/H|$$

mit Satz 3.2.54 und

$$|G/H| \cdot |H| = |G|$$

nach der Indexformel 3.2.48. ■

Beispiel 3.2.56 (Symmetriegruppe des Tetraeders) Sei T ein regulärer Tetraeder mit den Ecken $1, \dots, 4$ wie in Abbildung 3.8. Die Symmetrien von T sind durch ihre Wirkung auf den Ecken eindeutig bestimmt. Wir können also die Symmetriegruppe $\text{Sym}(T)$ 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 3.9 eingezeichneten Ebene entspricht $(2, 3)$. Da die S_4 von den Transpositionen erzeugt wird, folgt:

$$\text{Sym}(T) \cong S_4.$$

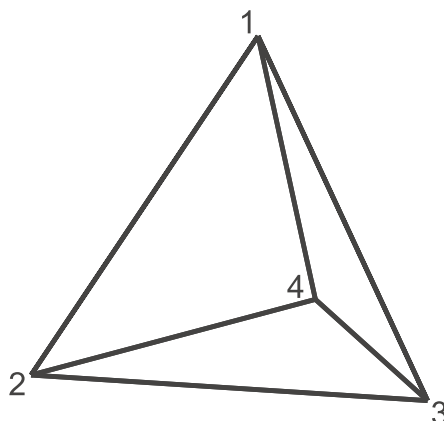


Abbildung 3.8: Tetraeder

Beispiel 3.2.57 (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 3.10 markiert sind:

Bahnen Gm	$ Gm $	Stabilisatoren $\text{Stab}(m)$	$ \text{Stab}(m) $
$G1 = \{1, 2, 3, 4\}$	4	S_3	6
Gm_{12} $= \{m_{12}, \dots, m_{34}\}$	6	$\text{Stab}(m_{12})$ $= \{e, (12), (34), (12)(34)\}$ $\cong \mathbb{Z}_2 \times \mathbb{Z}_2$	4
Gp	24	$\text{Stab}(p) = \{e\}$	1
$G0 = \{0\}$	1	$\text{Stab}(0) = S_4$	24

Wir bemerken, dass stets $|Gm| \cdot |\text{Stab}(m)| = |G|$.

Bemerkung 3.2.58 Umgekehrt kann man die Ordnung der Symmetriegruppe bestimmen mittels der Formel

$$|G| = |Gm| \cdot |\text{Stab}(m)|$$

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 3.10 wählen.

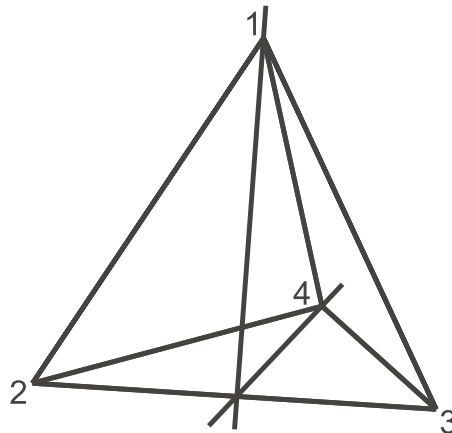


Abbildung 3.9: Spiegelsymmetrie (2, 3) des Tetraeders

Satz 3.2.59 (Bahnengleichung) Sei $R \subset M$ ein vollständiges Repräsentantensystem der Bahnen einer Operation $G \times M \rightarrow M$. Dann gilt

$$|M| = \sum_{r \in R} \frac{|G|}{|\text{Stab}(r)|}$$

Beweis. M ist nach Definition und Satz 3.2.30 die disjunkte Vereinigung

$$M = \bigcup_{r \in R} G \cdot r$$

also

$$|M| = \sum_{r \in R} |G \cdot r| = \sum_{r \in R} \frac{|G|}{|\text{Stab}(r)|}.$$

■

Beispiel 3.2.60 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

$$G = \langle \sigma \rangle = \{\text{id}, \sigma, \sigma^2, \dots, \sigma^{11}\}$$

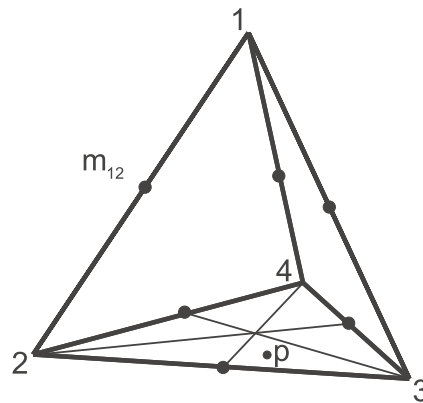


Abbildung 3.10: Bahnen von Punkten des Tetraeders

der Ordnung $12 = \text{kgV}(4, 3, 2)$ (siehe Aufgabe 3.9 zur Berechnung der Ordnung). Die Operation von $\langle \sigma \rangle$ zerlegt

$$\{1, \dots, 10\} = \{1, 2, 3, 4\} \dot{\cup} \{5, 8, 9\} \dot{\cup} \{6, 7\} \dot{\cup} \{10\}$$

in Bahnen. Also gilt die Bahngleichung

$$\begin{aligned} 10 &= 4 + 3 + 2 + 1 \\ &= \frac{12}{3} + \frac{12}{4} + \frac{12}{6} + \frac{12}{12} \end{aligned}$$

mit

$$\begin{aligned} \text{Stab}(1) &= \{\text{id}, \sigma^4, \sigma^8\} \\ \text{Stab}(5) &= \{\text{id}, \sigma^3, \sigma^6, \sigma^9\} \\ \text{Stab}(6) &= \{\text{id}, \sigma^2, \sigma^4, \sigma^6, \sigma^8, \sigma^{10}\} \\ \text{Stab}(10) &= \{\text{id}, \sigma^1, \sigma^2, \dots, \sigma^{11}\} = G, \end{aligned}$$

wobei wir das vollständige Repräsentantensystem $R = \{1, 5, 6, 10\}$ gewählt haben.

Eine weitere Anwendung ist die Klassifikation von Graphen bis auf Isomorphie:

3.2.5 Anwendung: Aufzählen von Graphen

Definition 3.2.61 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 3.2.62 Durch $V = \{1, 2, 3\}$ und $E = \{\{1, 2\}, \{2, 3\}\}$ ist der Graph $\Gamma = (V, E)$ in Abbildung 3.11 gegeben.

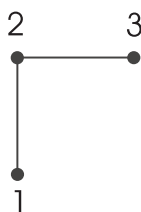


Abbildung 3.11: Graph

Bemerkung 3.2.63 Es gibt offenbar genau $2^{\binom{n}{2}}$ Graphen auf n Vertices (Übung).

Beispiel 3.2.64 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 3.12 zeigt die Nachbarschaftsverhältnisse von Rheinland-Pfalz und seinen Nachbarn.

Oft will man Graphen, die durch Ummummerieren der Vertices auseinander hervorgehen, gleich behandeln:

Definition 3.2.65 Zwei Graphen (V_1, E_1) und (V_2, E_2) heißen **isomorph**, wenn eine bijektive Abbildung $\varphi : V_1 \rightarrow V_2$ existiert, sodass

$$\{v, w\} \in E_1 \iff \{\varphi(v), \varphi(w)\} \in E_2$$

für alle $v, w \in V_1$.

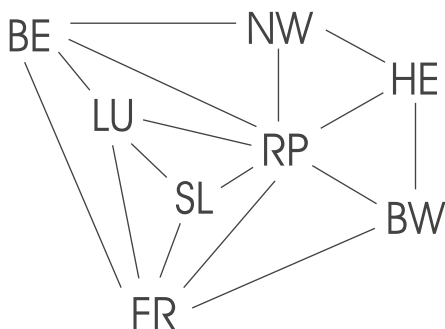


Abbildung 3.12: Nachbarschaftsverhältnisse

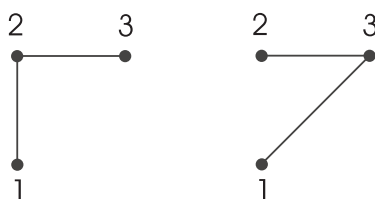
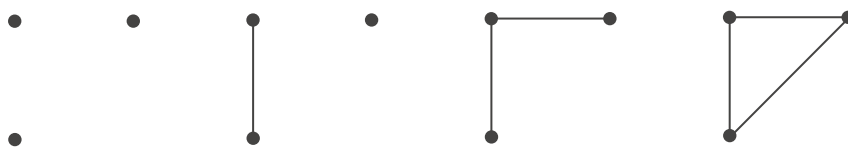


Abbildung 3.13: Isomorphe Graphen

Beispiel 3.2.66 Die beiden Graphen in Abbildung 3.13 sind isomorph durch $\varphi = (2, 3) \in S_3$.

Satz 3.2.67 Es gibt genau 4 Isomorphieklassen von Graphen mit 3 Ecken.

Beweis. Die Graphen




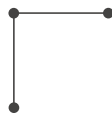
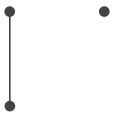
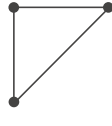
sind offenbar paarweise nicht isomorph. Wir zeigen, dass sie ein vollständiges Repräsentantensystem der Graphen mit 3 Vertices bilden: Sei

$$V = \{1, 2, 3\}$$

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 Isomphietyp des Stabilisators und mit Hilfe der Bahnenformel die Länge der Bahn an:

	m	$\text{Stab}(m)$	$ Gm $		r	$\text{Stab}(m)$	$ Gm $
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 [3.15](#).

3.3 Normalteiler

3.3.1 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 $G \times H \rightarrow G$, $(g, h) \mapsto g \circ h$ von H auf G .

Beispiel 3.3.1 Für $H = n\mathbb{Z} \subset \mathbb{Z} = G$ haben wir schon gesehen, dass die Menge

$$G/H = \mathbb{Z}/n = \{\overline{0}, \dots, \overline{n-1}\}$$

der Nebenklassen

$$\bar{a} = a + n\mathbb{Z}$$

mit der von der Addition in \mathbb{Z} induzierten Verknüpfung

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

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 3.3.2 Wir betrachten nochmals die entsprechende Rechnung für \mathbb{Z}/n : Sei $\bar{a}_1 = \bar{a}_2$ und $\bar{b}_1 = \bar{b}_2$, 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 $H = \text{Ker}(\pi)$. Für den Kern eines Gruppenhomomorphismus beobachten wir allgemein:

Bemerkung 3.3.3 Sei

$$\varphi : G \longrightarrow F$$

ein Gruppenhomomorphismus und

$$H = \text{Ker}(\varphi) \subset G.$$

Dann gilt für $g \in G$ und

$$gHg^{-1} := \{ghg^{-1} \mid h \in H\},$$

dass

$$gHg^{-1} = H.$$

Beweis. Ist $h \in \text{Ker} \varphi$, dann gilt für jedes $g \in G$

$$\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1} = \varphi(g)\varphi(g)^{-1} = e,$$

also $ghg^{-1} \in H$ 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 3.3.4 Sei $H \subset G$ eine Untergruppe. H heißt **Normalteiler** von G (in Zeichen $H \triangleleft G$), 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 3.3.5 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 3.17.

Satz 3.3.6 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

$$a_2 \in a_1H \quad b_2 \in b_1H$$

müssen wir zeigen, dass

$$(a_2 \circ b_2)H = (a_1 \circ b_1)H.$$

Schreibe

$$a_2 = a_1 \circ h \quad b_2 = b_1 \circ h'$$

mit $h, h' \in H$. Da H ein Normalteiler ist, gilt

$$Hb = bH,$$

also existiert ein $h'' \in H$ mit

$$h \circ b = b \circ h''$$

und damit

$$(a_2 \circ b_2)H = (a_1 \circ h \circ b_1 \circ h')H = (a_1 \circ b_1 \circ h'' \circ h')H = (a \circ b)H.$$

Man beachte, dass $hH = H$ für alle $h \in H$, da Multiplikation mit h eine bijektive Abbildung $H \rightarrow H$ 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 3.3.7 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

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/n = \{\bar{0}, \dots, \overline{n-1}\}.$$

Das neutrale Element ist $\bar{0} = 0 + n\mathbb{Z} = n\mathbb{Z}$ und das Inverse $-\bar{a} = \overline{-a} = \overline{n-a}$.

Beispiel 3.3.8 $A_n = \ker(\text{sign}) \subset S_n$ ist nach Bemerkung 3.3.3 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 3.3.9 Jede Untergruppe $U \subset G$ vom Index $\frac{|G|}{|U|} = [G : U] = 2$ ist ein Normalteiler von G .

Den kurzen Beweis geben wir in Übungsaufgabe 3.16. Siehe auch Übungsaufgabe 3.13.

3.3.2 Homomorphiesatz

Ist $\varphi : G \rightarrow F$ 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 3.3.10 (Homomorphiesatz) *Sei $\varphi : G \rightarrow F$ ein Gruppenhomomorphismus. Dann gilt*

$$G / \text{Ker } \varphi \cong \text{Bild}(\varphi).$$

Beweis. Wir definieren

$$\begin{aligned} \tilde{\varphi} : G / \text{Ker } \varphi &\rightarrow \text{Bild } \varphi \\ \tilde{\varphi}(a \text{Ker } \varphi) &:= \varphi(a) \end{aligned}$$

Dies ist wohldefiniert, da

$$\begin{aligned} a' &= ah \in a \text{Ker } \varphi \text{ mit } h \in \text{Ker } \varphi \\ \Rightarrow \varphi(a') &= \varphi(a) \cdot \varphi(h) = \varphi(a) \cdot e = \varphi(a). \end{aligned}$$

Mit φ ist auch $\tilde{\varphi}$ ein Homomorphismus, surjektiv auf das Bild von φ , und injektiv, denn

$$\begin{aligned} \tilde{\varphi}(a \text{Ker } \varphi) &= e \\ \Rightarrow \varphi(a) &= e \Rightarrow a \in \text{Ker } \varphi \\ \Rightarrow a \text{Ker } \varphi &= \text{Ker } \varphi = e_{G/\text{Ker } \varphi}. \end{aligned}$$

■

Also faktorisiert $\varphi : G \rightarrow F$ in

$$\begin{array}{ccccc} & G & \xrightarrow{\varphi} & F & \\ \text{Projektion} & \downarrow & & \uparrow & \text{Inklusion} \\ & G / \text{Ker } \varphi & \cong & \text{Bild } \varphi & \end{array}$$

Beispiel 3.3.11 *Sei $n \geq 2$. Angewendet auf $\text{sign} : S_n \rightarrow (\{-1, 1\}, \cdot)$ mit Kern A_n und $\text{Bild}(\text{sign}) = \{-1, 1\} \cong \mathbb{Z}/2$ gibt Satz 3.3.10, dass*

$$S_n / A_n \cong \mathbb{Z}/2.$$

Beispiel 3.3.12 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 3.18, 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 3.3.13 (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

$$\begin{aligned} \varphi: (\mathbb{Z}, +) &\longrightarrow \langle g \rangle = G \\ k &\longmapsto g^k \end{aligned}$$

ein Epimorphismus. Die Ordnung $\text{ord}(g) = |G|$ kann endlich oder unendlich sein. Im Fall $\text{ord}(g)$ unendlich ist φ ein Isomorphismus, denn nur $g^0 = e$. Anderenfalls ist $\text{Ker } \varphi = \langle n \rangle = n\mathbb{Z}$ (da jede

Untergruppe von \mathbb{Z} von der Form $n\mathbb{Z}$ ist) und der Homomorphiesatz gibt

$$\begin{aligned}\mathbb{Z}/n\mathbb{Z} &\cong \langle g \rangle \\ \bar{k} &\mapsto g^k\end{aligned}$$

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} .

3.4 Übungsaufgaben

Übung 3.1 Basteln Sie Papiermodelle der Platonischen Körper Tetraeder, Würfel, Oktaeder, Dodekaeder und Ikosaeder (siehe Abbildung 3.1).

Übung 3.2 Sei G eine Menge zusammen mit einer Verknüpfung

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

die folgende Axiome erfüllt:

(G1) Assoziativität

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

(G2') Es existiert ein linksneutrales Element, d.h. ein

$$e \in G$$

mit

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

(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 $a \in G$.
- 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 3.3 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

$$(a_1, \dots, a_n) + (b_1, \dots, b_n) = (a_1 + b_1, \dots, a_n + b_n).$$

Übung 3.4 Sei $\varphi : G_1 \rightarrow G_2$ ein Gruppenhomomorphismus. Zeigen Sie:

- 1) $\text{Ker}(\varphi) \subset G_1$ und $\text{Bild}(\varphi) \subset G_2$ von φ sind Untergruppen.
- 2) Ist φ ein Isomorphismus, dann ist auch die Umkehrabbildung

$$\varphi^{-1} : G_2 \rightarrow G_1$$

ein Gruppenisomorphismus.

Übung 3.5 Zeigen Sie, dass

$$\begin{aligned} \text{sign} : S_n &\longrightarrow (\{\pm 1\}, \cdot) \\ \sigma &\longmapsto \text{sign}(\sigma) = \prod_{\substack{i, j=1 \\ i < j}}^n \frac{\sigma(i) - \sigma(j)}{i - j} \end{aligned}$$

ein Gruppenepimorphismus ist.

Übung 3.6 Lässt sich bei dem bekannten Schiebepiel 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 3.7 Schreiben Sie

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 4 & 2 & 6 & 5 & 7 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 1 & 4 & 5 & 7 & 6 \end{pmatrix},$$

$\sigma \circ \tau$ und $\tau \circ \sigma$ sowohl als Produkt disjunkter Zyklen als auch als Produkt von Transpositionen. Bestimmen Sie jeweils Ordnung und sign.

Übung 3.8 1) Zeigen Sie: Sind $a, b \in \mathbb{Z}$ mit $a, b \geq 1$ und $\text{ggT}(a, b) = 1$. Dann gilt

$$\mathbb{Z}/(a \cdot b) \cong \mathbb{Z}/a \times \mathbb{Z}/b.$$

2) Bestimmen Sie das Urbild von $(2 + 6\mathbb{Z}, -7 + 35\mathbb{Z})$ unter dem Gruppenisomorphismus

$$\mathbb{Z}/210 \cong \mathbb{Z}/6 \times \mathbb{Z}/35.$$

Übung 3.9 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:

$$\text{ord}(x \cdot y) = \text{kgV}(\text{ord}(x), \text{ord}(y)).$$

2) Sei

$$\sigma = c_1 \cdot \dots \cdot c_r \in S_n$$

Produkt disjunkter Zyklen c_i der Längen m_i . Bestimmen Sie $\text{ord}(\sigma)$.

Übung 3.10 Welche Ordnungen treten bei den Elementen von S_6 auf?

Übung 3.11 1) Schreiben Sie jedes Element der S_4 als Produkt disjunkter Zyklen.

2) Ordnen Sie jedem $\sigma \in S_4$ eine Partition von 4 zu (d.h. eine Summe $4 = p_1 + \dots + p_r$ 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 3.14) auffassen.

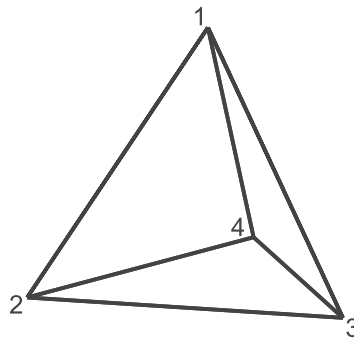


Abbildung 3.14: Tetraeder

Übung 3.12 1) Zeigen Sie: Die Abbildung

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

definiert eine Operation von G auf G von links, die **Konjugation**.

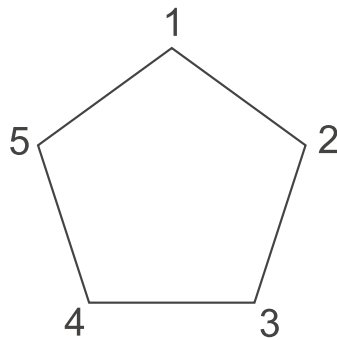


Abbildung 3.15: Regelmäßiges 5-Eck

2) Die Bahn von $b \in G$

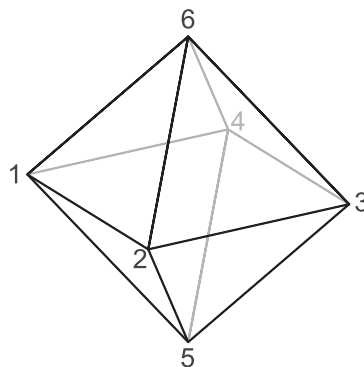
$$b^G := \{aba^{-1} \mid a \in G\}$$

heißt **Konjugationsklasse** von b . Bestimmen Sie alle Konjugationsklassen der S_3 .

Übung 3.13 Sei G die Symmetriegruppe des regelmäßigen 5-Ecks (Abbildung 3.15). 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 3.14 Sei $G = \text{Sym}(O)$ 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 3.15 Zeigen Sie, dass es genau 11 Isomorphieklassen von (ungerichteten) Graphen mit 4 Vertices gibt.

Übung 3.16 Sei H eine Untergruppe von G . Zeigen Sie: Ist $[G : H] = 2$, dann ist H ein Normalteiler in G .

Übung 3.17 Sei $\varphi : G \rightarrow F$ 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 3.18 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

$$S_4/V_4 \cong S_3.$$

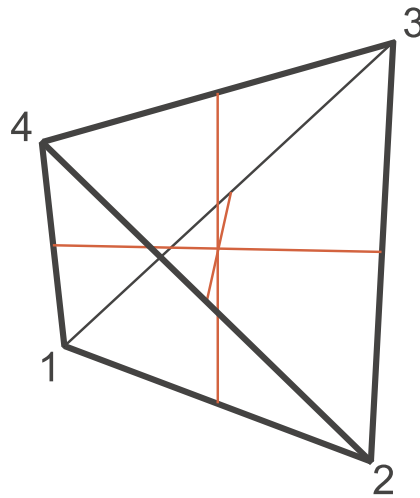


Abbildung 3.16: Tetraeder mit Kantenmittendiagonalen

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 3.16. Dies induziert einen Gruppenhomomorphismus

$$\varphi : S_4 \rightarrow S_3.$$

Übung 3.19 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 3.20 Sei G die Symmetriegruppe des Ikosaeders.

1) Bestimmen Sie die Gruppenordnung von G .

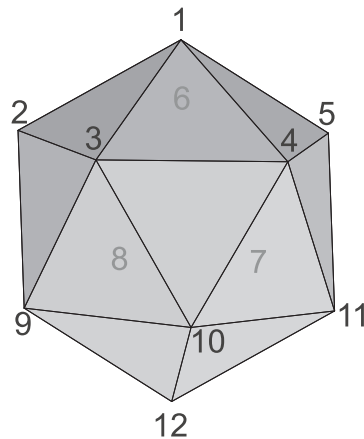


Abbildung 3.17: Ikosaeder mit Nummerierung der Ecken

- 2) Finden Sie Erzeuger der Symmetriegruppe G des Ikosaeders (Abbildung 3.17) als Untergruppe der S_{12} . Beweisen Sie Ihre Behauptung mit Hilfe von GAP.

Übung 3.21 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

$$(n-1, n) \cdot \dots \cdot (k, k+1) \cdot \sigma \in S_{n-1}.$$

- 2) Die symmetrische Gruppe S_n wird erzeugt von den Transpositionen $(1, 2), (2, 3), \dots, (n-1, n)$, d.h.

$$S_n = \langle (1, 2), (2, 3), \dots, (n-1, n) \rangle.$$

Übung 3.22 Sei $G \subset S_n$ eine Untergruppe mit $(1, 2) \in G$ und $(1, 2, \dots, n) \in G$. Zeigen Sie

$$G = S_n.$$

4

Ringe

4.1 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

$$\mathbb{Z}/n = \{\bar{0}, \dots, \overline{n-1}\}$$

ein Ring durch Multiplikation der Repräsentanten

$$\bar{a} \cdot \bar{b} = \overline{a \cdot b}.$$

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 4.1.1 *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*

$$5 + 30 \cdot k \equiv 1 \pmod{7},$$

d.h. $\bar{k} \in \mathbb{Z}/7$ mit

$$\bar{2} \cdot \bar{k} = \bar{3} \in \mathbb{Z}/7.$$

Können wir durch $\bar{2}$ teilen, dann lässt sich \bar{k} berechnen. Tatsächlich besitzt $\bar{2} \in \mathbb{Z}/7$ ein multiplikativ Inverses, denn

$$\bar{4} \cdot \bar{2} = \bar{1}.$$

Somit ist

$$\bar{k} = \bar{2}^{-1} \cdot \bar{3} = \bar{4} \cdot \bar{3} = \bar{12} = \bar{5}.$$

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 $\bar{1}$ immer invertierbar und $\bar{0}$ nie invertierbar. Betrachten wir als Beispiel $\mathbb{Z}/4$. Die Verknüpfungen sind gegeben durch

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	·	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Wir sehen, dass $\bar{3}$ bezüglich \cdot ein Inverses besitzt, denn

$$\bar{3} \cdot \bar{3} = \bar{1}.$$

Dagegen ist $\bar{2}$ nicht invertierbar, da in der Gruppentafel der Multiplikation in der entsprechenden Zeile (oder Spalte) keine $\bar{1}$ 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

$$\begin{array}{c|cc} \cdot & \bar{1} & \bar{3} \\ \hline \bar{1} & \bar{1} & \bar{3} \\ \bar{3} & \bar{3} & \bar{1} \end{array}$$

Viele praktische Anwendungen von Gruppen verwenden $(\mathbb{Z}/n)^\times$, etwa die RSA Public-Key-Kryptographie.

Das Element $\bar{2}$ ist nicht nur keine Einheit, es gilt sogar

$$\bar{2} \cdot \bar{2} = \bar{0}.$$

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. 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, 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 Primfaktorisation 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 Primfaktorisation, 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 Algo- rithmus zur Bestim- mung 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.

4.2 Grundbegriffe

Definition 4.2.1 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.

$$\begin{aligned} a \cdot (b + c) &= a \cdot b + a \cdot c \\ (a + b) \cdot c &= a \cdot c + b \cdot c \end{aligned}$$

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 $\emptyset \neq U \subset R$ 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 4.2.2 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 4.2.3 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 4.2.4 Das Bild von $\varphi(R) \subset S$ ist ein Unterring, ebenso der Kern

$$\text{Ker } \varphi = \{r \in R \mid \varphi(r) = 0\} \subset R.$$

Bemerkung 4.2.5 Für einen Ring R mit 1 ist $\text{Ker } \varphi$ ein Ring mit 1 nur in dem Spezialfall der Nullabbildung, denn

$$1_R \in \text{Ker } \varphi \Leftrightarrow \varphi(1_R) = \varphi(1_R \cdot 1_R) = \varphi(1_R) \cdot \varphi(1_R) = 0 \quad \forall r \in R \Leftrightarrow \text{Ker } \varphi = R.$$

Dies liegt daran, dass $\text{Ker } \varphi$ ein Ideal ist. Darauf werden wir im nächsten Abschnitt über Ideale zurückkommen.

Definition 4.2.6 Sei R ein kommutativer Ring mit 1. Der **Polynomring** $R[x]$ über R in der Unbestimmten x ist die Menge aller Ausdrücke

$$f = a_0x^0 + a_1x^1 + \dots + a_nx^n$$

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:

$$\begin{aligned} & (a_0x^0 + a_1x^1 + \dots + a_nx^n) + (b_0x^0 + b_1x^1 + \dots + b_mx^m) \\ &= (a_0 + b_0)x^0 + (a_1 + b_1)x^1 + \dots + (a_{\max(n,m)} + b_{\max(n,m)})x^{\max(n,m)} \end{aligned}$$

und

$$\begin{aligned} & (a_0x^0 + a_1x^1 + \dots + a_nx^n) \cdot (b_0x^0 + b_1x^1 + \dots + b_mx^m) \\ &= c_0x^0 + c_1x^1 + \dots + c_{n+m}x^{n+m} \end{aligned}$$

wobei

$$c_k = \sum_{j=0}^k a_j b_{k-j}.$$

Polynomringe in mehr als einer Variablen definieren wir induktiv als

$$R[x_1, \dots, x_r] = R[x_1, \dots, x_{r-1}][x_r].$$

Als Datenstruktur ist ein Polynom vom Grad n nichts anderes als eine Liste

$$a_0x^0 + a_1x^1 + \dots + a_nx^n = (a_0, \dots, a_n) \in R^{n+1}.$$

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 4.2.7 In $\mathbb{Q}[X]$ ist z.B.

$$\begin{aligned}(x^2 + x + 1) \cdot (x + 1) &= x^3 + 2x^2 + 2x + 1 \\ (x^2 + x + 1) + (x + 1) &= x^2 + 2x + 2.\end{aligned}$$

Setzen wir den Wert $x = 2$ in

$$\begin{aligned}g &= x^2 + x + 1 \\ h &= x + 1\end{aligned}$$

und

$$f = g \cdot h = x^3 + 2x^2 + 2x + 1$$

ein, so erhalten wir

$$\begin{aligned}g(2) &= 7 \\ h(2) &= 3 \\ f(2) &= 21\end{aligned}$$

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

$$(f + g)(s) = f(s) + g(s) \quad (f \cdot g)(s) = f(s) \cdot g(s)$$

Wir präzisieren zunächst, was es bedeutet, in ein Polynom einzusetzen. Dazu definiert man:

Definition 4.2.8 Eine **R -Algebra** S ist gegeben durch einen Homomorphismus kommutativer Ringe $\varphi : R \rightarrow S$. Man bezeichnet dann

$$\begin{aligned}R \times S &\rightarrow S \\ (r, s) &\mapsto r \cdot s := \varphi(r) \cdot s\end{aligned}$$

als die **Skalarmultiplikation**.

Beispiel 4.2.9 Durch die Inklusion $\mathbb{Z} \subset \mathbb{C}$ ist \mathbb{C} eine \mathbb{Z} -Algebra. Mit dem Monomorphismus

$$R \longrightarrow R[x], a_0 \longmapsto a_0x^0$$

wird $R[x]$ zu einer R -Algebra.

Ist S eine R -Algebra, d.h. gibt es eine Skalarmultiplikation $R \times S \rightarrow S$, dann können wir Elemente von S in Polynome über R einsetzen:

Satz 4.2.10 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

$$\psi(a_0x^0 + a_1x^1 + \dots + a_nx^n) := a_0 + a_1s + \dots + a_ns^n$$

ist der eindeutig bestimmte Homomorphismus gegeben. Man überprüfe als Übung, dass ψ multiplikativ und $R[s] \subset S$ ein Unterring ist. ■

Beispiel 4.2.11 Durch Einsetzen in das Polynom $x^2 + 1 \in \mathbb{R}[x]$ erhalten wir die Polynomfunktion

$$\begin{aligned} \mathbb{R} &\rightarrow \mathbb{R} \\ s &\mapsto s^2 + 1 \end{aligned}$$

siehe Abbildung 4.1.

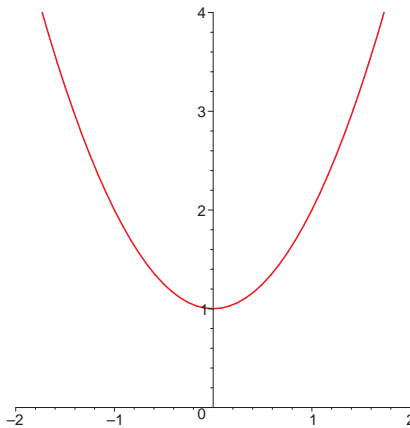


Abbildung 4.1: Polynomfunktion

4.3 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 4.3.1 Sei $d \in \mathbb{Z}$. Betrachte den Substitutionshomomorphismus

$$\mathbb{Z}[x] \rightarrow \mathbb{C}, x \mapsto \sqrt{d}$$

der in Polynomen mit ganzzahligen Koeffizienten x durch $\sqrt{d} \in \mathbb{C}$ ersetzt. Dann ist

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$$

denn wegen $\sqrt{d^2} = d \in \mathbb{Z}$ treten nur konstante und lineare Terme 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 4.3.2 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 4.3.3 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 4.3.4 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

$$f = (x - c_1) \cdot \dots \cdot (x - c_n)$$

mit $c_i \in \mathbb{C}$, hat also mit Vielfachheit gezählt genau n Nullstellen in \mathbb{C} .

Bemerkung 4.3.5 Sind $c_1, \dots, c_n \in \mathbb{C}$ die Nullstellen des Grad n Polynoms $f \in \mathbb{Q}[x]$, dann zerfällt f in dem durch iterative Adjunktion von c_1, \dots, c_n konstruierten Körper

$$K := \mathbb{Q}[c_1, \dots, c_n] := \mathbb{Q}[c_1][c_2] \dots [c_n]$$

in Linearfaktoren und die Erweiterung

$$\mathbb{Q} \subset K$$

ist algebraisch, d.h. K lässt sich exakt im Computer darstellen.

4.4 Die Einheitengruppe von \mathbb{Z}/n

Definition 4.4.1 Sei R ein kommutativer Ring mit 1. Ein Element $u \in R$ heißt **Einheit** von R , wenn ein $x \in R$ existiert mit

$$xu = 1.$$

Die Menge der Einheiten wird mit R^\times bezeichnet. Mit u ist offenbar auch x eine Einheit und (R^\times, \cdot) ist eine Gruppe, die **Einheitengruppe** von R .

Gilt $1 \neq 0$ und ist

$$R^\times = R \setminus \{0\},$$

so heißt R **Körper**.

Bemerkung: Das Inverse $w = u^{-1}$ ist in R^\times eindeutig (Übung 3.2).

Ein Element $\bar{a} \in \mathbb{Z}/n$ ist also invertierbar genau dann, wenn es ein $b \in \mathbb{Z}$ gibt mit $\bar{a} \cdot \bar{b} = \bar{1}$, 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

$$\text{ggT}(a, n) = 1.$$

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 4.4.2 Für $n \in \mathbb{N}$ ist

$$(\mathbb{Z}/n)^\times = \{\bar{a} \in \mathbb{Z}/n \mid \text{ggT}(a, n) = 1\}$$

Die Elemente heißen **prime Restklassen**. Die Gruppe $(\mathbb{Z}/n)^\times$ bezeichnen wir auch als die **prime Restklassengruppe**.

Als direkte Folgerung erhalten wir:

Corollar 4.4.3 Der Ring \mathbb{Z}/n ist ein Körper genau dann, wenn n eine Primzahl ist.

Beispiel 4.4.4 Die Restklasse $\bar{8} \in \mathbb{Z}/15$ hat ein Inverses, d.h. $\bar{8} \in (\mathbb{Z}/15)^\times$, denn

$$\text{ggT}(8, 3 \cdot 5) = 1$$

Mit dem erweiterten Euklidischen Algorithmus erhalten wir eine Darstellung des größten gemeinsamen Teilers

$$1 = (2) \cdot 8 + (-1) \cdot 15$$

also ist

$$\bar{8}^{-1} = \bar{2}$$

Definition 4.4.5 Die **Eulersche φ -Funktion** $\varphi : \mathbb{N} \rightarrow \mathbb{Z}$ ist definiert durch

$$\varphi(n) := |(\mathbb{Z}/n)^\times| = |\{r \in \mathbb{Z} \mid 1 \leq r \leq n, \text{ggT}(r, n) = 1\}|$$

gibt also für n die Ordnung der Einheitengruppe $(\mathbb{Z}/n)^\times$ an.

Satz 4.4.6 (Satz von Fermat-Euler) Für alle $a, n \in \mathbb{Z}$, $n \geq 1$ mit $\text{ggT}(a, n) = 1$ gilt

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Beweis. Nach Corollar 3.2.52 teilt die Ordnung jedes Elements g einer Gruppe G die Gruppenordnung, also

$$g^{|G|} = e.$$

Angewendet auf $\bar{a} \in (\mathbb{Z}/n)^\times$ erhalten wir

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

■

Für Primzahlen p ist

$$\varphi(p) = p - 1,$$

also

$$a^{p-1} \equiv 1 \pmod{p} \quad \text{falls } p \nmid a$$

und somit (denn für $p \mid a$ ist $a^p \equiv 0 \equiv a \pmod{p}$):

Corollar 4.4.7 (Kleiner Satz von Fermat) *Ist p eine Primzahl und $a \in \mathbb{Z}$, dann gilt*

$$a^p \equiv a \pmod{p}.$$

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 3.8) ist tatsächlich ein Ringisomorphismus:

Satz 4.4.8 *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 3.8 gezeigt ist durch

$$\begin{aligned} \pi : \quad \mathbb{Z}/m_1m_2 &\longrightarrow \mathbb{Z}/m_1 \times \mathbb{Z}/m_2 \\ a + m_1m_2\mathbb{Z} &\longmapsto (a + m_1\mathbb{Z}, a + m_2\mathbb{Z}) \end{aligned}$$

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 4.4.9 Mit Satz 2.5.1 erhalten wir durch Bestimmung der Lösungsmenge der simultanen Kongruenzen

$$x \equiv 7 \pmod{15} \iff \begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 2 \pmod{5} \end{cases}$$

Entsprechend Satz 4.4.8 läßt sich diese Aussage umformulieren als

$$\mathbb{Z}/15 \cong \mathbb{Z}/3 \times \mathbb{Z}/5 \quad \text{und}$$

$$\bar{7} \mapsto (\bar{1}, \bar{2})$$

Die Bestimmung des Urbilds von $(\bar{1}, \bar{2})$ unter diesem Isomorphismus ist also das Lösen der simultanen Kongruenz

$$\begin{aligned} x &\equiv 1 \pmod{3} \\ x &\equiv 2 \pmod{5} \end{aligned}$$

Umgekehrt ist die Berechnung des Bildes von $\bar{7}$ einfach die Reduktion modulo 3 und 5.

Bezüglich der Multiplikation gilt z.B.

$$\begin{aligned} \pi(\bar{7}) \cdot \pi(\bar{4}) &= (\bar{1}, \bar{2}) \cdot (\bar{1}, \bar{4}) = (\bar{1}, \bar{8}) = (\bar{1}, \bar{3}) \\ &= \pi(\bar{13}) = \pi(\bar{7} \cdot \bar{4}). \end{aligned}$$

Mit Satz 4.4.8 ist die φ -Funktion multiplikativ:

Corollar 4.4.10 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 4.4.11 Ist $n = p \cdot q$ das Produkt von zwei Primzahlen, so gilt

$$\varphi(n) = (p-1)(q-1).$$

4.5 Anwendung: RSA Kryptosystem

4.5.1 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

$$\{\text{Klartextnachrichten}\} \rightarrow \{\text{verschlüsselte Nachrichten}\},$$

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 (Moore's 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. Insbesondere interessiert uns die Gruppenordnung, denn die Ordnung jedes Elements teilt die Gruppenordnung (Corollar 3.2.52).

4.5.2 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 $p \cdot q > N$.
- 2) Berechne

$$n := p \cdot q$$

und den Wert der Eulerfunktion

$$\varphi(n) = (p-1)(q-1).$$

Die Zahlen p und q können nun gelöscht werden.

- 3) Wähle eine Zahl $e \in \mathbb{N}$ mit

$$\text{ggT}(e, \varphi(n)) = 1.$$

- 4) Berechne das Inverse $0 < d < \varphi(n)$ von e modulo $\varphi(n)$, also mit

$$ed \equiv 1 \pmod{\varphi(n)}.$$

Nun kann $\varphi(n)$ gelöscht werden.

Der öffentliche Schlüssel ist das Tupel (n, e) und der private Schlüssel d .

4.5.3 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

$$c := m^{e_A} \pmod{n_A}$$

und überträgt c an Alice. Wir nehmen an, dass $\text{ggT}(m, n_A) = 1$, was mit sehr hoher Wahrscheinlichkeit der Fall ist. Anderenfalls hat B einen Teiler von n_A gefunden und kann damit den privaten Schlüssel 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

$$\tilde{m} \equiv c^{d_A} \equiv (m^{e_A})^{d_A} = m^{e_A d_A} = m^{1+k \cdot \varphi(n_A)} = m \cdot (m^{\varphi(n_A)})^k \equiv m \bmod n_A$$

mit dem Satz von Fermat-Euler [4.4.6](#).

Beispiel 4.5.1 *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

$$1 = \text{ggT}(e_A, \varphi(n_A)) = (-23) \cdot 13 + (5) \cdot 60$$

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 4.3.

Bemerkung 4.5.2 *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 4.5. In MAPLE ist ein solches Verfahren in dem Kommando

$$\text{Power}(a, b) \bmod n$$

implementiert.

4.6 Anwendung: Primfaktorisation 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 4.6.1 (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 $\text{ggT}(a, n) = 1$ (wenn nicht, haben wir einen echten Teiler gefunden). Sind a und n teilerfremd, erhalten wir einen Faktor von n als

$$\text{ggT}(a^k - 1, n) > 1$$

denn k ist nach Voraussetzung ein Vielfaches von $\varphi(p)$, also $k = k' \cdot \varphi(p)$. Damit gibt der kleine Fermatsche Satz

$$a^k = (a^{\varphi(p)})^{k'} \equiv 1 \pmod{p}$$

also $p \mid \text{ggT}(a^k - 1, n)$. 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 4.6.2 *Sei $n = 21733$ und $B = 10$, also*

$$k = 2^3 \cdot 3^2 \cdot 5 \cdot 7.$$

Sei weiter $a = 2$. Dann ist

$$2^k - 1 \equiv 16037 \pmod{n}$$

und

$$\text{ggT}(16037, n) = 211.$$

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 4.4.

4.7 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

$$(g^b)^a = (g^a)^b$$

- 5) Alice und Bob löschen a bzw. b .

Bemerkung 4.7.1 *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 4.7.2 *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 4.7.3 *Sei $p = 11$ und $g = \bar{2}$. Tatsächlich ist g ein Erzeuger:*

$$(\mathbb{Z}/11)^\times = \langle \bar{2} \rangle = \{\bar{2}, \bar{4}, \bar{8}, \bar{5}, \bar{10}, \bar{9}, \bar{7}, \bar{3}, \bar{6}, \bar{1}\}.$$

Alice wählt $a = 3$ und sendet

$$\bar{2}^3 = \bar{8},$$

Bob wählt $b = 9$ und sendet

$$\bar{2}^9 = \overline{512} = \bar{6}.$$

Beide teilen nun das Geheimnis

$$\bar{8}^9 = \bar{6}^3 = \bar{7}.$$

4.8 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

$$\begin{array}{ccc} \pi: (R, +) & \longrightarrow & (R/I, +) \\ r & \longmapsto & \bar{r} = r + I \end{array}$$

hat $\text{Ker } \pi = I$ 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

$$\bar{r}_1 \cdot \bar{r}_2 = \pi(r_1) \cdot \pi(r_2) = \pi(r_1 r_2) = \overline{r_1 r_2}.$$

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 4.8.1 Sei R ein kommutativer Ring mit 1. Ein **Ideal** ist eine nicht leere Teilmenge $I \subset R$ mit

$$\begin{aligned} a + b &\in I \\ ra &\in I \end{aligned}$$

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 4.8.2 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 4.8.3 1) Sind $I_1, I_2 \subset R$ Ideale, dann auch deren Durchschnitt $I_1 \cap I_2$.

2) Seien $a_1, \dots, a_n \in R$. Dann ist

$$(a_1, \dots, a_n) := \left\{ \sum_{i=1}^n r_i a_i \mid r_i \in R \right\}$$

ein Ideal, das von dem **Erzeugendensystem** a_1, \dots, a_n erzeugte Ideal.

3) In Abschnitt 4.1 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 4.8.2, dass $\mathbb{Z}/n\mathbb{Z}$ ein kommutativer Ring mit 1 ist. Die Elemente sind genau die Restklassen $\overline{0}, \overline{1}, \dots, \overline{n-1}$, d.h.

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/n.$$

4) Sei $\varphi: R \rightarrow S$ ein Ringhomomorphismus. Der Kern

$$\text{Ker } \varphi = \{r \in R \mid \varphi(r) = 0\} \subset R$$

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 4.8.4 (Homomorphiesatz) Sei $\varphi: R \rightarrow S$ ein Ringhomomorphismus. Dann gilt

$$R/\text{Ker } \varphi \cong \text{Bild } \varphi$$

Beweis. Aus Satz 3.3.10 erhalten wir einen Isomorphismus

$$\begin{aligned} \tilde{\varphi}: R/\text{Ker } \varphi &\rightarrow \text{Bild } \varphi \\ \bar{r} = r + \text{Ker } \varphi &\mapsto \varphi(r) \end{aligned}$$

der additiven abelschen Gruppen. Weiter ist $\tilde{\varphi}$ ein Ringhomomorphismus, denn

$$\begin{aligned} \tilde{\varphi}(\overline{r_1 \cdot r_2}) &= \tilde{\varphi}(\overline{r_1} \cdot \overline{r_2}) = \varphi(r_1 \cdot r_2) \\ &= \varphi(r_1) \cdot \varphi(r_2) = \tilde{\varphi}(\overline{r_1}) \cdot \tilde{\varphi}(\overline{r_2}). \end{aligned}$$

■

4.9 Integritätsringe und Körper

Definition 4.9.1 Sei R ein kommutativer Ring mit 1.

- 1) Ein Element $a \in R$ heißt **Nullteiler** von R , wenn ein $x \in R \setminus \{0\}$ existiert mit

$$xa = 0.$$
- 2) Hat R außer 0 keine Nullteiler und ist $1 \neq 0$, so heißt R **Integritätsring**.

Wir haben bereits gesehen, dass ein Element von R nicht sowohl eine Einheit und ein Nullteiler sein kann.

Beispiel 4.9.2 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 $K^\times = K \setminus \{0\}$.
- 3) $\mathbb{Z}/6 = \{\bar{0}, \bar{1}, \dots, \bar{5}\}$ ist kein Integritätsring, $\bar{2}, \bar{3}, \bar{4}$ (und natürlich $\bar{0}$) sind Nullteiler, $\bar{1}$ und $\bar{5}$ sind Einheiten.
Siehe auch Übungsaufgabe 4.2.
- 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 $\deg(f) = \deg(g) = 0$.

- 5) Der Ring der Gaußschen Zahlen

$$\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$$

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 Übung 4.20.

Bemerkung 4.9.3 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 4.11.

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 4.9.4 Jeder endliche Integritätsring ist ein Körper.

Dies zeigen wir in Übung 4.10. Damit erhalten wir auch nochmals das Resultat aus Corollar 4.4.3:

Corollar 4.9.5 Ist p eine Primzahl, dann ist

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$$

ein Körper.

Beweis. Folgt direkt aus Satz 4.9.4: Ist $\bar{a} \cdot \bar{b} = \bar{0}$ für $\bar{a}, \bar{b} \in \mathbb{F}_p$ dann $p \mid ab$, also $p \mid a$ oder $p \mid b$, somit $\bar{a} = \bar{0}$ oder $\bar{b} = \bar{0}$. ■

Bemerkung 4.9.6 Sei K ein Körper und

$$\begin{aligned} \chi: \mathbb{Z} &\longrightarrow K \\ n &\longmapsto n \cdot 1_K \end{aligned}$$

die charakteristische Abbildung. Der Kern ist ein Ideal

$$\text{Ker } \chi = p\mathbb{Z}$$

mit $p \geq 0$. Man nennt

$$\text{char}(K) = p \geq 0$$

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

$$\mathbb{Z}/p\mathbb{Z} \rightarrow K$$

nach dem Homomorphiesatz 4.8.4 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 4.9.7 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 $\text{char}(\mathbb{F}_{p^r}) = p$. Siehe auch Aufgabe 4.9, 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.

4.10 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 4.10.1 *Ein euklidischer Ring ist ein Integritätsring R mit einer Abbildung*

$$d: R \setminus \{0\} \longrightarrow \mathbb{N}_0$$

sodass für je zwei Elemente $a, b \in R \setminus \{0\}$ 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 4.10.2 1) \mathbb{Z} ist euklidisch mit der Betragsabbildung

$$d(n) = |n|$$

und der üblichen Division mit Rest, siehe auch Beispiel 2.3.5.

- 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

$$\begin{aligned} x^2 + \frac{1}{2}x + \frac{1}{2} &= \left(\frac{1}{2}x\right) \cdot (2x - 1) + \left(x + \frac{1}{2}\right) \\ &= \underbrace{\left(\frac{1}{2}x + \frac{1}{2}\right)}_g \cdot (2x - 1) + \underbrace{1}_r \end{aligned}$$

also $d(r) = 0 < 1 = d(b)$.

3) $\mathbb{Z}[i]$ ist euklidisch mit

$$d: R \setminus \{0\} \longrightarrow \mathbb{Z}_{\geq 0}$$

$$d(a + i \cdot b) = a^2 + b^2$$

(dies zeigen wir in Übung 4.20).

Analog zu Definition 2.3.1 für \mathbb{Z} definiert man in jedem Integritätsring einen größten gemeinsamen Teiler (ggT) und ein kleinstes gemeinsame Vielfache (kgV). Diese sind eindeutig bis auf Multiplikation mit Einheiten (die natürlich jedes Element von R teilen).

In euklidischen Ringen kann wie in \mathbb{Z} die Division mit Rest und der euklidische Algorithmus (Satz 2.3.4) zur Bestimmung des ggT durchgeführt werden.

Satz 4.10.3 (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*

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

mit $u, v \in R$.

Beispiel 4.10.4 *Wir bestimmen den größten gemeinsamen Teiler von*

$$f = x^4 + x^3 \quad \text{und} \quad g = x^4 - 1$$

in $\mathbb{Q}[x]$ mit dem euklidischen Algorithmus

$$\begin{array}{rclcl} x^4 + x^3 & = & 1 & \cdot & (x^4 - 1) & + & \boxed{x^3 + 1} \\ x^4 - 1 & = & x & \cdot & (x^3 + 1) & + & \boxed{-x - 1} \\ x^3 + 1 & = & (-x^2) & \cdot & (-x - 1) & + & \boxed{-x^2 + 1} \\ & = & (-x^2 + x) & \cdot & (-x - 1) & + & \boxed{x + 1} \\ & = & (-x^2 + x - 1) & \cdot & (-x - 1) & + & \boxed{0} \end{array}$$

und erhalten

$$\text{ggT}(f, g) = -x - 1.$$

Da der ggT nur bis auf Multiplikation mit Elementen aus $\mathbb{Q}[x]^\times = \mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$ eindeutig ist, können wir genauso schreiben

$$\text{ggT}(f, g) = x + 1.$$

Siehe auch Übungsaufgabe 4.20.

Genau wie Ideale in \mathbb{Z} , haben Ideale in einem Euklidischen Ring R eine besonders einfache Struktur: Ein Ideal in R wird von einem einzigen Element a erzeugt

$$(a) = \{ar \mid r \in R\},$$

d.h. besteht genau aus den R -Vielfachen von a .

Definition 4.10.5 Sei R ein Integritätsring. Ist jedes Ideal von R von einem einzigen Element erzeugt, so heißt R **Hauptidealring**.

Satz 4.10.6 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 $b \in I \setminus \{0\}$ 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 4.10.7 Insbesondere sind \mathbb{Z} und $\mathbb{Q}[x]$ Hauptidealringe.

Ohne Beweis bemerken wir:

Satz 4.10.8 Hauptidealringe sind **faktoriell**, d.h. es gibt eine bis auf Einheiten eindeutige Primfaktorisation (ohne Beweis). Insbesondere existiert der ggT und ist bis auf Einheiten eindeutig.

Beispiel 4.10.9 In \mathbb{Z} ist

$$\text{ggT}(2^2 \cdot 5^3, 2^3 \cdot 5) = 2^2 \cdot 5,$$

in $\mathbb{Q}[x]$ ist

$$\text{ggT}(x^4 + x^3, x^4 - 1) = \text{ggT}(x^2 \cdot (x+1), (x^3 - x^2 + x - 1) \cdot (x+1)) = x+1.$$

Diesen ggT haben wir in Beispiel 4.10.4 auch schon mit dem Euklidischen Algorithmus berechnet.

Mit Hilfe des ggT können wir zu jedem Ideal einen Erzeuger angeben:

Bemerkung 4.10.10 *Ist R ein Hauptidealring, dann gilt*

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

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

$$d = \text{ggT}(a_1, a_2).$$

■

Für mehr als zwei Erzeuger geht man induktiv vor.

Beispiel 4.10.11 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: $\{\text{Euklidische Ringe}\} \subset \{\text{Hauptidealringe}\} \subset \{\text{Faktorielle Ringe}\} \subset \{\text{Integritätsringe}\}$, und dies sind echte Inklusionen:

Beispiel 4.10.12 *Der Ring $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ ist ein Hauptidealring, aber kein euklidischer Ring (ohne Beweis).*

Beispiel 4.10.13 *Der Ring $\mathbb{Z}[x]$ ist kein Hauptidealring (siehe auch Übungsaufgabe 4.14), aber faktoriell:*

Satz 4.10.14 (Satz von Gauß) Sei R ein Integritätsring. Dann gilt

$$R \text{ faktoriell} \iff R[x] \text{ faktoriell}$$

(ohne Beweis).

Beispiel 4.10.15 Der Integritätsring

$$R = K[x, y, z, w] / (xy - zw)$$

ist nicht faktoriell, denn

$$\bar{x}\bar{y} = \bar{z}\bar{w}.$$

4.11 Chinesischer Restsatz

Wir wollen nun das Lösen von simultanen Kongruenzen, das wir in Kapitel 2 über dem Ring der ganzen Zahlen kennengelernt haben, allgemein für einen kommutativen Ring R mit 1 betrachten. Für ganze Zahlen gilt

$$x \equiv a \pmod{n} \iff \bar{x} = \bar{a} \in \mathbb{Z}/n\mathbb{Z}.$$

Dabei ist $n\mathbb{Z} \subset \mathbb{Z}$ ein Ideal. Nach Satz 4.8.2 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 4.11.1 Sind $I_1, I_2 \subset R$ Ideale, dann sind die **Summe**

$$I_1 + I_2 = \{a + b \mid a \in I_1, b \in I_2\}$$

und der **Durchschnitt**

$$I_1 \cap I_2 \subset R$$

wieder Ideale.

Zwei Ideale I_1 und I_2 heißen **coprim**, wenn

$$I_1 + I_2 = R.$$

Beispiel 4.11.2 Ist R ein Hauptidealring und $a_1, a_2 \in R$, dann

$$\begin{aligned}(a_1) + (a_2) &= (\text{ggT}(a_1, a_2)) \\ (a_1) \cap (a_2) &= (\text{kgV}(a_1, a_2)).\end{aligned}$$

Insbesondere gilt

$$(a_1) \text{ und } (a_2) \text{ coprime} \iff \text{ggT}(a_1, a_2) = 1.$$

Beweis. Die erste Aussage folgt sofort aus Bemerkung 4.10.10, 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

$$m = \text{kgV}(a_1, a_2).$$

■

Satz 4.11.3 (Chinesischer Restsatz) Sei R ein kommutativer Ring mit 1 und I_1, \dots, I_n paarweise coprime Ideale. Dann ist der Ringhomomorphismus

$$\begin{aligned}\varphi: R &\longrightarrow R/I_1 \times \dots \times R/I_n \\ r &\longmapsto (r + I_1, \dots, r + I_n)\end{aligned}$$

surjektiv (ohne Beweis) und hat Kern

$$\text{Ker } \varphi = I_1 \cap \dots \cap I_n.$$

Mit dem Homomorphiesatz 4.8.4 gilt damit

$$\begin{aligned}R / (I_1 \cap \dots \cap I_n) &\cong R/I_1 \times \dots \times R/I_n \\ r + (I_1 \cap \dots \cap I_n) &\longmapsto (r + I_1, \dots, r + I_n)\end{aligned}$$

Als Corollar zu Satz 4.11.3 erhalten wir für den Fall $R = \mathbb{Z}$ wieder Satz 4.4.8:

Corollar 4.11.4 (Chinesischer Restsatz über \mathbb{Z}) Sind $n_1, \dots, n_t \in \mathbb{Z}_{>0}$ paarweise teilerfremd, dann gilt

$$\begin{aligned} \mathbb{Z}/(n_1 \cdot \dots \cdot n_t) &\cong \mathbb{Z}/(n_1) \times \dots \times \mathbb{Z}/(n_t) \\ \bar{r} &\longmapsto (\bar{r}, \dots, \bar{r}) \end{aligned}$$

Beweis. Mit Beispiel 4.11.2 folgt: Die Ideale $I_j = (n_j) \subset \mathbb{Z}$ sind coprim, denn für $i \neq j$ ist

$$(n_i) + (n_j) = (\text{ggT}(n_i, n_j)) = (1) = \mathbb{Z}.$$

Außerdem ist

$$I_1 \cap \dots \cap I_t = (\text{kgV}(n_1, \dots, n_t)) = (n_1 \cdot \dots \cdot n_t).$$

■

Mit dem Euklidischen Algorithmus kann man analog zum Fall $R = \mathbb{Z}$ simultane Kongruenzen auch über $R = K[x]$ lösen:

Beispiel 4.11.5 Wir bestimmen die Lösungsmenge $L \subset \mathbb{Q}[x]$ der simultanen Kongruenzen

$$\begin{aligned} f &\equiv 3 \pmod{x+1} \\ f &\equiv 2+x \pmod{x^2+x+1} \end{aligned}$$

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

$$\text{ggT}(x+1, x^2+x+1) = 1 = (-x) \cdot (x+1) + 1 \cdot (x^2+x+1)$$

$$\text{Weiter ist } -x^3+x+3 = (2+x) \cdot (-x) \cdot (x+1) + 3 \cdot 1 \cdot (x^2+x+1)$$

eine Lösung der simultanen Kongruenzen (analog zur Lösungsformel in \mathbb{Z} aus Kapitel 2) und somit

$$\begin{aligned} L &= \{-x^3+x+3 + g \cdot (x^3+2x^2+2x+1) \mid g \in \mathbb{Q}[x]\} \\ &= -x^3+x+3 + (x^3+2x^2+2x+1) \\ &= 2x^2+3x+4 + (x^3+2x^2+2x+1) \end{aligned}$$

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.

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 $(\overline{3}, \overline{2+x})$ ist, d.h.

$$L = \overline{2x^2 + 3x + 4} \mapsto (\overline{3}, \overline{2+x}).$$

Siehe auch Übung 4.17.

4.12 Anwendung: Modulares Rechnen

Mit Hilfe des Chinesischen Restsatzes lassen sich viele Algorithmen mit ganzzahligem Input und Output beschleunigen.

Bemerkung 4.12.1 *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 $n = n_1 \cdot \dots \cdot n_r > 2C$ mit n_i paarweise teilerfremd und alle n_i etwa gleich groß und rechnet in*

$$\mathbb{Z}/n_1 \times \dots \times \mathbb{Z}/n_r \cong \mathbb{Z}/n$$

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 4.12.2 *Zur Berechnung von $32 \cdot 45$ betrachten wir*

$$\begin{array}{rcccccc} \mathbb{Z} & \rightarrow & \mathbb{Z}/2310 & \cong & \mathbb{Z}/2 & \times & \mathbb{Z}/3 & \times & \mathbb{Z}/5 & \times & \mathbb{Z}/7 & \times & \mathbb{Z}/11 \\ 32 & \mapsto & \overline{32} & \mapsto & (\overline{0} & , & \overline{2} & , & \overline{2} & , & \overline{4} & , & \overline{10}) \\ 45 & \mapsto & \overline{45} & \mapsto & (\overline{1} & , & \overline{0} & , & \overline{0} & , & \overline{3} & , & \overline{1}) \\ & & & & & & & & \parallel & & & & \\ & & \overline{1440} & \mapsto & (\overline{0} & , & \overline{0} & , & \overline{0} & , & \overline{5} & , & \overline{10}) \end{array}$$

Dabei ist $\overline{1440} = 1440 + 2310\mathbb{Z}$ die Lösungsmenge der simultanen Kongruenzen

$$\begin{aligned} x &\equiv 0 \pmod{2} \\ x &\equiv 0 \pmod{3} \\ x &\equiv 0 \pmod{5} \\ x &\equiv 5 \pmod{7} \\ x &\equiv 10 \pmod{11} \end{aligned}$$

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

4.13 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 4.13.1 Für ein Polynom $f \in K[x]$ und $t, c \in K$ ist die Bedingung

$$f(t) = c$$

äquivalent zu der Kongruenz

$$f \equiv c \pmod{(x-t)}$$

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 $\bar{f} = \bar{c} \in K[x]/(x-t)$.

Satz 4.13.2 (Lagrange-Interpolation) Sei K ein Körper. Sind $t_1, \dots, t_k \in K$ paarweise verschiedene Stützstellen und $c_1, \dots, c_k \in K$, dann gibt es genau ein Polynom $f \in K[x]$ mit $\deg f < k$ und

$$f(t_i) = c_i \quad \forall i.$$

Beweis. Es gilt für alle $i \neq j$, dass

$$1 \in (t_i - t_j) \quad \text{und} \quad t_i - t_j \in (x - t_i) + (x - t_j)$$

also

$$K[x] = (1) \subset t_i - t_j \subset (x - t_i) + (x - t_j)$$

d.h.

$$(x - t_i) + (x - t_j) = (1) = K[x].$$

Somit liefert der Chinesische Restsatz

$$K[x]/\left(\prod_{i=1}^k (x - t_i)\right) \cong K[x]/(x - t_1) \times \dots \times K[x]/(x - t_k) \cong K^k$$

also existiert ein eindeutiges Urbild \bar{g} mit

$$\bar{g} \longmapsto (\bar{c}_1, \dots, \bar{c}_k).$$

Dabei ist g eine Lösung der simultanen Kongruenzen

$$g \equiv c_i \pmod{(x - t_i)} \quad \forall i$$

Es gilt also $g - c_i = q_i \cdot (x - t_i) \quad \forall i$ und somit $g(t_i) - c_i = 0 \quad \forall i$.

Division mit Rest

$$g = q \cdot \prod_{i=1}^k (x - t_i) + f$$

gibt ein eindeutiges $f \in \bar{g}$ mit $\deg(f) < k$. Weiter ist $g(t_i) = f(t_i) \quad \forall i$. ■

Beispiel 4.13.3 Wir suchen das eindeutige Polynom $f \in \mathbb{R}[x]$ vom Grad 1 mit

$$\begin{aligned} f(-1) &= 1 \\ f(1) &= 2 \end{aligned}$$

Der erweiterte Euklidische Algorithmus liefert

$$1 = \frac{1}{2} \cdot (x + 1) + \left(-\frac{1}{2}\right) \cdot (x - 1)$$

also ist

$$f = 2 \cdot \frac{1}{2} \cdot (x + 1) + 1 \cdot \left(-\frac{1}{2}\right) \cdot (x - 1) = \frac{1}{2}x + \frac{3}{2}$$

siehe Abbildung 4.2.

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 4.13.4 Mit den **Lagrangepolynomen**

$$f_i = \prod_{\substack{j=1 \\ j \neq i}}^k \frac{x - t_j}{t_i - t_j}$$

ist

$$\begin{aligned} f_i &\equiv 1 \pmod{(x - t_i)} \\ f_i &\equiv 0 \pmod{(x - t_j)} \quad \text{für } j \neq i \end{aligned}$$

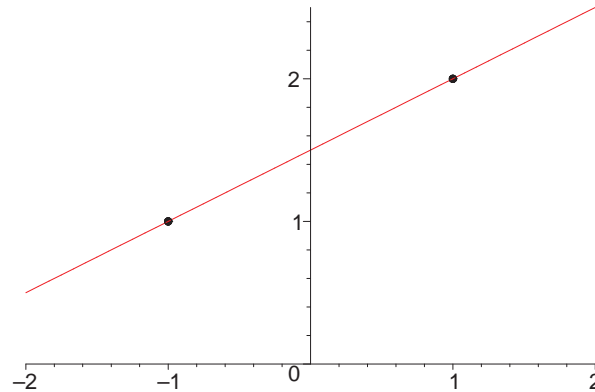


Abbildung 4.2: Interpolation

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 4.13.5 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

$$\begin{aligned} f &= 1 \cdot \frac{(x-0)(x-2)}{(-1-0)(-1-2)} + 0 \cdot \frac{(x+1)(x-2)}{(0+1)(0-2)} + 1 \cdot \frac{(x+1)(x-0)}{(2+1)(2-0)} \\ &= \frac{1}{3}(x^2 - 2x) + \frac{1}{6}(x^2 + x) \\ &= \frac{1}{2}x^2 - \frac{1}{2}x \end{aligned}$$

berechnen. Abbildung 4.3 zeigt den Graphen der Funktion $\mathbb{R} \rightarrow \mathbb{R}$, $x \mapsto f(x)$.

In MAPLE ist die Lagrange-Interpolation implementiert in dem Befehl `interp`:

```
f:=interp([-1,0,2],[1,0,1],x);
```

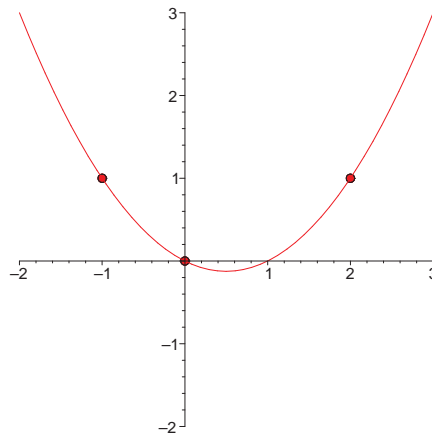


Abbildung 4.3: Interpolation

$$f = \frac{1}{2}x^2 - \frac{1}{2}x$$

Den Funktionsgraphen können wir plotten durch:
`plot(f, x=-2..2);`

4.14 Übungsaufgaben

Übung 4.1 Sei R ein Ring. Zeigen Sie durch Verwendung der Ringaxiome, dass für alle $x, y \in R$ gilt

$$0x = x0 = 0$$

$$(-x)y = x(-y) = -xy$$

$$(-x)(-y) = xy$$

Übung 4.2 Stellen Sie die Verknüpfungstabellen 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 4.3 Der öffentliche RSA-Schlüssel von Alice ist

$$n_A = 16193582284064670754749147755570104509669721475765293619$$

$$e_A = 2^{16} + 1$$

Bob hat eine verschlüsselte Nachricht

$c = 14068462319149774133380855330222038912509815146884619993$

an Alice geschickt. Was war der Inhalt der Nachricht?

Hinweise: Um für $a, b, n \in \mathbb{N}$ effizient $a^b \bmod n$ zu berechnen, können Sie das MAPLE Kommando

$$\text{Power}(a, b) \bmod n$$

verwenden.

Verwenden Sie die MAPLE-Funktion `ifactor`.

Übung 4.4 1) Implementieren Sie das Faktorisierungsverfahren von Pollard.

2) Testen Sie Ihre Implementierung an Beispielen, insbesondere auch an Aufgabe 4.3.

Hinweis: Alice hat ungeschickterweise einen Primfaktor p von $n_A = p \cdot q$ so gewählt, dass $\varphi(p)$ nur Primpotenzfaktoren ≤ 200000 hat.

Übung 4.5 Seien $a, b, n \in \mathbb{N}$ und

$$b = b_0 2^0 + b_1 2^1 + b_2 2^2 + \dots$$

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 4.3.

Übung 4.6 Der Fermatsche Primzahltest: n heißt **Fermatsche Pseudoprimzahl** zur Basis a , wenn n nicht prim ist, aber dennoch $a^{n-1} \equiv 1 \pmod n$ 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 4.7 Sei $m \in \mathbb{Z}_{\geq 2}$. Für ein $a \in \mathbb{Z}$ gelte $a^{m-1} \equiv 1 \pmod{m}$ und $a^{\frac{m-1}{p}} \not\equiv 1 \pmod{m}$ für jeden Primteiler p von $m-1$. Zeigen Sie, dass dann m prim ist.

Übung 4.8 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 4.2.6 ein Integritätsring.
- 2) Implementieren Sie die Addition und Multiplikation in $K[x]$.

Übung 4.9 Zeigen Sie, dass es einen Körper K mit genau 4 Elementen gibt, indem Sie die Verknüpfungstabellen der Addition und Multiplikation aufstellen.

Hinweis: Bezeichnen Sie die Elemente von K als $0, 1, a, a+1$.

Übung 4.10 Zeigen Sie:

- 1) Jeder Integritätsring mit endlich vielen Elementen ist ein Körper.
- 2) In einem endlichen Ring ist jedes Element entweder eine Einheit oder ein Nullteiler.

Übung 4.11 Sei R ein Integritätsring und $S = R \setminus \{0\}$. 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

$$\begin{aligned} \frac{r_1}{s_1} + \frac{r_2}{s_2} &= \frac{r_1 s_2 + r_2 s_1}{s_1 s_2} \\ \frac{r_1}{s_1} \cdot \frac{r_2}{s_2} &= \frac{r_1 r_2}{s_1 s_2} \end{aligned}$$

- 1) Zeigen Sie: Addition und Multiplikation sind wohldefiniert und $Q(R)$ ist ein Körper.

- 2) Implementieren Sie die Arithmetik in $\mathbb{Q} = \mathbb{Q}(\mathbb{Z})$, 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 $\mathbb{Q}(X) = \mathbb{Q}(\mathbb{Q}[X])$ funktioniert?

Übung 4.12 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 4.13 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 4.14 Zeigen Sie, dass $\mathbb{Z}[x]$ kein Hauptidealring ist.

Hinweis: Betrachten Sie das Ideal $(2, x)$.

Übung 4.15 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 4.16 Bestimmen Sie in $\mathbb{Q}[x]$ den größten gemeinsamen Teiler $\text{ggT}(f, g)$ von

$$f = x^2 + 2x + 1 \quad g = x^2 - 2x + 1$$

und $a, b \in \mathbb{Q}[x]$ mit

$$\text{ggT}(f, g) = a \cdot f + b \cdot g.$$

Überprüfen Sie Ihr Ergebnis mit dem MAPLE-Befehl `gcdex`.

Übung 4.17 Bestimmen Sie die Menge $L \subset \mathbb{R}[x]$ aller Lösungen f der simultanen Kongruenzen

$$f \equiv 2 + 3(x - 1) \pmod{(x - 1)^2}$$

$$f \equiv 1 + 2(x + 1) \pmod{(x + 1)^2}$$

Finden Sie die eindeutige Lösung $f \in L$ minimalen Grades. Siehe auch Abbildung 4.4.

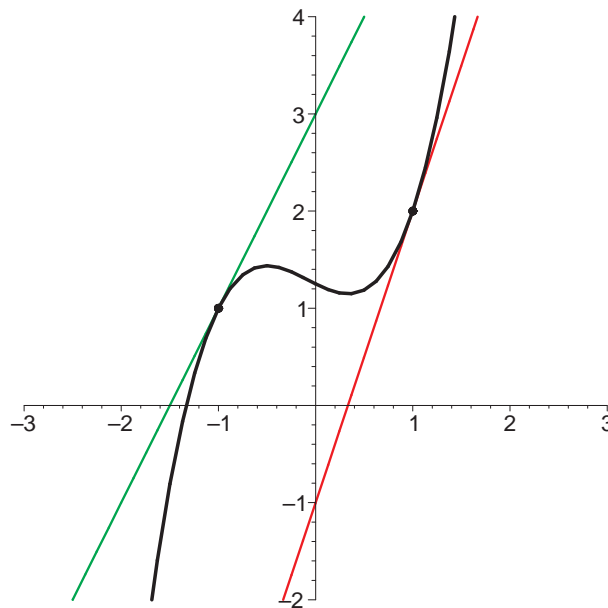


Abbildung 4.4: Polynom mit vorgegebenen Funktionswerten und Ableitungen

Übung 4.18 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 4.19 Seien $a_1, \dots, a_r \in \mathbb{R}$ paarweise verschieden und $m_1, \dots, m_r \in \mathbb{N}$ mit $\sum_{j=1}^r m_j = d + 1$. Zeigen Sie mit Hilfe des Chinesischen Restsatzes, dass es für alle

$$b_{1,0}, \dots, b_{1,m_1-1}, \dots, b_{r,0}, \dots, b_{r,m_r-1} \in \mathbb{R}$$

ein eindeutiges Polynom $f \in \mathbb{R}[x]_{\leq d}$ gibt mit

$$f^{(j)}(a_i) = b_{i,j}$$

für alle $j = 0, \dots, m_i - 1$ und $i = 1, \dots, r$.

Übung 4.20 Sei $i \in \mathbb{C}$ die imaginäre Einheit, also $i^2 = -1$, $R = \mathbb{Z}[i]$ und

$$\begin{aligned} d: R \setminus \{0\} &\rightarrow \mathbb{N}_0 \\ a + b \cdot i &\mapsto a^2 + b^2 \end{aligned}$$

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 4.21 Zeigen Sie für $n = -1, -2, 2, 3$, dass $R = \mathbb{Z}[\sqrt{n}]$ zusammen mit

$$\begin{aligned} d: R \setminus \{0\} &\rightarrow \mathbb{N}_0 \\ a + b\sqrt{n} &\mapsto |(a + b\sqrt{n})(a - b\sqrt{n})| \end{aligned}$$

ein euklidischer Ring ist. Geben Sie ein Verfahren an, um die Division mit Rest durchzuführen.

Übung 4.22 Schreiben Sie ein MAPLE Programm, das in $R = \mathbb{Z}[\sqrt{n}]$, $n = -1, -2, 2, 3$ die Division mit Rest und den Euklidischen Algorithmus zur Bestimmung des ggT durchführt.

Übung 4.23 Bestimmen Sie jeweils einen Erzeuger der Ideale

$$(2 - i, 2 + i) \subset \mathbb{Z}[i] \quad (11 + 8\sqrt{3}, 7 + 2\sqrt{3}) \subset \mathbb{Z}[\sqrt{3}].$$

5

Vektorräume

5.1 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

$$f = x_1 t^3 + x_2 t^2 + x_3 t + x_4 \in \mathbb{R}[t]$$

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

$$\begin{array}{rcccccc} -x_1 & + & x_2 & - & x_3 & + & x_4 & = & 0 \\ & & 2x_2 & & & & & = & 0 \\ 8x_1 & + & 4x_2 & + & 2x_3 & + & x_4 & = & 0 \end{array}$$

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 5.1.1 Ein Polynom $f \in K[x_1, \dots, x_n]$ heißt **homogen**, wenn alle Terme von f denselben Grad haben.

Beispiel 5.1.2 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.

5.2 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 5.2.1 Sind $l_1, l_2 \in K[x_1, \dots, x_n]$ Polynome und $0 \neq c \in K$, dann gilt für alle $x \in K^n$

$$\left. \begin{array}{l} l_1(x) = 0 \\ l_2(x) = 0 \end{array} \right\} \iff \left\{ \begin{array}{l} l_1(x) = 0 \\ l_2(x) + c \cdot l_1(x) = 0 \end{array} \right.$$

und

$$l_1(x) = 0 \iff c \cdot l_1(x) = 0$$

und

$$\left. \begin{array}{l} l_1(x) = 0 \\ l_2(x) = 0 \end{array} \right\} \iff \left\{ \begin{array}{l} l_2(x) = 0 \\ l_1(x) = 0 \end{array} \right.$$

Um dies systematisch durchzuführen, müssen wir eine Reihenfolge für die Variablen festlegen. Die Idee ist hier, bezüglich der Totalordnung $x_1 > x_2 > \dots > x_n$ auf der Menge der Variablen den größten Term auszuwählen, man könnte aber auch jede andere Sortierung der Variablen verwenden. Bezüglich dieser Reihenfolge definieren wir:

Definition 5.2.2 Ist $f = c_s x_s + \dots + c_n x_n$ mit $c_s \neq 0$, dann heißt

$$L(f) = x_s$$

die *Leitvariable* (oder das *Leitmonom* von f),

$$LC(f) = c_s$$

der *Leitkoeffizient* von f ,

$$LT(f) = c_s x_s$$

der *Leitterm* von f , und

$$\text{tail}(f) = f - LT(f) = c_{s+1} x_{s+1} + \dots + c_n x_n$$

der *Tail* von f .

Beispiel 5.2.3 Für

$$f = 2x_2 + 5x_3 + x_4$$

ist

$$\begin{aligned} L(f) &= x_2 \\ LC(f) &= 2 \\ LT(f) &= 2x_2 \\ \text{tail}(f) &= 5x_3 + x_4. \end{aligned}$$

Leitterme markieren wir im Text typischerweise in rot.

Satz 5.2.4 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 5.1 ein äquivalentes System, sodass alle Leitmonome paarweise verschieden sind.

Siehe auch Aufgabe 5.2.

Algorithmus 5.1 Gaußalgorithmus

```

1: for all  $i$  do  $l_i = \frac{1}{\text{LC}(l_i)} \cdot l_i$ 
2: while exist  $i \neq j$  with  $L(l_i) = L(l_j)$  do
3:    $l_j = l_j - l_i$ 
4:   if  $l_j = 0$  then
5:     delete  $l_j$ 
6:   else
7:      $l_j = \frac{1}{\text{LC}(l_j)} \cdot l_j$ 

```

Beispiel 5.2.5 In dem obigen Beispiel

$$\begin{aligned} l_1 &= -\mathbf{x}_1 + x_2 - x_3 + x_4 = 0 \\ l_2 &= \mathbf{x}_2 = 0 \\ l_3 &= \mathbf{8x}_1 + 4x_2 + 2x_3 + x_4 = 0 \end{aligned}$$

geht der Algorithmus wie folgendermaßen vor:

- $l_1 := -l_1$, $l_2 := \frac{1}{2}l_2$ und $l_3 := \frac{1}{8}l_3$

$$\begin{aligned} \mathbf{x}_1 - x_2 + x_3 - x_4 &= 0 \\ \mathbf{x}_2 &= 0 \\ \mathbf{x}_1 + \frac{1}{2}x_2 + \frac{1}{4}x_3 + \frac{1}{8}x_4 &= 0 \end{aligned}$$

- $l_3 := l_3 - l_1$

$$\begin{aligned} \mathbf{x}_1 - x_2 + x_3 - x_4 &= 0 \\ \mathbf{x}_2 &= 0 \\ \frac{3}{2}\mathbf{x}_2 - \frac{3}{4}x_3 + \frac{9}{8}x_4 &= 0 \end{aligned}$$

- $l_3 := \frac{2}{3}l_3$

$$\begin{aligned} \mathbf{x}_1 - x_2 + x_3 - x_4 &= 0 \\ \mathbf{x}_2 &= 0 \\ \mathbf{x}_2 - \frac{1}{2}x_3 + \frac{3}{4}x_4 &= 0 \end{aligned}$$

- $l_3 := l_3 - l_2$

$$\begin{array}{rccccrcr} \mathbf{x}_1 & - & x_2 & + & x_3 & - & x_4 & = & 0 \\ & & \mathbf{x}_2 & & & & & = & 0 \\ & & & & -\frac{1}{2}\mathbf{x}_3 & + & \frac{3}{4}x_4 & = & 0 \end{array}$$

- $l_3 := -2l_3$

$$\begin{array}{rccccrcr} \mathbf{x}_1 & - & x_2 & + & x_3 & - & x_4 & = & 0 \\ & & \mathbf{x}_2 & & & & & = & 0 \\ & & & & \mathbf{x}_3 & - & \frac{3}{2}x_4 & = & 0 \end{array}$$

Bemerkung 5.2.6 Durch Sortieren der l_i nach aufsteigendem Index der Leitvariable $L(l_i)$ erhält man die **Zeilenstufenform** des Systems.

Beispiel 5.2.7 In Beispiel 5.2.5 ist das System schon in Zeilenstufenform, das System

$$\begin{array}{rccccrcr} l_1 = & \mathbf{x}_1 & & & & & & = & 0 \\ l_2 = & & & & \mathbf{x}_3 & & & = & 0 \\ l_3 = & & \mathbf{x}_2 & & & & & = & 0 \end{array}$$

dagegen nicht. Durch Vertauschen von l_2 und l_3 erhält man das System in Zeilenstufenform.

$$\begin{array}{rccccrcr} l_1 = & \mathbf{x}_1 & & & & & & = & 0 \\ l_2 = & & \mathbf{x}_2 & & & & & = & 0 \\ l_3 = & & & & \mathbf{x}_3 & & & = & 0 \end{array}$$

Bemerkung 5.2.8 Durch Algorithmus 5.2 können wir erreichen, dass die Variable $L(l_i)$ genau in l_i vorkommt. Man spricht dann von einer **reduzierten Zeilenstufenform**.

Siehe auch Aufgabe 5.2.

Algorithmus 5.2 Reduktion

- 1: **while** exist $i \neq j$ with $L(l_j)$ in $\text{tail}(l_i)$ with coeff c **do**
 - 2: $l_i = l_i - c \cdot l_j$
-

Beispiel 5.2.9 In Beispiel 5.2.5 erhalten wir durch $l_1 := l_1 + l_2$

$$\begin{array}{rccccrcr} \mathbf{x}_1 & & + & x_3 & - & x_4 & = & 0 \\ & \mathbf{x}_2 & & & & & = & 0 \\ & & & \mathbf{x}_3 & - & \frac{3}{2}x_4 & = & 0 \end{array}$$

und $l_1 := l_1 - l_3$ die reduzierte Zeilenstufenform

$$\begin{array}{rccccrcr} \mathbf{x}_1 & & & & - & \frac{1}{2}x_4 & = & 0 \\ & \mathbf{x}_2 & & & & & = & 0 \\ & & & \mathbf{x}_3 & - & \frac{3}{2}x_4 & = & 0 \end{array}$$

Bemerkung 5.2.10 (Lösungsmenge) Von der reduzierten Zeilenstufenform lässt sich die Lösungsmenge des Gleichungssystems direkt ablesen:

$$V = \{x \in K^n \mid L(l_i) = -\text{tail}(l_i) \text{ für alle } i\}$$

Alle Variablen, die nicht als Leitmonome auftreten, können also beliebige Werte in K annehmen, und die anderen Variablen berechnen sich durch die Gleichungen $L(l_i) = -\text{tail}(l_i)$ aus diesen. Wir können in x für $L(l_i)$ also $-\text{tail}(l_i)$ einsetzen.

Beispiel 5.2.11 Die Lösungsmenge des Gleichungssystems aus Beispiel 5.2.5 ist

$$V = \left\{ x \in \mathbb{R}^4 \mid \mathbf{x}_1 = -\frac{1}{2}x_4, \mathbf{x}_2 = 0, \mathbf{x}_3 = \frac{3}{2}x_4 \right\}.$$

Die Variable x_4 kann also beliebige Werte annehmen, während x_1, x_2, x_3 dann bestimmt sind. Durch Einsetzen lässt sich die Lösungsmenge damit auch schreiben als

$$V = \left\{ \left(\begin{array}{c} -\frac{1}{2}x_4 \\ 0 \\ \frac{3}{2}x_4 \\ x_4 \end{array} \right) \mid x_4 \in \mathbb{R} \right\}$$

Beispiel 5.2.12 Die Menge der in dem Beispiel in Abschnitt 5.1 gesuchten Polynome

$$f = x_1 t^3 + x_2 t^2 + x_3 t + x_4 \in \mathbb{R}[t]$$

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 5.1 zeigt die Graphen von einigen $f \in V$ (aufgefasst als Abbildungen $\mathbb{R} \rightarrow \mathbb{R}$, $x \mapsto f(x)$). Insbesondere sehen wir, dass jede solche Funktion bei $t = -1$ sogar eine doppelte Nullstelle hat.

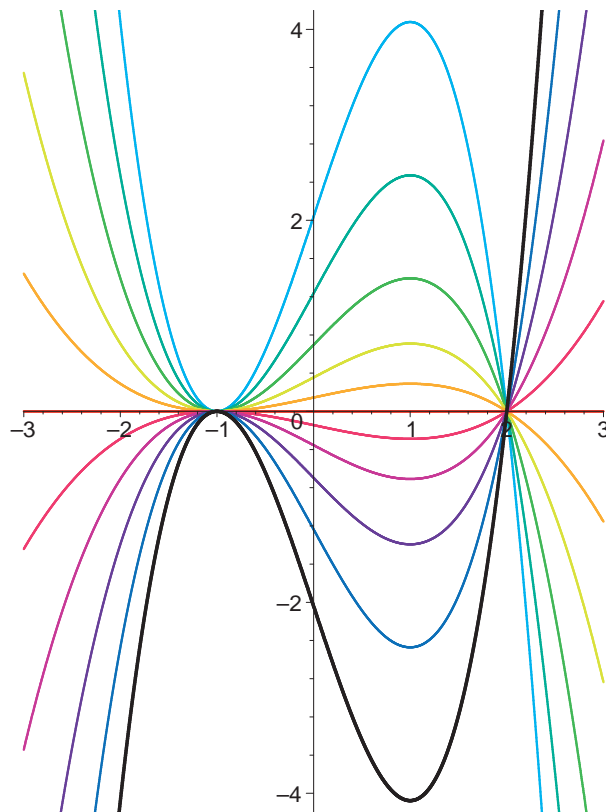


Abbildung 5.1: Kubische Polynome mit Nullstellen bei -1 und 2 und Wendepunkt bei 0

Für weitere Beispiele siehe Aufgabe 5.16.1.

Wir können M in Beispiel 5.2.11 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 : Summen und K -Vielfache von Lösungen sind wieder Lösungen. Eine Menge mit diesen Eigenschaften 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.

$$V = \{x_1 \cdot f_1 + \dots + x_r \cdot f_r \mid x_i \in K\}$$

mit geeigneten $f_i \in V$. Man bezeichnet dann f_1, \dots, 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 $1, t, t^2, \dots$ eine Basis, und somit hat $\mathbb{R}[t]$ unendliche Dimension.

Das Konzept der Vektorräume, Erzeugendensysteme und Basen wollen wir im folgenden Abschnitt allgemein einführen.

5.3 Vektorräume und Basen

Definition 5.3.1 Sei K ein Körper. Ein K -Vektorraum ist eine Menge V zusammen mit zwei Verknüpfungen

$$\begin{aligned} V \times V &\longrightarrow V && \text{(Addition)} \\ (v, w) &\longmapsto v + w \end{aligned}$$

$$\begin{aligned} K \times V &\longrightarrow V && \text{(Skalarmultiplikation)} \\ (\lambda, v) &\longmapsto \lambda \cdot v \end{aligned}$$

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

$$\begin{aligned} (\lambda + \mu) \cdot v &= \lambda \cdot v + \mu \cdot v \\ \lambda \cdot (v + w) &= \lambda \cdot v + \lambda \cdot w \end{aligned}$$

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 5.3.2 Sei K ein Körper. Beispiele von K -Vektorräumen sind:

1) $K^n = \{(a_1, \dots, a_n) \mid a_i \in K\}$ mit

$$(a_1, \dots, a_n) + (b_1, \dots, b_n) := (a_1 + b_1, \dots, a_n + b_n)$$

$$\lambda (a_1, \dots, a_n) := (\lambda a_1, \dots, \lambda a_n)$$

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

$$K^{\mathbb{N}} = \{a : \mathbb{N} \rightarrow K\}$$

mit

$$(a + b)(m) := a(m) + b(m)$$

$$(\lambda \cdot f)(m) := \lambda \cdot f(m)$$

für $m \in \mathbb{N}$.

Bemerkung 5.3.3 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) $\lambda \cdot v = 0 \implies \lambda = 0$ 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 5.1). 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 5.3.4 Wir geben Beispiele für die Aussagen in Bemerkung 5.3.3:

1)

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

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 5.3.5 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 5.3.3 im Allgemeinen nicht mehr korrekt ist. Beispielsweise ist $\mathbb{Z}/2$ ein \mathbb{Z} -Modul mit der Skalarmultiplikation

$$\begin{aligned} \mathbb{Z} \times \mathbb{Z}/2 &\rightarrow \mathbb{Z}/2 \\ (n, \bar{a}) &\mapsto n \cdot \bar{a} = \underbrace{\bar{a} + \dots + \bar{a}}_n = \overline{n \cdot a} \end{aligned}$$

und es gilt

$$2 \cdot \bar{1} = \bar{2} = \bar{0},$$

obwohl $2 \neq 0$ und $\bar{1} \neq 0$. 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

$$\begin{aligned} \mathbb{Z} \times G &\rightarrow G \\ (n, g) &\mapsto n \cdot g = \underbrace{g + \dots + g}_n \end{aligned}$$

eine \mathbb{Z} -Modulstruktur geben.

Summen und Vielfache von Lösungen von homogenen linearen Gleichungssystemen sind wieder Lösungen. Deshalb definieren wir:

Definition 5.3.6 Sei V ein K -Vektorraum. Eine nichtleere Teilmenge $U \subset V$ heißt **Untervektorraum**, wenn

$$\begin{aligned} u_1, u_2 \in U &\implies u_1 + u_2 \in U \\ \lambda \in K, u \in U &\implies \lambda \cdot u \in U. \end{aligned}$$

Bemerkung 5.3.7 1) U mit der von V induzierten Addition und Skalarmultiplikation ist ein K -Vektorraum (siehe Übung 5.1).

2) Jeder Untervektorraum U enthält die $0 \in V$ (denn es gibt ein $u \in U$ und $0 = 0 \cdot u \in U$).

Satz 5.3.8 Die Lösungsmenge eines homogenen linearen Gleichungssystems für x_1, \dots, x_n über dem Körper K ist ein Untervektorraum von K^n .

Beweis. Betrachte das System

$$\begin{aligned} a_{1,1}x_1 + \dots + a_{1,n}x_n &= 0 \\ &\vdots \\ a_{r,1}x_1 + \dots + a_{r,n}x_n &= 0 \end{aligned}$$

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 $i = 1, \dots, r$, 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

$$\sum_{j=1}^n a_{i,j}(\lambda \cdot x_j) = \lambda \cdot \sum_{j=1}^n a_{i,j}x_j = 0.$$

■

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 5.3.9 Eine Gerade $L \subset \mathbb{R}^n$ ist ein Untervektorraum genau dann, wenn $0 \in L$ (siehe Abbildung 5.2).

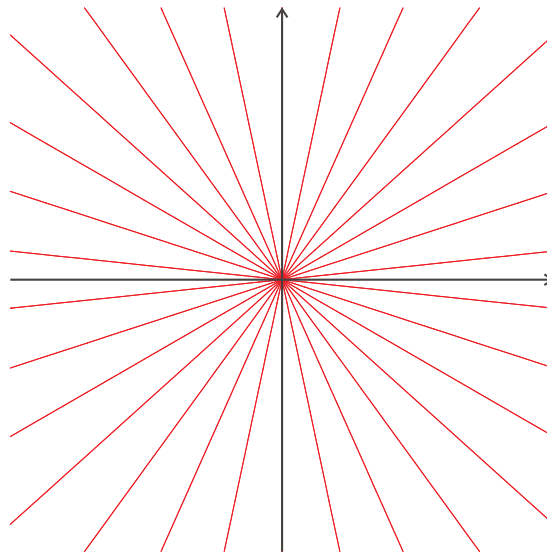


Abbildung 5.2: Geraden im \mathbb{R}^2 , die Untervektorräume sind

Beweis. Die Notwendigkeit von $0 \in L$ ist klar. Falls $0 \in L$, dann

$$L = \{\lambda v \mid \lambda \in \mathbb{R}\}$$

mit $0 \neq v \in L$. Somit ist

$$\lambda_1 v + \lambda_2 v = (\lambda_1 + \lambda_2) v \in L$$

$$\lambda_1 (\lambda_2 v) = (\lambda_1 \lambda_2) v \in L$$

für alle $\lambda_i \in \mathbb{R}$. ■

Beispiel 5.3.10 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

$$U_1 = \{(x, y) \in \mathbb{R}^2 \mid y \geq a\}$$

mit $a \in \mathbb{R}$ (siehe Abbildung 5.3 für $a = 0$) und

$$U_2 = \{(x, y) \in \mathbb{R}^2 \mid y = x^2\}$$

(siehe Abbildung 5.4) sind keine Untervektorräume von \mathbb{R}^2 . Warum?

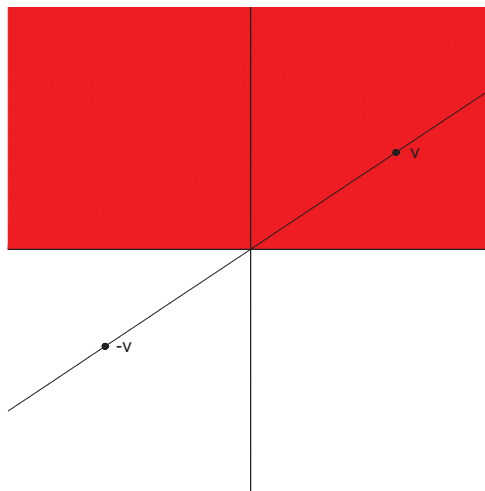


Abbildung 5.3: Halbebene

4) Sind $a_1, \dots, a_n \in K$, dann ist die Hyperebene

$$H = \{(x_1, \dots, x_n) \in K^n \mid a_1 x_1 + \dots + a_n x_n = 0\}$$

ein Untervektorraum. Dies haben wir schon allgemeiner in Bemerkung 5.3.8 für Lösungsmengen von homogenen linearen Gleichungssystemen beobachtet.

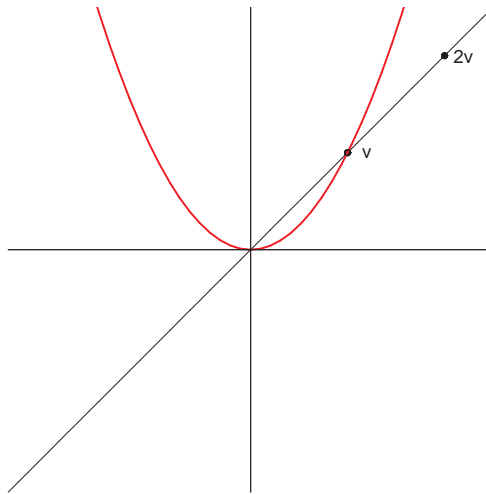


Abbildung 5.4: Parabel

Definition und Satz 5.3.11 Sei V ein K -Vektorraum und $v_1, \dots, v_n \in V$. Ein Vektor $v \in V$ ist eine **Linearkombination** von v_1, \dots, v_n , wenn es $\lambda_i \in K$ gibt mit

$$v = \lambda_1 v_1 + \dots + \lambda_n v_n.$$

Die Menge aller Linearkombinationen

$$\langle v_1, \dots, v_n \rangle := \{ \lambda_1 v_1 + \dots + \lambda_n v_n \mid \lambda_i \in K \} \subset V$$

ist ein Untervektorraum, der **von v_1, \dots, v_n aufgespannte Untervektorraum**.

Beweis. Sind $v, w \in \langle v_1, \dots, v_n \rangle$ 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

$$v + w = \sum_{i=1}^n (\lambda_i + \mu_i) v_i \in \langle v_1, \dots, v_n \rangle$$

und

$$\lambda v = \sum_{i=1}^n (\lambda \cdot \lambda_i) v_i \in \langle v_1, \dots, v_n \rangle.$$

■

Beispiel 5.3.12 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

$$\langle v_1, v_2 \rangle \subset \langle w_1, w_2 \rangle.$$

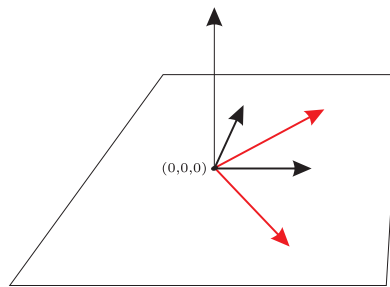
Siehe auch Abbildung 5.5.

2) Die Polynome $1, x, \dots, x^d \in K[x]$ spannen $K[x]_{\leq d}$ auf.

Definition 5.3.13 Sei V ein K -Vektorraum.

1) Vektoren $v_1, \dots, v_n \in V$ heißen ein **Erzeugendensystem** von V , wenn

$$V = \langle v_1, \dots, v_n \rangle.$$

Abbildung 5.5: Zwei Erzeugendensysteme der Ebene $\{z = 0\} \subset \mathbb{R}^3$

- 2) Vektoren $v_1, \dots, v_n \in V$ heißen **linear unabhängig**, wenn aus

$$\lambda_1 v_1 + \dots + \lambda_n v_n = 0$$

folgt, dass

$$\lambda_1 = \dots = \lambda_n = 0,$$

anderenfalls **linear abhängig**.

- 3) Ein Erzeugendensystem v_1, \dots, v_n von V aus linear unabhängigen Vektoren heißt **Basis** von V .

Algorithmus 5.3.14 Vektoren $v_1, \dots, v_n \in K^m$ sind linear unabhängig genau dann, wenn das homogene lineare Gleichungssystem

$$\lambda_1 v_1 + \dots + \lambda_n v_n = 0$$

nur die Lösung

$$\begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

hat. Dies können wir mit dem Gaußalgorithmus entscheiden.

Beispiel 5.3.15 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

$$\lambda_1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \lambda_2 \begin{pmatrix} 0 \\ 1 \end{pmatrix} + \lambda_3 \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

d.h.

$$\begin{array}{rcl} \lambda_1 & + & \lambda_3 = 0 \\ & \lambda_2 + & \lambda_3 = 0 \end{array}$$

hat den Lösungsraum

$$\left\{ \begin{pmatrix} -\lambda_3 \\ -\lambda_3 \\ \lambda_3 \end{pmatrix} \mid \lambda_3 \in \mathbb{R} \right\} \neq \left\{ \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \right\}$$

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**

$$e_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \dots, e_n = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \in K^n$$

bilden eine Basis von K^n , die sogenannte **Standardbasis**:
Jeder Vektor in K^n lässt sich schreiben als

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = a_1 e_1 + \dots + a_n e_n$$

und e_1, \dots, e_n sind linear unabhängig, denn

$$a_1 e_1 + \dots + a_n e_n = 0 \implies a_1 = \dots = a_n = 0$$

3) Die Polynome $1, x, \dots, x^d$ bilden eine Basis von $K[x]_{\leq d}$,
denn

$$a_0 \cdot 1 + \dots + a_d \cdot x^d = 0 \implies a_0 = \dots = a_d = 0.$$

Siehe auch Übungsaufgabe 5.4.

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 5.3.16 (Basis des Lösungsraums) Sei

$$\begin{aligned} l_1 &= x_{i_1} + t_{i_1}(x_{j_1}, \dots, x_{j_{n-r}}) = 0 \\ &\vdots \\ l_r &= x_{i_r} + t_{i_r}(x_{j_1}, \dots, x_{j_{n-r}}) = 0 \end{aligned}$$

mit $l_i \in K[x_1, \dots, x_n]$ homogen linear in reduzierter Zeilenstufenform mit **Leitvariablen**

$$x_{i_1}, \dots, x_{i_r}$$

und **freien Variablen**

$$x_{j_1}, \dots, x_{j_{n-r}}$$

(also $\{j_1, \dots, j_{n-r}\} = \{1, \dots, n\} \setminus \{i_1, \dots, i_r\}$). Mit

$$g_i := \begin{cases} -t_{i_i}(x_{j_1}, \dots, x_{j_{n-r}}) & \text{falls } x_i \text{ eine Leitvariable} \\ x_i & \text{falls } x_i \text{ eine freie Variable} \end{cases}$$

können wir die Lösungsmenge schreiben als

$$L = \left\{ \left(\begin{array}{c} g_1(x_{j_1}, \dots, x_{j_{n-r}}) \\ \vdots \\ g_n(x_{j_1}, \dots, x_{j_{n-r}}) \end{array} \right) \mid x_{j_1}, \dots, x_{j_{n-r}} \in K \right\}$$

Da die g_i homogene lineare Polynome in $x_{j_1}, \dots, x_{j_{n-r}}$ sind und somit

$$\left(\begin{array}{c} g_1(x_{j_1}, \dots, x_{j_{n-r}}) \\ \vdots \\ g_n(x_{j_1}, \dots, x_{j_{n-r}}) \end{array} \right) = x_{j_1} \cdot \left(\begin{array}{c} g_1(1, 0, \dots, 0) \\ \vdots \\ g_n(1, 0, \dots, 0) \end{array} \right) + \dots + x_{j_{n-r}} \cdot \left(\begin{array}{c} g_1(0, \dots, 0, 1) \\ \vdots \\ g_n(0, \dots, 0, 1) \end{array} \right)$$

erhalten wir ein Erzeugendensystem

$$L = \left\langle \left(\begin{array}{c} g_1(1, 0, \dots, 0) \\ \vdots \\ g_n(1, 0, \dots, 0) \end{array} \right), \dots, \left(\begin{array}{c} g_1(0, \dots, 0, 1) \\ \vdots \\ g_n(0, \dots, 0, 1) \end{array} \right) \right\rangle$$

Da in den Koordinaten $x_{j_1}, \dots, x_{j_{n-r}}$ der Erzeuger eine Einheitsbasis von K^{n-r} steht, sind diese linear unabhängig und bilden somit eine Basis von L .

Siehe auch Aufgabe 5.2.

Beispiel 5.3.17 *Das System*

$$\begin{array}{rclclcl} l_1 & = & \mathbf{x}_1 & + & 2x_2 & & - & 2x_5 & = & 0 \\ l_2 & = & & & & \mathbf{x}_3 & + & x_5 & = & 0 \\ l_3 & = & & & & & \mathbf{x}_4 & + & 2x_5 & = & 0 \end{array}$$

in $\mathbb{Q}[x]$ ist schon in reduzierter Zeilenstufenform, also die Lösungsmenge

$$V = \left\{ \left(\begin{array}{c} -2x_2 + 2x_5 \\ x_2 \\ -x_5 \\ -2x_5 \\ x_5 \end{array} \right) \mid x_2, x_5 \in \mathbb{Q} \right\}$$

und somit erhalten wir mit $(x_2, x_5) = (1, 0)$ und $(x_2, x_5) = (0, 1)$ eine Basis:

$$V = \left\langle \left(\begin{array}{c} -2 \\ 1 \\ 0 \\ 0 \\ 0 \end{array} \right), \left(\begin{array}{c} -2 \\ 0 \\ -1 \\ -2 \\ 1 \end{array} \right) \right\rangle$$

Wir überprüfen nochmals in diesem Spezialfall, dass es sich tatsächlich um eine Basis handelt: Jedes Element von V lässt sich als eindeutige Linearkombination darstellen

$$\left(\begin{array}{c} -2x_2 + 2x_5 \\ x_2 \\ -x_5 \\ -2x_5 \\ x_5 \end{array} \right) = x_2 \cdot \left(\begin{array}{c} -2 \\ 1 \\ 0 \\ 0 \\ 0 \end{array} \right) + x_5 \cdot \left(\begin{array}{c} -2 \\ 0 \\ -1 \\ -2 \\ 1 \end{array} \right)$$

und die Vektoren sind linear unabhängig, denn

$$x_2 \cdot \left(\begin{array}{c} -2 \\ \mathbf{1} \\ 0 \\ 0 \\ \mathbf{0} \end{array} \right) + x_5 \cdot \left(\begin{array}{c} -2 \\ \mathbf{0} \\ -1 \\ -2 \\ \mathbf{1} \end{array} \right) = \left(\begin{array}{c} 0 \\ \mathbf{0} \\ 0 \\ 0 \\ \mathbf{0} \end{array} \right) \implies \begin{array}{l} x_2 = 0 \\ x_5 = 0 \end{array}$$

Für weitere Beispiele siehe auch die Aufgaben 5.16.1 und 5.16.2.

5.4 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 5.4.1 *Sei V ein K -Vektorraum und $\Omega = (v_1, \dots, v_n)$ 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

$$v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_n$$

sind auch ein Erzeugendensystem von V . Dann ist insbesondere

$$v_i = \lambda_1 v_1 + \dots + \lambda_{i-1} v_{i-1} + \lambda_{i+1} v_{i+1} + \dots + \lambda_n v_n$$

eine Linearkombination mit $\lambda_j \in K$, also

$$\lambda_1 v_1 + \dots + \lambda_{i-1} v_{i-1} - v_i + \lambda_{i+1} v_{i+1} + \dots + \lambda_n v_n = 0,$$

ein Widerspruch zur linearen Unabhängigkeit von v_1, \dots, v_n .

(2 \Rightarrow 3): Wir zeigen zunächst, dass v_1, \dots, v_n linear unabhängig sind. Angenommen

$$\lambda_1 v_1 + \dots + \lambda_n v_n = 0$$

und $\lambda_i \neq 0$. Dann ist

$$v_i = \frac{1}{\lambda_i} (\lambda_1 v_1 + \dots + \lambda_{i-1} v_{i-1} + \lambda_{i+1} v_{i+1} + \dots + \lambda_n v_n)$$

also $v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_n$ ein kürzeres Erzeugendensystem von V (d.h. eines mit weniger Elementen), ein Widerspruch zu (2).

Da nach (2) die Vektoren v_1, \dots, v_n den Vektorraum V erzeugen, wäre jedes weitere $v \in V$ eine Linearkombination von v_1, \dots, v_n und somit v_1, \dots, v_n, v linear abhängig.

(3 \Rightarrow 4): Wir zeigen, dass v_1, \dots, v_n ein Erzeugendensystem von V sind: Sei $v \in V$ beliebig. Nach Voraussetzung sind v_1, \dots, v_n, v linear abhängig, also gibt es $\lambda_i, \lambda \in K$, nicht alle 0, mit

$$\lambda_1 v_1 + \dots + \lambda_n v_n + \lambda v = 0.$$

Angenommen $\lambda = 0$. Dann ist $\lambda_1 v_1 + \dots + \lambda_n v_n = 0$, wegen v_1, \dots, v_n linear unabhängig also auch $\lambda_1 = \dots = \lambda_n = 0$, ein Widerspruch. Somit lässt sich v darstellen als

$$v = \frac{\lambda_1}{\lambda} v_1 + \dots + \frac{\lambda_n}{\lambda} v_n.$$

Zum Beweis der Eindeutigkeit nehmen wir an, dass

$$\lambda_1 v_1 + \dots + \lambda_n v_n = v = \mu_1 v_1 + \dots + \mu_n v_n$$

also

$$(\lambda_1 - \mu_1) v_1 + \dots + (\lambda_n - \mu_n) v_n = 0.$$

Da v_1, \dots, v_n linear unabhängig sind, folgt $\lambda_i = \mu_i \forall i$.

(4 \Rightarrow 1): Nach Voraussetzung ist v_1, \dots, v_n ein Erzeugendensystem. Wären die Vektoren linear abhängig, dann gäbe es zwei unterschiedliche Darstellungen der 0

$$\lambda_1 v_1 + \dots + \lambda_n v_n = 0 = 0v_1 + \dots + 0v_n.$$

■

Aus einem Erzeugendensystem können wir also durch sukzessives Weglassen von Erzeugern ein unverkürzbares Erzeugendensystem, d.h. eine Basis, erhalten:

Corollar 5.4.2 (Basisauswahlsatz) *Ist V ein K -Vektorraum und v_1, \dots, v_m ein Erzeugendensystem von V , dann gibt es $i_1, \dots, i_n \in \{1, \dots, m\}$, sodass v_{i_1}, \dots, v_{i_n} eine Basis von V bilden.*

Siehe auch Übungsaufgabe 5.7.

Beispiel 5.4.3 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.

$$\begin{array}{rcccc} \lambda_1 & & + & \lambda_3 & = & 0 \\ & \lambda_2 & + & \lambda_3 & = & 0 \\ & & & & \lambda_4 & = & 0 \end{array}$$

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, \dots, 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

$$1, (x-b), (x-b)^2, \dots, (x-b)^d$$

eine Basis von $\mathbb{R}[x]_{\leq d}$ (siehe Übungsaufgabe 5.5). Insbesondere für $b = 0$ erhalten wir die Standardbasis $1, x, \dots, x^d$.

Die Anzahl der Basiselemente ist jedoch von der Wahl der Basis unabhängig. Dies werden wir im folgenden Satz zeigen.

Definition 5.4.4 *Ein Vektorraum heißt **endlichdimensional**, wenn er ein endliches Erzeugendensystem besitzt.*

Mit dem Basisauswahlsatz 5.4.2 hat der Vektorraum dann auch eine (endliche) Basis.

Definition und Satz 5.4.5 (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 5.4.6 *Mit Satz 5.4.5 und den Basen aus Beispiel 5.3.15 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 $\mathbb{Q}^n \rightarrow \mathbb{R}$. 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 5.4.5 beruht auf folgendem Lemma:

Lemma 5.4.7 (Austauschlemma) *Sei v_1, \dots, v_n eine Basis von V und $0 \neq w \in V$ ein weiterer Vektor. Dann existiert ein $i \in \{1, \dots, n\}$, sodass auch $v_1, \dots, v_{i-1}, w, v_{i+1}, \dots, v_n$ eine Basis von V bilden.*

Beweis. Da v_1, \dots, v_n ein Erzeugendensystem sind, gibt es $\lambda_1, \dots, \lambda_n \in K$ mit

$$w = \lambda_1 v_1 + \dots + \lambda_n v_n.$$

Hier muss ein $\lambda_i \neq 0$ sein, da $w \neq 0$. Nach Umm nummerieren können wir $\lambda_1 \neq 0$ annehmen. Also ist

$$v_1 = \frac{1}{\lambda_1} (w - (\lambda_2 v_2 + \dots + \lambda_n v_n))$$

eine Linearkombination von w, v_2, \dots, 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

$$\mu w + \mu_2 v_2 + \dots + \mu_n v_n = 0,$$

also

$$\mu \lambda_1 v_1 + (\mu_2 + \mu \lambda_2) v_2 + \dots + (\mu_n + \mu \lambda_n) v_n = 0.$$

Da v_1, \dots, v_n linear unabhängig sind, gilt

$$\mu \lambda_1 = \mu_2 + \mu \lambda_2 = \dots = \mu_n + \mu \lambda_n = 0$$

Aus $\lambda_1 \neq 0$ folgt $\mu = 0$ und somit $\mu_2 = \dots = \mu_n = 0$. ■

Beispiel 5.4.8 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 5.4.9 (Austauschsatz) Sei V ein K -Vektorraum, v_1, \dots, v_n eine Basis von V und w_1, \dots, w_s linear unabhängig. Dann gilt

$$s \leq n.$$

Weiter gibt es $i_1, \dots, i_{n-s} \in \{1, \dots, n\}$, sodass

$$w_1, \dots, w_s, v_{i_1}, \dots, v_{i_{n-s}}$$

eine Basis von V bilden.

Beweis. Für $s = 1$ ist dies Lemma 5.4.7. Induktionsschritt $s-1 \mapsto s$: Nach Induktionsvoraussetzung können wir w_1, \dots, 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

$$w_s = \lambda_1 w_1 + \dots + \lambda_{s-1} w_{s-1} + \lambda_s v_s + \dots + \lambda_n v_n.$$

Wären $\lambda_s = \dots = \lambda_n = 0$, 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 5.4.7 gegen w_s austauschen. ■

Insbesondere erhalten wir:

Corollar 5.4.10 (Basisergänzungssatz) *Ist V ein endlichdimensionaler K -Vektorraum und v_1, \dots, v_m linear unabhängig. Dann gibt es $v_{m+1}, \dots, v_n \in V$, sodass v_1, \dots, v_n eine Basis bilden.*

Beweis. Nach Corollar 5.4.2 hat V eine Basis und nach Satz 5.4.9 lassen sich in der Basis Vektoren durch v_1, \dots, v_m austauschen. ■

Der Austauschsatz impliziert auch direkt Satz 5.4.5:

Beweis. Satz 5.4.9 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 5.4.11 *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

$$x + 1 = \underset{\neq 0}{2} \cdot 1 + 1 \cdot (x^2 + x) + (-1) \cdot (x^2 + 1).$$

Aus dem Austauschsatz folgt auch:

Corollar 5.4.12 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, \dots, v_n eine Basis von V und w_1, \dots, w_s eine Basis von U , so gilt $s \leq n$ mit Satz 5.4.9.

Für $s = n$ lassen sich v_1, \dots, v_n mit Satz 5.4.9 vollständig gegen w_1, \dots, w_n austauschen. Somit bilden w_1, \dots, w_n eine Basis. ■

Bemerkung 5.4.13 Sei V ein Vektorraum der Dimension $n < \infty$ und $v_1, \dots, v_n \in V$. Dann sind äquivalent:

- 1) v_1, \dots, v_n bilden eine Basis,
- 2) v_1, \dots, v_n sind linear unabhängig,
- 3) v_1, \dots, v_n sind ein Erzeugendensystem von V .

Beweis. Seien v_1, \dots, v_n linear unabhängig. Dann bilden v_1, \dots, v_n eine Basis von $U = \langle v_1, \dots, v_n \rangle$ und somit ist

$$\dim U = n = \dim V$$

also mit Corollar 5.4.12 $U = V$.

Seien v_1, \dots, v_n ein Erzeugendensystem von V . Somit können wir v_1, \dots, v_n mit Corollar 5.4.2 zu einer Basis verkürzen. Wäre die Basis echt kürzer, dann wäre $\dim V < n$, ein Widerspruch. Also sind v_1, \dots, v_n ein unverkürzbares Erzeugendensystem, d.h. nach Satz 5.4.1 eine Basis. ■

5.5 Vektorraumhomomorphismen

Um mit Elementen eines K -Vektorraums V im Computer rechnen zu können, muss man eine geeignete Darstellung von Vektoren finden. Dazu wählt man eine Basis $\Omega = (v_1, \dots, v_n)$ von V . Nach Satz 5.4.1 hat jedes $v \in V$ eine eindeutige Darstellung

$$v = a_1v_1 + \dots + a_nv_n$$

mit $a_i \in K$. Wir können also v im Computer durch

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \in K^n$$

repräsentieren. Anders ausgedrückt, die **Linearkombinationsabbildung**

$$\begin{aligned} \text{lc}_\Omega : K^n &\longrightarrow V \\ \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} &\longmapsto a_1v_1 + \dots + a_nv_n \end{aligned}$$

ist bijektiv. Ihre Umkehrabbildung

$$\text{co}_\Omega = \text{lc}_\Omega^{-1} : V \longrightarrow K^n$$

bezeichnen wir als **Koordinatendarstellung** bezüglich Ω . Vom praktischen Standpunkt können wir uns co_Ω als Parser und lc_Ω als Ausgaberoutine vorstellen.

Beispiel 5.5.1 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

$$\begin{aligned} \text{lc}_\Omega : K^3 &\longrightarrow K[x]_{\leq 2} \\ \begin{pmatrix} a_0 \\ a_1 \\ a_2 \end{pmatrix} &\longmapsto a_0 + a_1x + a_2x^2 \end{aligned}$$

Somit ist z.B. die Koordinatendarstellung des Polynoms $3x^2 + x$

$$\text{co}_\Omega(3x^2 + x) = \begin{pmatrix} 0 \\ 1 \\ 3 \end{pmatrix}$$

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

$$\begin{aligned} \text{lc}_\Omega \left(\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} + \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \right) &= \text{lc}_\Omega \begin{pmatrix} a_1 + b_1 \\ \vdots \\ a_n + b_n \end{pmatrix} = \sum_{i=1}^n (a_i + b_i) v_i \\ &= \sum_{i=1}^n a_i v_i + \sum_{i=1}^n b_i v_i = \text{lc}_\Omega \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} + \text{lc}_\Omega \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \end{aligned}$$

und

$$\begin{aligned} \text{lc}_\Omega \left(\lambda \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \right) &= \text{lc}_\Omega \begin{pmatrix} \lambda a_1 \\ \vdots \\ \lambda a_n \end{pmatrix} = \sum_{i=1}^n (\lambda a_i) v_i \\ &= \lambda \sum_{i=1}^n a_i v_i = \lambda \cdot \text{lc}_\Omega \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}. \end{aligned}$$

Das heißt, dass lc_Ω ein Homomorphismus von Vektorräumen ist:

Definition 5.5.2 *Ein K -Vektorraumhomomorphismus ist eine K -lineare Abbildung $F: V \rightarrow W$ 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 5.5.3 1) Analog können wir die Linearkombinationsabbildung lc_Ω auch für eine beliebige Liste $\Omega = (v_1, \dots, v_n)$ von Vektoren in V definieren, nach unserem obigen Beweis ist sie immer noch ein Homomorphismus, aber i.A. weder

injektiv noch surjektiv. Es gilt offenbar:

$$\begin{aligned} \text{lc}_\Omega \text{ Epimorphismus} &\Leftrightarrow \Omega \text{ Erzeugendensystem von } V \\ \text{lc}_\Omega \text{ Monomorphismus} &\Leftrightarrow \Omega \text{ linear unabhängig} \\ \text{lc}_\Omega \text{ Isomorphismus} &\Leftrightarrow \Omega \text{ Basis von } V \end{aligned}$$

Man zeigt wie üblich, dass mit lc_Ω auch $\text{co}_\Omega = \text{lc}_\Omega^{-1}$ ein Isomorphismus ist.

2) Insbesondere ist z.B.

$$\begin{aligned} \text{lc}_{(1,x,\dots,x^d)} : K^{d+1} &\longrightarrow K[x]_{\leq d} \\ \begin{pmatrix} a_0 \\ \vdots \\ a_d \end{pmatrix} &\longmapsto a_0 + a_1x + \dots + a_dx^d \end{aligned}$$

ein K -Vektorraumisomorphismus.

Die Klassifikation von endlichdimensionalen Vektorräumen bis auf Isomorphie ist sehr einfach, die Dimension ist dafür schon ausreichend:

Satz 5.5.4 (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 Definition und Satz 5.4.5 hat V eine Basis $\Omega = (v_1, \dots, v_n)$, und nach Beispiel 5.5.3.(1) ist

$$\text{lc}_\Omega : K^n \rightarrow V$$

ein Isomorphismus. ■

Definition und Satz 5.5.5 Eine $n \times m$ -**Matrix** A über K ist eine Tabelle

$$A = \begin{pmatrix} a_{1,1} & \cdots & a_{1,m} \\ \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,m} \end{pmatrix} = (a_{i,j})_{\substack{i=1,\dots,n \\ j=1,\dots,m}}$$

Die Menge der $n \times m$ -Matrizen bezeichnen wir mit $K^{n \times m}$.

Durch die **Matrixmultiplikation**

$$\begin{pmatrix} a_{11} & \cdots & a_{1,m} \\ \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,m} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} := \begin{pmatrix} (\sum_{j=1}^m a_{1,j}x_j) \\ \vdots \\ (\sum_{j=1}^m a_{n,j}x_j) \end{pmatrix}$$

ist ein Vektorraumhomomorphismus

$$K^m \rightarrow K^n, x \mapsto A \cdot x$$

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 $A = (A_1 \mid \dots \mid A_m)$, d.h.

$$(A_1 \mid \dots \mid A_m) \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = \sum_{j=1}^m x_j \cdot A_j.$$

Beweis. Die Abbildung $A = \text{lc}_{(A_1, \dots, A_m)}$, sie ist also eine Linearkombinationsabbildung und somit wie oben bemerkt ein Homomorphismus. ■

Beispiel 5.5.6 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 5.5.7 Die Ableitung

$$\frac{d}{dx} : \mathbb{R}[x] \longrightarrow \mathbb{R}[x]$$

ist ein \mathbb{R} -Vektorraumhomomorphismus, da

$$\frac{d}{dx} \left(\sum_{i=0}^d a_i x^i \right) = \sum_{i=1}^d i a_i x^{i-1}$$

also das Bild linear von den Koeffizienten a_i von p abhängt. Sie ist kein Monomorphismus, denn z.B.

$$\frac{d}{dx}0 = \frac{d}{dx}1,$$

aber ein Epimorphismus, denn

$$\frac{d}{dx} \left(\sum_{i=0}^d \frac{a_i}{i+1} x^{i+1} \right) = \sum_{i=0}^d a_i x^i,$$

d.h. jedes Polynom besitzt eine Stammfunktion.

Lemma 5.5.8 Sei $F : V \rightarrow W$ ein Vektorraumhomomorphismus. Dann sind $\text{Ker}(F) \subset V$ und $\text{Bild}(F) \subset W$ Untervektorräume. Die Dimension des Bildes bezeichnen wir auch als **Rang** von F

$$\text{rk}(F) := \dim \text{Bild}(F).$$

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 5.5.9 Da ein Vektorraumhomomorphismus $F : V \rightarrow W$ insbesondere ein Gruppenhomomorphismus $(V, +) \rightarrow (W, +)$ ist, gilt nach Lemma 3.2.13, dass

$$F \text{ Monomorphismus} \iff \text{Ker}(F) = \{0\},$$

wobei $\text{Ker}(F) = \{v \in V \mid F(v) = 0\}$.

In Verallgemeinerung von 5.5.3.(1) haben wir:

Bemerkung 5.5.10 Sei $F : V \rightarrow W$ ein Homomorphismus, $\Omega = (v_1, \dots, v_n)$ eine Basis von V und $\Delta = (F(v_1), \dots, F(v_n))$ das Bild von Ω unter F . Dann gilt

$$\begin{aligned} F \text{ Epimorphismus} &\iff \Delta \text{ Erzeugendensystem von } W \\ F \text{ Monomorphismus} &\iff \Delta \text{ linear unabhängig} \\ F \text{ Isomorphismus} &\iff \Delta \text{ Basis von } W \end{aligned}$$

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

$$\begin{aligned} \text{Bild}(F) &= \{F(\sum_{i=1}^n \lambda_i v_i) \mid \lambda_i \in K\} \\ &= \{\sum_{i=1}^n \lambda_i F(v_i) \mid \lambda_i \in K\}. \end{aligned}$$

Somit ist $\text{Bild}(F) = W$ genau dann, wenn die $F(v_i)$ ein Erzeugendensystem bilden.

Weiter ist

$$\begin{aligned} \text{Ker}(F) &= \{\sum_{i=1}^n \lambda_i v_i \mid F(\sum_{i=1}^n \lambda_i v_i) = 0, \lambda_i \in K\} \\ &= \{\sum_{i=1}^n \lambda_i v_i \mid \sum_{i=1}^n \lambda_i F(v_i) = 0, \lambda_i \in K\} \end{aligned}$$

Somit ist $\text{Ker}(F) = \{0\}$ 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:

$$\begin{aligned} F \text{ Epimorphismus} &\Rightarrow \dim V \geq \dim W \\ F \text{ Monomorphismus} &\Rightarrow \dim V \leq \dim W \\ F \text{ Isomorphismus} &\Rightarrow \dim V = \dim W \end{aligned}$$

5.6 Inhomogene lineare Gleichungssysteme

In vielen praktischen Anwendungen möchte man (in Verallgemeinerung von homogenen linearen Gleichungssystemen) **inhomogene lineare Gleichungssysteme** der Form

$$\begin{aligned} a_{1,1}x_1 + \dots + a_{1,m}x_m &= b_1 \\ &\vdots \\ a_{n,1}x_1 + \dots + a_{n,m}x_m &= b_n \end{aligned} \tag{5.1}$$

lösen.

Beispiel 5.6.1 (Lagrange-Interpolation) *Will man alle*

$$f = x_1 t^3 + x_2 t^2 + x_3 t + x_4 \in \mathbb{R}[t]_{\leq 3}$$

finden mit

$$f(-1) = 1, f(0) = 0, f(2) = 1,$$

so muss man

$$\begin{array}{rccccrcr} -x_1 & + & x_2 & - & x_3 & + & x_4 & = & 1 \\ & & & & & & x_4 & = & 0 \\ 8x_1 & + & 4x_2 & + & 2x_3 & + & x_4 & = & 1 \end{array}$$

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 (5.1) mit Hilfe der Matrixmultiplikation auch übersichtlich schreiben als

$$A \cdot x = b$$

wobei $x = (x_j) \in K^m$.

Beispiel 5.6.2 Das Gleichungssystem aus Beispiel 5.6.1 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 5.6.3 Wir bezeichnen die Lösungsmenge von $A \cdot x = b$ mit

$$L(A, b) = \{x \in K^m \mid A \cdot x = b\}.$$

Bemerkung 5.6.4 Mit dem durch die Matrix $A \in K^{n \times m}$ definierten Vektorraumhomomorphismus

$$A: K^m \rightarrow K^n$$

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 5.6.5 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

$$L = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix} + x_2 \begin{pmatrix} -2 \\ 1 \end{pmatrix} \mid x_2 \in \mathbb{R} \right\} \subset \mathbb{R}^2$$

in Abbildung 5.6. Mit

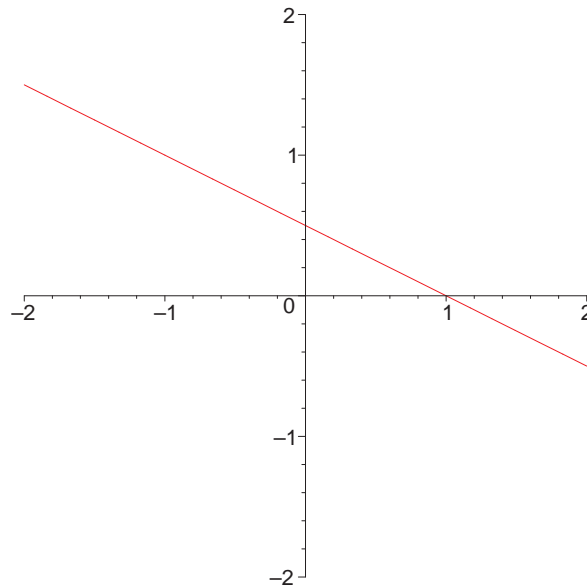


Abbildung 5.6: Affine Gerade

$$c = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ und } U = \left\langle \begin{pmatrix} -2 \\ 1 \end{pmatrix} \right\rangle \subset \mathbb{R}^2$$

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 5.6.6 Ein **affiner Unterraum** von V ist eine Nebenklasse

$$\bar{v} = v + U$$

eines Untervektorraums $U \subset V$. Dabei bezeichnen wir den Repräsentanten $v \in V$ als den **Aufpunkt**. Jedes Element von \bar{v} ist ein valider Aufpunkt, denn \bar{v} ist eine Äquivalenzklasse.

Bemerkung 5.6.7 Ein affiner Unterraum ist ein Untervektorraum genau dann, wenn er 0 enthält.

Lösungsmengen von inhomogenen linearen Gleichungssystemen sind affine Unterräume:

Satz 5.6.8 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 $b \in \text{Bild}(A)$, 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

$$L(A, b) = c + \text{Ker}(A) \subset K^m.$$

Beweis. Zu (1): $\text{Bild}(A) = \{A \cdot x \mid x \in K^m\}$

Zu (2): Für $v \in \text{Ker}(A)$ ist

$$A \cdot (c + v) = A \cdot c + 0 = b$$

Gilt umgekehrt $A \cdot x = b$, dann ist $A \cdot (x - c) = 0$, also $x - c \in \text{Ker}(A)$.

■

Wie bestimmt man nun $L(A, b)$ praktisch? Dazu führen wir das Lösen des inhomogenen Gleichungssystems

$$A \cdot x = b$$

für $x_1, \dots, x_m \in K$ 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 5.2 auf reduzierte Zeilenstufenform und bestimmen dann mit Bemerkung 5.3.16 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 5.3.16 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 5.3). 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.

Algorithmus 5.3 Löse inhomogenes lineares Gleichungssystem**Input:** $A \in K^{n \times m}$, $b \in K^n$ **Output:** $L(A, b)$ 1: Bestimme mit Bemerkung 5.3.16 eine Basis von $\ker(A \mid -b)$

$$\begin{pmatrix} c_1 \\ d_1 \end{pmatrix}, \dots, \begin{pmatrix} c_r \\ d_r \end{pmatrix}$$

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** $L(A, b) = \emptyset$

- Ist x_{m+1} eine freie Variable in

$$A \cdot x - b \cdot x_{m+1} = 0$$

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 5.6.8.

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 5.6.9 Für die Gleichung

$$x_1 + 2x_2 = 1$$

aus Beispiel 5.6.5 erhalten wir die homogenisierte Gleichung

$$x_1 + 2x_2 - x_3 = 0.$$

Diese ist als einzelne Gleichung schon in reduzierter Zeilenstufenform, hat Leitvariable x_1 , 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 5.6.10 Im Fall von Beispiel 5.6.1 bestimmen wir im Algorithmus für das homogenisierte System

$$\begin{array}{rcccccc} -x_1 & + & x_2 & - & x_3 & + & x_4 & - & x_5 & = & 0 \\ & & & & & & x_4 & & & = & 0 \\ 8x_2 & + & 4x_2 & + & 2x_3 & + & x_4 & - & x_5 & = & 0 \end{array}$$

die reduzierte Zeilenstufenform

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

und erhalten damit die Basis des Lösungsraums

$$\left(\begin{pmatrix} -\frac{1}{2} \\ \frac{1}{2} \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} -\frac{1}{4} \\ \frac{3}{4} \\ 0 \\ 0 \\ 1 \end{pmatrix} \right)$$

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 5.6.1 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 5.17, 5.18 und 5.11.

5.7 Darstellende Matrix eines Homomorphismus

Im letzten Abschnitt haben wir gesehen, dass sich durch Matrixmultiplikation gegebene Homomorphismen $A: K^m \rightarrow K^n$ 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 5.7.1 Sei $F: V \rightarrow W$ ein K -Vektorraumhomomorphismus. Für Basen $\Omega = (v_1, \dots, v_m)$ von V und $\Delta = (w_1, \dots, w_n)$ von W definiere den K -Vektorraumhomomorphismus

$$M_{\Delta}^{\Omega}(F): K^m \rightarrow K^n$$

durch

$$M_{\Delta}^{\Omega}(F) := \text{co}_{\Delta} \circ F \circ \text{lc}_{\Omega}.$$

Wir haben also ein Diagramm

$$\begin{array}{ccccc} & V & \xrightarrow{F} & W & \\ \text{lc}_\Omega & \uparrow & & \uparrow & \text{lc}_\Delta \\ & K^m & \xrightarrow{M_\Delta^\Omega(F)} & K^n & \end{array}$$

Wegen

$$F = \text{lc}_\Delta \circ M_\Delta^\Omega(F) \circ \text{co}_\Omega$$

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 Ausgaberroutine lc_Δ . Entscheidend für dieses Verfahrens ist, dass sich $M_\Delta^\Omega(F)$ durch Matrixmultiplikation darstellen lässt:

Satz 5.7.2 Sei $F : K^m \rightarrow K^n$ 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

$$A = (F(e_1) \mid \dots \mid F(e_m))$$

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

$$\begin{aligned} F(c) &= F\left(\sum_{j=1}^m c_j e_j\right) = \sum_{j=1}^m c_j F(e_j) = \sum_{j=1}^m c_j \sum_{i=1}^n a_{i,j} e_i \\ &= \sum_{i=1}^n \left(\sum_{j=1}^m a_{i,j} c_j\right) e_i = \begin{pmatrix} \left(\sum_{j=1}^m a_{1,j} c_j\right) \\ \vdots \\ \left(\sum_{j=1}^m a_{n,j} c_j\right) \end{pmatrix} = A \cdot c. \end{aligned}$$

■

Jeder Homomorphismus $F : K^m \rightarrow K^n$ ist also gegeben durch Multiplikation mit einer $n \times m$ -Matrix A .

Definition 5.7.3 Für einen K -Vektorraumhomomorphismus $F: V \rightarrow W$ und Basen $\Omega = (v_1, \dots, v_m)$ von V und $\Delta = (w_1, \dots, w_n)$ 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 5.7.4 In der i -ten Spalte von $M_\Delta^\Omega(F)$ stehen die Koeffizienten der Darstellung von $F(v_i)$ bezüglich der Basis Δ .

Beweis. Die i -te Spalte von $M_\Delta^\Omega(F)$ ist

$$M_\Delta^\Omega(F)(e_i) = (\text{co}_\Delta \circ F \circ \text{lc}_\Omega)(e_i) = (\text{co}_\Delta \circ F)(v_i) = \text{co}_\Delta(F(v_i)),$$

also

$$M_\Delta^\Omega(F) = (\text{co}_\Delta(F(v_1)) \mid \dots \mid \text{co}_\Delta(F(v_m))) \in K^{n \times m}$$

■

Beispiel 5.7.5 Betrachte die Ableitung

$$\frac{d}{dx} : \mathbb{R}[x]_{\leq 3} \rightarrow \mathbb{R}[x]_{\leq 2}$$

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

$$M_\Delta^\Omega\left(\frac{d}{dx}\right) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}.$$

Damit berechnen wir z.B.

$$\begin{aligned} \frac{d}{dx}(x^3 - 5x^2 + 7x - 11) &= \text{lc}_\Delta \left(M_\Delta^\Omega\left(\frac{d}{dx}\right) \cdot \text{co}_\Omega(x^3 - 5x^2 + 7x - 11) \right) \\ &= \text{lc}_\Delta \left(\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix} \cdot \begin{pmatrix} -11 \\ 7 \\ -5 \\ 1 \end{pmatrix} \right) \\ &= \text{lc}_\Delta \begin{pmatrix} 7 \\ -10 \\ 3 \end{pmatrix} = 3x^2 - 10x + 7 \end{aligned}$$

Siehe auch die Übungsaufgaben 5.13 und 5.12.

Die Implementierung eines K -Vektorraumhomomorphismus $F : V \rightarrow W$ 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 5.5.5 spaltenweise zu verwenden:

Definition 5.7.6 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 5.9 und 5.15.

Satz 5.7.7 Betrachte folgende K -Vektorraumhomomorphismen

$$\begin{array}{ccccc} V & \xrightarrow{F} & W & \xrightarrow{G} & U \\ \text{lc}_\Omega \uparrow & & \text{lc}_\Delta \uparrow & & \uparrow \text{lc}_\Gamma \\ K^r & \xrightarrow{M_\Delta^\Omega(F)} & K^m & \xrightarrow{M_\Gamma^\Delta(G)} & K^n \end{array}$$

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 5.7.8 Für

$$F = \frac{d}{dx} : \mathbb{R}[x]_{\leq 3} \rightarrow \mathbb{R}[x]_{\leq 2}$$

$$G = \frac{d}{dx} : \mathbb{R}[x]_{\leq 2} \rightarrow \mathbb{R}[x]_{\leq 1}$$

und $\Omega = (1, x, x^2, x^3)$, $\Delta = (1, x, x^2)$, $\Gamma = (1, x)$ erhalten wir

$$M_{\Sigma}^{\Omega}(G \circ F) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 6 \end{pmatrix}$$

das heißt für die zweite Ableitung $\left(\frac{d}{dx}\right)^2 = G \circ F$ gilt

$$\left(\frac{d}{dx}\right)^2 1 = 0 \quad \left(\frac{d}{dx}\right)^2 x = 0 \quad \left(\frac{d}{dx}\right)^2 x^2 = 2 \quad \left(\frac{d}{dx}\right)^2 x^3 = 6x.$$

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 5.7.9 Die Menge der $n \times m$ -Matrizen $K^{n \times m}$ ist ein K -Vektorraum durch

$$\begin{aligned} (a_{i,j}) + (b_{i,j}) &= (a_{i,j} + b_{i,j}) \\ \lambda \cdot (a_{i,j}) &= (\lambda a_{i,j}) \end{aligned}$$

ebenso die Menge

$$\text{Hom}_K(V, W) = \{F : V \rightarrow W \mid F \text{ Vektorraumhomomorphismus}\}$$

der K -Vektorraumhomomorphismen $V \rightarrow W$ durch

$$\begin{aligned} (f + g)(v) &= f(v) + g(v) \\ (\lambda \cdot f)(v) &= \lambda \cdot f(v) \end{aligned}$$

für $f, g \in \text{Hom}_K(V, W)$, $v \in V$ und $\lambda \in K$.

Bemerkung 5.7.10 Mit Satz 5.7.2 folgt dann (leichte Übung)

$$\text{Hom}_K(K^m, K^n) \cong K^{n \times m}, \quad F \mapsto (a_{i,j}),$$

wobei

$$F(e_j) = \sum_{i=1}^n a_{i,j} e_i$$

für $j = 1, \dots, m$.

Bemerkung 5.7.11 *Mit dieser Identifikation und Definition 5.7.1 erhalten wir, dass für Basen $\Omega = (v_1, \dots, v_m)$ von V und $\Delta = (w_1, \dots, w_n)$ von W*

$$M_{\Delta}^{\Omega}: \begin{array}{ccc} \text{Hom}_K(V, W) & \cong & K^{n \times m} \\ F & \mapsto & M_{\Delta}^{\Omega}(F) \end{array}$$

ein Isomorphismus ist. Die Umkehrabbildung

$$L_{\Delta}^{\Omega}: \begin{array}{ccc} K^{n \times m} & \cong & \text{Hom}_K(V, W) \\ A & \mapsto & L_{\Delta}^{\Omega}(A) \end{array}$$

ordnet einer Matrix $A = (a_{ij}) \in K^{n \times m}$ die lineare Abbildung

$$L_{\Delta}^{\Omega}(A): \begin{array}{ccc} V & \rightarrow & W \\ v & \mapsto & \text{lc}_{\Delta}(A \cdot \text{co}_{\Omega}(v)) \end{array}$$

zu (siehe Beispiel 5.7.5). Für die Details siehe Übungsaufgabe 5.14.

5.8 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 5.6 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

$$\left. \begin{array}{l} a_{1,1}x_1 + \dots + a_{1,m}x_m = 0 \\ \vdots \\ a_{n,1}x_1 + \dots + a_{n,m}x_m = 0 \end{array} \right\} \iff \overset{A:=}{\begin{pmatrix} a_{1,1} & \cdots & a_{1,m} \\ \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,m} \end{pmatrix}} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = 0$$

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 5.8.1 *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.

Man beachte, dass in unserer Formulierung des Gauß-Algorithmus

Satz 5.8.2 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 $T : K^n \rightarrow K^n$:

- 1) Multiplikation der i -ten Zeile mit $0 \neq \lambda \in K$ entspricht

$$T = \begin{matrix} i \\ \left(\begin{array}{ccccccc} 1 & & & & & & 0 \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & \lambda & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ 0 & & & & & & 1 \end{array} \right) \in K^{n \times n} \end{matrix}$$

- 2) Addition des λ -fachen der i -ten Zeile zur j -ten Zeile entspricht

$$T = \begin{matrix} j \\ \left(\begin{array}{ccccccc} 1 & & & & & & 0 \\ & \ddots & & & & & \\ & & \ddots & & & & \\ & & & \lambda & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ 0 & & & & & & 1 \end{array} \right) \in K^{n \times n} \\ i \end{matrix}$$

form hat, d.h.

$$T \cdot A = \begin{pmatrix} & \overset{j_1}{\underbrace{} \left| } & \overset{j_2}{} & \overset{j_r}{} & & \\ & 1 & & & & * \\ & & \underbrace{} \left| } & & & \\ & & & \ddots & & \\ 0 & & & & \underbrace{} \left| } & \\ & & & & & 1 \end{pmatrix}$$

Es gilt dann

$$\dim \text{Bild}(A) = r \quad \dim \text{Ker}(A) = m - r \quad ,$$

insbesondere ist

$$\dim \text{Bild}(A) + \dim \text{Ker}(A) = m.$$

Die Variablen x_{j_1}, \dots, x_{j_r} sind die Leitterme im Gleichungssystem $(T \cdot A) \cdot x = 0$.

Beweis. Mit dem Gaußalgorithmus 5.1 und Satz 5.8.2 gibt es T_1, \dots, T_s sodass

$$(T_s \cdot \dots \cdot T_1 \cdot A) \cdot x = 0$$

Zeilenstufenform hat. Als Produkt von Isomorphismen ist

$$T = T_s \cdot \dots \cdot T_1$$

ein Isomorphismus.

Zu den Dimensionsaussagen: Mit Bemerkung 5.3.16 ist

$$\dim \text{Ker}(A) = m - r.$$

Da T ein Isomorphismus ist, gilt

$$\dim(\text{Bild}(A)) = \dim(\text{Bild}(T \cdot A)).$$

Weiter ist $\text{Bild}(T \cdot A) \subset \langle e_1, \dots, e_r \rangle$ und somit $\dim(\text{Bild}(T \cdot A)) \leq r$. Andererseits sind die Spalten j_1, \dots, j_r wegen der Stufenform linear unabhängig (leichte Übung mit Algorithmus 5.3.14), und somit $\dim(\text{Bild}(T \cdot A)) \geq r$. ■

Bemerkung 5.8.5 Durch Zeilenoperationen entsprechend Bemerkung 5.2.8 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 5.8.6 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:

$$\begin{aligned} A &\mapsto \begin{pmatrix} \mathbf{1} & 1 & 0 & 0 & 1 \\ 0 & 0 & \mathbf{2} & 2 & 0 \\ 0 & 0 & \mathbf{1} & 1 & 0 \end{pmatrix} \mapsto \begin{pmatrix} \mathbf{1} & 1 & 0 & 0 & 1 \\ 0 & 0 & \mathbf{1} & 1 & 0 \\ 0 & 0 & \mathbf{1} & 1 & 0 \end{pmatrix} \\ &\mapsto \begin{pmatrix} \mathbf{1} & 1 & 0 & 0 & 1 \\ 0 & 0 & \mathbf{1} & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \end{aligned}$$

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);`

$$\begin{bmatrix} \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{1} \\ \mathbf{0} & \mathbf{0} & \mathbf{2} & \mathbf{2} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \end{bmatrix}$$

Satz 5.8.7 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 5.8.4.

Beweis. Seien $T_1, \dots, T_s \in K^{n \times n}$ die den elementaren Zeilentransformationen entsprechenden Matrizen, sodass

$$\underbrace{T_s \cdot \dots \cdot T_1 \cdot A}_{T:=}$$

Zeilenstufenform hat. Anwenden der Transformationen auf die Einheitsmatrix gibt

$$T_s \cdot \dots \cdot T_1 \cdot E = T_s \cdot \dots \cdot T_1 = T.$$

■

Beispiel 5.8.8 Mit den Zeilentransformationen aus [Beispiel 5.8.6](#) 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

$$T \cdot A = \begin{pmatrix} 1 & 0 & 0 \\ -\frac{1}{2} & \frac{1}{2} & 0 \\ -\frac{1}{2} & -\frac{1}{2} & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 2 & 2 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

hat Zeilenstufenform.

Beispiel 5.8.9 Wir bestimmen für das Beispiel noch eine Basis von $\text{Ker } A = \text{Ker}(T \cdot A)$: Die Lösungsmenge des linearen Gleichungssystems $(T \cdot A) \cdot x = 0$, d.h.

$$\begin{array}{rclcl} \mathbf{x}_1 & + & x_2 & & + & x_5 & = & 0 \\ & & & \mathbf{x}_3 & + & x_4 & & = & 0 \end{array}$$

ist

$$\text{Ker } A = \left\{ \left(\begin{array}{c} -x_2 - x_5 \\ x_2 \\ -x_4 \\ x_4 \\ x_5 \end{array} \right) \mid x_2, x_4, x_5 \in \mathbb{Q} \right\} = \left\langle \begin{pmatrix} -1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ -1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right\rangle$$

In MAPLE können wir $\text{Ker}(A)$ mit folgendem Code bestimmen:

`with(LinearAlgebra):`

`A := <<1, 1, 1>|<1, 1, 1>|<0, 2, 1>|<0, 2, 1>|<1, 1, 1>>;`

`NullSpace(A);`

$$\left[\begin{bmatrix} -1 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ -1 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} -1 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \right]$$

Bilder von Matrizen spielen ebenfalls eine wichtige Rolle, denn jeder Untervektorraum von K^n ist das Bild einer Matrix:

Lemma 5.8.10 *Ist*

$$A = (a_1 \mid \dots \mid a_m) \in K^{n \times m}$$

mit den Spalten a_1, \dots, a_m , so gilt

$$\text{Bild}(A) = \langle a_1, \dots, a_m \rangle.$$

Beweis. Wegen

$$A \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = x_1 \cdot a_1 + \dots + x_n \cdot a_n.$$

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 5.8.11 *Führen wir (analog zu Definition 5.8.2) mit A elementare Spaltentransformationen durch, können wir entsprechend eine Spaltenstufenform erreichen.*

Algorithmus 5.4 berechnet dann eine Basis des Bildes. Wir zeigen die Korrektheit von Algorithmus 5.4:

Beweis. Für jeden Isomorphismus $S : K^m \rightarrow K^m$ gilt

$$\text{Bild}(A) = \text{Bild}(A \cdot S),$$

Algorithmus 5.4 Bild**Input:** $A \in K^{n \times m}$ **Output:** Basis von $\text{Bild}(A)$

- 1: Berechne mit Bemerkung 5.8.11 eine Spaltenstufenform A' von A .
- 2: **return** Spalten $\neq 0$ von A' .

denn $\text{Bild}(S) = K^m$. In unserem Fall ist S eine Komposition von Spaltenoperationen, 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 5.8.12 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 $\text{Bild}(A) = \text{Bild}(B)$ genau dann, wenn die reduzierten Spaltenstufenformen von A und B übereinstimmen.

Beispiel 5.8.13 Für A wie in Beispiel 5.8.6 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

$$\begin{aligned}
 A &= \begin{pmatrix} \mathbf{1} & \mathbf{1} & 0 & 0 & 1 \\ 1 & 1 & \mathbf{2} & \mathbf{2} & 1 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix} \mapsto \begin{pmatrix} \mathbf{1} & \mathbf{1} & 0 & 0 & \mathbf{1} \\ 1 & 1 & \mathbf{1} & \mathbf{1} & 1 \\ 1 & 1 & \frac{1}{2} & \frac{1}{2} & 1 \end{pmatrix} \\
 &\mapsto \begin{pmatrix} \mathbf{1} & 0 & 0 & 0 & 0 \\ 1 & 0 & \mathbf{1} & 0 & 0 \\ 1 & 0 & \frac{1}{2} & 0 & 0 \end{pmatrix} \mapsto \begin{pmatrix} \mathbf{1} & 0 & 0 & 0 & 0 \\ 0 & \mathbf{1} & 0 & 0 & 0 \\ \frac{1}{2} & \frac{1}{2} & 0 & 0 & 0 \end{pmatrix}
 \end{aligned}$$

und somit eine Basis des Bilds

$$\text{Bild}(A) = \left\langle \left(\begin{pmatrix} 1 \\ 0 \\ \frac{1}{2} \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ \frac{1}{2} \end{pmatrix} \right) \right\rangle$$

In MAPLE können wir $\text{Bild}(A)$ wie folgt berechnen:
`with(LinearAlgebra):`

$A := \langle\langle 1, 1, 1 \rangle \mid \langle 1, 1, 1 \rangle \mid \langle 0, 2, 1 \rangle \mid \langle 0, 2, 1 \rangle \mid \langle 1, 1, 1 \rangle \rangle;$

$\text{ColumnSpace}(A);$

$$\left[\left[\begin{array}{c} 1 \\ 0 \\ \frac{1}{2} \end{array} \right], \left[\begin{array}{c} 0 \\ 1 \\ \frac{1}{2} \end{array} \right] \right]$$

5.9 Isomorphismen

Die Matrix T , die im Gauß-Algorithmus 5.8.4 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 5.5.10): Ist $F : V \rightarrow W$ ein Homomorphismus und $\Omega = (v_1, \dots, v_n)$ eine Basis von V , dann ist

$$F \text{ Isomorphismus} \Leftrightarrow (F(v_1), \dots, F(v_n)) \text{ Basis von } W,$$

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 5.9.1 Eine Matrix $A \in K^{n \times n}$ heißt *invertierbar*, wenn der Homomorphismus $K^n \rightarrow K^n$, $x \mapsto A \cdot x$ 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 $\text{id} : K^n \rightarrow K^n$ 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 1.4.18 über die Umkehrabbildung und Satz 5.7.7 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 5.9.2 *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 5.9.3 *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 3.2.3.(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 5.5 berechnet mit dem Gaußalgorithmus die Inverse von $A \in \mathrm{GL}(n, K)$: Wegen Satz 5.8.4 und $\dim \ker(A) = 0$ hat die reduzierte Zeilenstufenform von A genau n Einträge 1 auf der Diagonalen, ist also die Einheitsmatrix E .

Algorithmus 5.5 Inverse

Input: $A \in \mathrm{GL}(n, K)$

Output: A^{-1}

- 1: Bestimme mit Satz 5.8.4 und Satz 5.8.7 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 5.8.2). Oder anders ausgedrückt: Die Gruppe $\mathrm{GL}(n, K)$ wird von der Menge aller dieser Matrizen erzeugt.

Beispiel 5.9.4 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:

$$A = \begin{pmatrix} 1 & 0 & 0 \\ -\frac{1}{2} & \frac{1}{2} & 0 \\ -\frac{1}{2} & -\frac{1}{2} & 1 \end{pmatrix} \quad E = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{2} & 0 \\ 0 & -\frac{1}{2} & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 \\ \frac{1}{2} & 1 & 0 \\ \frac{1}{2} & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{2} & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 \\ \frac{1}{2} & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

$$E = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad A^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 2 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

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 5.21 und 5.22.

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 5.9.5 Sei $A \in \text{GL}(n, K)$ 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 5.9.6 Um (wie in Beispiel 4.13.5) 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

$$\underbrace{\begin{pmatrix} 1 & -1 & 1 \\ 0 & 0 & 1 \\ 4 & 2 & 1 \end{pmatrix}}_A \cdot \underbrace{\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}}_b = \underbrace{\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}}_b$$

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 5.6.10 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:

5.10 Basiswechsel

Wie in Satz 5.7.2 gezeigt, lässt sich jeder Homomorphismus $K^m \rightarrow K^n$ 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 $\Omega = (v_1, \dots, v_m)$ von K^m und $\Delta = (w_1, \dots, w_n)$ 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

$$\text{lc}_\Omega : K^m \rightarrow K^m$$

ist (mit Beispiel 5.5.3.(1)) ein Isomorphismus und wird als **Basiswechsel** bezeichnet. Da

$$\text{lc}_\Omega \begin{pmatrix} c_1 \\ \vdots \\ c_m \end{pmatrix} = c_1 \cdot v_1 + \dots + c_m \cdot v_m = (v_1 \mid \dots \mid v_m) \cdot \begin{pmatrix} c_1 \\ \vdots \\ c_m \end{pmatrix}$$

können wir lc_Ω (nach Satz 5.7.2) mit der invertierbaren Matrix

$$\text{lc}_\Omega = (v_1 \mid \dots \mid v_m) \in \text{GL}(m, K)$$

identifizieren, in deren Spalten die Basisvektoren v_i stehen. Genauso ist als Matrix geschrieben

$$\text{lc}_\Delta = (w_1 \mid \dots \mid w_n) \in \text{GL}(n, K).$$

Das Diagramm aus Definition 5.7.1 wird dann zu

$$\begin{array}{ccccc} & K^m & \xrightarrow{A} & K^n & \\ (v_1 \mid \dots \mid v_m) & \uparrow & & \uparrow & (w_1 \mid \dots \mid w_n) \\ & K^m & \xrightarrow{M_\Delta^\Omega(A)} & K^n & \end{array}$$

(wobei alle Abbildungen durch Matrixmultiplikation gegeben sind) und es gilt (mit Satz 5.7.7):

Satz 5.10.1 (Basiswechsel) Ist $A \in K^{n \times m}$ und $\Omega = (v_1, \dots, v_m)$ von K^m und $\Delta = (w_1, \dots, w_n)$ Basen von K^n , so gilt

$$M_{\Delta}^{\Omega}(A) = (w_1 \mid \dots \mid w_n)^{-1} \cdot A \cdot (v_1 \mid \dots \mid v_m).$$

Beispiel 5.10.2 Für

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

wie in [Beispiel 5.8.6](#) 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 5.9.4](#))

$$\begin{aligned} M_{\Delta}^{\Omega}(A) &= \begin{pmatrix} 1 & 0 & 0 \\ 1 & 2 & 0 \\ 1 & 1 & 1 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 2 & 2 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & -1 & 0 & -1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 0 \\ -\frac{1}{2} & \frac{1}{2} & 0 \\ -\frac{1}{2} & -\frac{1}{2} & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \end{aligned}$$

Bezüglich geeignet gewählter neuer Basen hat A also eine wesentlich einfachere Darstellung. Siehe auch die [Aufgaben 5.24](#) und [5.12](#).

Solche Basen kann man systematisch mit dem Gaußalgorithmus finden:

5.11 Klassifikation von Homomorphismen

Satz 5.11.1 (Klassifikationssatz) Sei $A \in K^{n \times m}$. Dann gibt es $S \in \text{GL}(m, K)$ und $T \in \text{GL}(n, K)$, sodass $T \cdot A \cdot S$ die **Normalform**

$$T \cdot A \cdot S = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}$$

hat, wobei $r = \text{rk } A$ 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 $E \in \text{GL}(n, K)$ aus, so erhalten wir T . Durch elementare Spaltentransformationen bringen wir dann $T \cdot A$ in die obige Form. Führen wir die Transformationen parallel mit $S \in \text{GL}(m, K)$ aus, so erhalten wir S . ■

In der Notation von Bemerkung 5.10.1 steht in den Spalten von T^{-1} die Basis Δ , in den Spalten von S die Basis Ω .

Beispiel 5.11.2 In Beispiel 5.8.8 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

$$T = \begin{pmatrix} 1 & 0 & 0 \\ -\frac{1}{2} & \frac{1}{2} & 0 \\ -\frac{1}{2} & -\frac{1}{2} & 1 \end{pmatrix} \in \text{GL}(3, \mathbb{Q})$$

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

$$\begin{aligned}
 T \cdot A &= \begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} & E &= \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \\
 & \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} & & \begin{pmatrix} 1 & -1 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \\
 & \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} & S &= \begin{pmatrix} 1 & 0 & -1 & 0 & -1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}
 \end{aligned}$$

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 5.25 und 5.26.

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 nicht.

Satz 5.11.3 (Dimensionsformel) Für jeden Vektorraumhomomorphismus $F : V \rightarrow W$ ist

$$\dim(V) = \dim \operatorname{Ker}(F) + \dim \operatorname{Bild}(F).$$

Beweis. Für $\dim V = \infty$ ist die Behauptung klar. Für $\dim V < \infty$ können wir mit Satz 5.11.1 durch Wahl geeigneter Basen von V und W annehmen, dass F durch eine Matrix in Normalform gegeben ist. Dann ist $\text{Bild}(F) = \langle e_1, \dots, e_r \rangle \subset K^n$ und $\text{Ker}(F) = \langle e_{r+1}, \dots, e_m \rangle \subset K^m$. Somit gilt

$$\dim(V) = m = (m - r) + r = \dim \text{Ker}(F) + \dim \text{Bild}(F).$$

■

5.12 Homomorphiesatz

Sei V ein K -Vektorraum. Ein Untervektorraum $U \subset V$ ist insbesondere eine Untergruppe von $(V, +)$.

Definition und Satz 5.12.1 Die Quotientengruppe V/U ist ein K -Vektorraum mit

$$\lambda \bar{v} = \overline{\lambda v}$$

für $\lambda \in K$ und $v \in V$, der **Quotientenvektorraum**.

Satz 5.12.2 (Homomorphiesatz) Sei $F : V \rightarrow W$ ein Vektorraumhomomorphismus. Dann gilt

$$V/\text{Ker}(F) \cong \text{Bild}(F)$$

Beweis. Für die Gruppenstruktur bezüglich $+$ haben wir dies schon in Satz 3.3.10 gezeigt. Weiter ist

$$\tilde{F} : V/\text{Ker}(F) \rightarrow \text{Bild}(F), \bar{v} \mapsto F(v)$$

ein Vektorraumhomomorphismus, denn

$$\tilde{F}(\lambda \cdot \bar{v}) = \tilde{F}(\overline{\lambda \cdot v}) = F(\lambda \cdot v) = \lambda \cdot F(v) = \lambda \cdot \tilde{F}(\bar{v})$$

für $\lambda \in K$. ■

Corollar 5.12.3 Für $\dim V < \infty$ gilt

$$\dim(V/U) = \dim(V) - \dim(U).$$

Beweis. Für $F: V \rightarrow V/U, v \mapsto \bar{v}$ gilt $\text{Ker}(F) = U$ und $\text{Bild}(F) = V/U$. Mit dem Homomorphiesatz 5.12.2 und der Dimensionsformel 5.11.3 folgt die Behauptung. ■

Die Elemente $\bar{v} \in V/U$ des Quotientenvektorraums sind affine Unterräume von V , d.h.

$$\bar{v} = v + U.$$

Betrachten wir inhomogene Gleichungssysteme noch einmal von einem höheren Standpunkt:

Bemerkung 5.12.4 *Mit Hilfe des Quotientenvektorraums lässt sich die Aussage von Satz 5.6.8 elegant formulieren: Nach Satz 5.12.2 ist*

$$\begin{aligned} \tilde{A}: K^m / \text{Ker}(A) &\rightarrow \text{Bild}(A) \\ \bar{x} &\mapsto A \cdot x \end{aligned}$$

ein Isomorphismus.

Sei $b \in K^n$. Ist $A \cdot x = b$ lösbar, d.h. $b \in \text{Bild}(A)$, dann hat b ein eindeutiges Urbild

$$\bar{c} := \tilde{A}^{-1}(b) \in K^m / \text{Ker}(A).$$

Dieser affine Unterraum von K^m ist genau die Lösungsmenge von $A \cdot x = b$, denn $A \cdot c = b$ und somit

$$\begin{aligned} \bar{c} = c + \text{Ker } A &= \{c + v \mid v \in \text{Ker}(A)\} \\ &= L(A, b) \subset K^m \end{aligned}$$

Die Klasse \bar{c} (d.h. die affine Ebene) ist eindeutig bestimmt, nicht aber der Aufpunkt c .

Beispiel 5.12.5 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

$$\begin{aligned} \tilde{A}: K^m / \text{Ker}(A) &\rightarrow \text{Bild}(A) \\ \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} &\mapsto x_1 + 2x_2 \end{aligned}$$

die Nebenklasse

$$\tilde{A}^{-1}(1) = \overline{\begin{pmatrix} 1 \\ 0 \end{pmatrix}} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \left\langle \begin{pmatrix} -2 \\ 1 \end{pmatrix} \right\rangle = L(A, b),$$

d.h. die affine Gerade in Abbildung 5.6.

5.13 Anwendung: Lineare Codes

5.13.1 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 Analogrechner¹ heute in der Computertechnik keine wesentliche Rolle mehr spielen, liegt u.a. an der Möglichkeit, Fehler in digitalen Daten zu 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 $\text{rk } G = m$. Die Matrix heißt **Generatormatrix** des Codes und definiert einen Monomorphismus

$$G : K^m \rightarrow K^n$$

denn mit Satz 5.8.4 ist

$$\dim \text{Ker}(G) = m - \dim \text{Bild}(G) = 0.$$

Somit ist die Abbildung

$$G : K^m \rightarrow \text{Bild}(G)$$

¹Analogrechner können zum Beispiel sehr gut integrieren. Die einfachste Implementation wäre folgende: Zur Bestimmung des Integrals einer nicht-negativen 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.

bijektiv. Den Code können wir bis auf Wahl einer Basis (Spalten von G) mit dem Untervektorraum

$$U = \text{Bild}(G) \subset K^n$$

identifizieren.

Definition 5.13.1 *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 $v \in K^m$ 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:

5.13.2 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 5.13.2 Für $A = (a_{i,j}) \in K^{n \times m}$ ist die **Transponierte** $A^t = (a_{j,i}) \in K^{m \times n}$.

Beispiel 5.13.3 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 5.13.4 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 5.32.

Satz 5.13.5 Für $A \in K^{n \times m}$ gilt

$$\text{rk } A = \text{rk } A^t$$

Beweis. Mit der Normalform gemäß Satz 5.11.1

$$T \cdot A \cdot S = \begin{pmatrix} E_s & 0 \\ 0 & 0 \end{pmatrix} \in K^{m \times n}$$

ist

$$S^t \cdot A^t \cdot T^t = \begin{pmatrix} E_s & 0 \\ 0 & 0 \end{pmatrix} \in K^{n \times m}$$

also

$$\text{rk } A = \dim \text{Bild}(A) = s = \dim \text{Bild}(A^t) = \text{rk } A^t$$

■

Satz 5.13.6 Sei $A \in K^{n \times m}$ mit $\text{rk } A = m \leq n$, also

$$\dim \text{Ker}(A^t) = n - m.$$

Schreiben wir eine Basis von $\text{Ker}(A^t)$ in die Spalten von

$$W \in K^{n \times (n-m)}$$

dann gilt

$$\text{Ker}(A^t) = \text{Bild}(W)$$

und

$$\text{Bild}(A) = \text{Ker}(W^t)$$

Beweis. Nach Konstruktion von W ist $\text{Ker}(A^t) = \text{Bild}(W)$ klar. Damit folgt

$$W^t \cdot A = (A^t \cdot W)^t = 0$$

also $\text{Bild}(A) \subset \text{Ker}(W^t)$. Nach Konstruktion ist

$$\dim \text{Bild}(W) = \dim \text{Ker}(A^t) = n - m.$$

Mit Satz 5.11.3 und Satz 5.13.5 gilt also

$$\begin{aligned} \dim \text{Ker}(W^t) &= n - \dim \text{Bild}(W^t) = n - \dim \text{Bild}(W) \\ &= n - (n - m) = m = \dim \text{Bild}(A) \end{aligned}$$

und damit $\text{Bild}(A) = \text{Ker}(W^t)$ nach Corollar 5.4.12. ■

Wir wenden dies nun auf die Generatormatrix G eines linearen Codes über $K = \mathbb{F}_2$ an:

Definition 5.13.7 Für die Generatormatrix $G \in K^{n \times m}$ heißt $H \in K^{(n-m) \times n}$ mit

$$\text{Bild}(G) = \text{Ker}(H)$$

die **Kontrollmatrix** des Codes. Es ist

$$c' \in \text{Bild}(G) \Leftrightarrow H \cdot c' = 0$$

Beispiel 5.13.8 Für die Generatormatrix

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

ist

$$\text{Ker}(G^t) = \text{Ker} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} = \left\langle \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \right\rangle$$

also

$$H = (1, 1, 1)$$

die Kontrollmatrix. Wir haben also Abbildungen

$$K^2 \xrightarrow{G} K^3 \xrightarrow{H} K$$

mit $\text{Ker}(H) = \text{Bild}(G)$. Zum Codieren verwenden wir die Abbildung

$$G: K^2 \rightarrow K^3 \\ \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} \mapsto \begin{pmatrix} v_1 \\ v_2 \\ v_1 + v_2 \end{pmatrix}$$

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

$$G: K^3 \rightarrow K \\ \begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix} \mapsto c_1 + c_2 + c_3$$

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

$$v = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \text{ codiert in } c = G \cdot v = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$$

Stören wir c in

$$c' = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \text{ so gilt } H \cdot c' = 1 \neq 0$$

und wir erkennen den Fehler.

Wie kann man quantifizieren, wieviele Fehler ein Code erkennen kann?

Definition 5.13.9 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 $U = \text{Bild}(G) \subset K^n$ 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 $c' \in U = \text{Bild}(G)$, 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 Bezeichnung sinnvoll:

Definition 5.13.10 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 5.13.11 Der Code aus Beispiel 5.13.8 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 5.30.

5.13.3 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 5.13.12 *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 5.13.13 *Der Code U ist r -fehlerkorrigierend, falls*

$$d_{\min}(U) \geq 2r + 1$$

Beweis. Gibt es ein $w \in K^n$ und $v, u \in U$, $v \neq u$ und

$$d(w, u) \leq r \text{ und } d(w, v) \leq r$$

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 $d(u, v) = 0 \Leftrightarrow u = v$

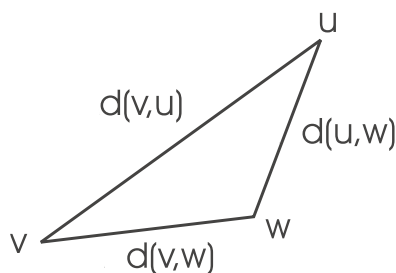


Abbildung 5.7: Dreiecksungleichung

für alle $u, v \in K^n$). Siehe Abbildung 5.7 für die Dreiecksungleichung im Fall des Euklidischen Abstands auf \mathbb{R}^2 .

■

Wir diskutieren nun einen Code, der einen Fehler korrigieren kann, d.h. 1-fehlerkorrigierend ist:

Definition 5.13.14 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 $\text{Ker}(H)$ 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

$$\text{Ker}(H) = \text{Bild}(G),$$

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 5.13.15 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 $U = \text{Bild}(G) = \text{Ker}(H)$

$$d_{\min}(U) = 3$$

und somit ist der Code 2-fehlererkennend und 1-fehlerkorrigierend.
Zum Beispiel wird die Nachricht

$$v = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} \text{ in den Vektor } c = G \cdot v = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

codiert. Stören wir c zu

$$c' = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} \text{ erhalten wir } H \cdot c' = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \neq 0$$

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

$$H \cdot \underbrace{\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}}_e = H \cdot c' = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$

und für den Einheitsvektor e ist klarerweise $d(e, 0) = 1$ minimal. Somit erhalten wir

$$c = c' - e = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} - \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

und daraus wiederum das korrekt dekodierte Urbild v mit $Av = c$.

Bemerkung 5.13.16 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 5.13.17 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 5.13.14 die Wahrscheinlichkeit einer mit Fehlerkorrektur richtigen Übertragung gleich

$$(p^n + n \cdot p^{n-1} \cdot (1-p)) \frac{N}{n-s},$$

denn in jedem Block von n Bits sind $n-s$ Datenbits codiert.

Beispiel 5.13.18 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 $s = 3$ Hamming-Code ist die Wahrscheinlichkeit einen Block von $n-s = 4$ Bits mit Fehlerkorrektur richtig zu übertragen

$$99.9999999999999979 \%,$$

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.

5.14 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

$$\det(A) = a_{11}a_{22} - a_{12}a_{21}.$$

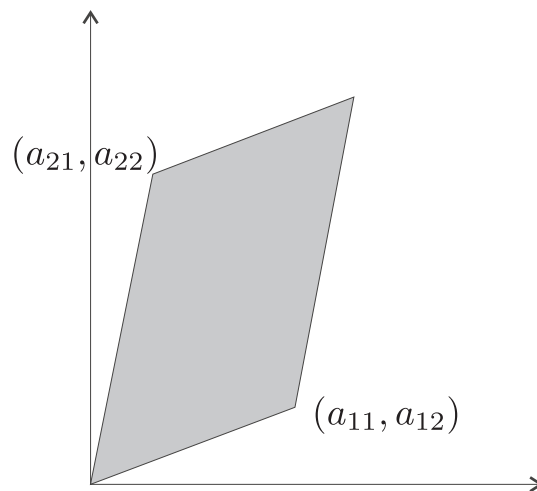


Abbildung 5.8: Parallelogramm

Geometrisch können wir $\det(A)$ (bis auf Vorzeichen) interpretieren als Fläche des **Parallelogramms** aufgespannt von den Zeilen von A (siehe Abbildung 5.8):

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 5.9. Damit erhalten wir

$$\begin{pmatrix} a_{11} & a_{12} \\ 0 & a_{22} - \frac{a_{21}}{a_{11}} a_{12} \end{pmatrix}$$

siehe Abbildung 5.10. 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 5.11. Die Zeilen dieser Matrix spannen ein Recht-

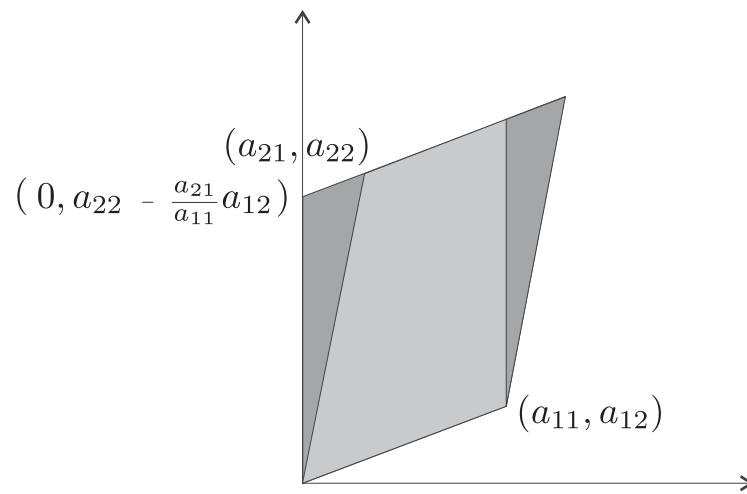


Abbildung 5.9: Subtraktion eines Vielfachen des ersten Erzeugers des Parallelogramms vom zweiten.

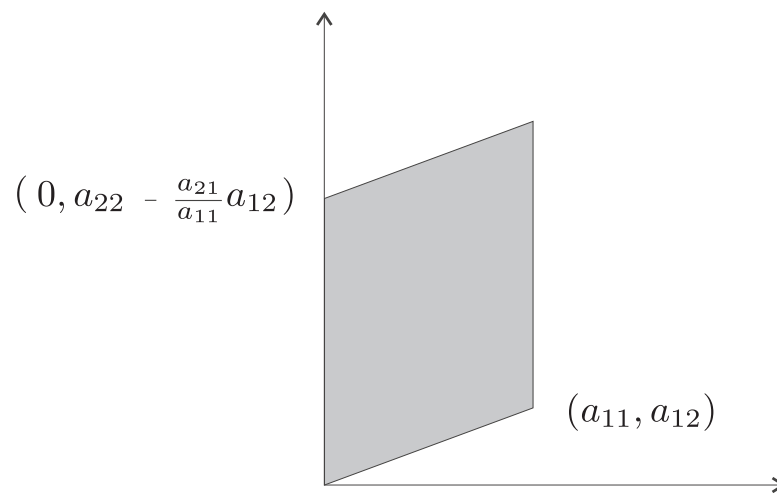


Abbildung 5.10: Parallelogramm nach Scherung

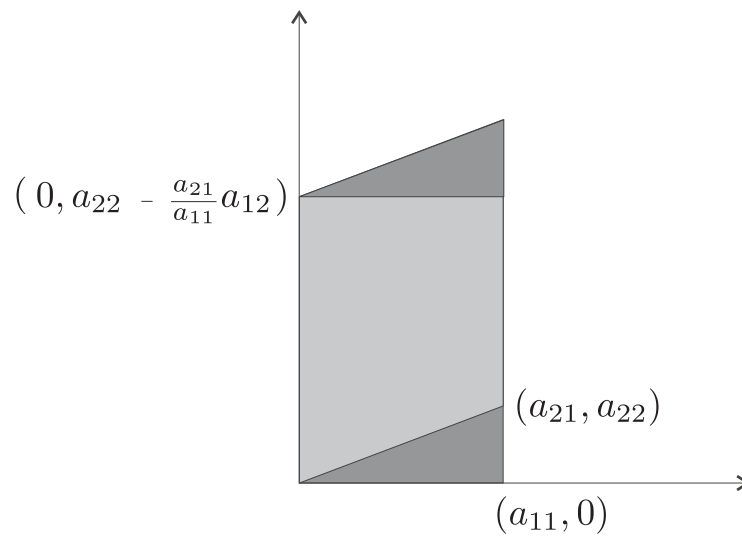


Abbildung 5.11: Scherung zum Rechteck

eck auf mit Fläche

$$a_{11} \cdot \left(a_{22} - \frac{a_{21}}{a_{11}} a_{12} \right) = \det(A)$$

was die Behauptung zeigt, siehe Abbildung 5.12.

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 5.14.1 Sei K ein Körper. Die **Determinantenabbildung** ist definiert als

$$\det : K^{n \times n} \rightarrow K$$

$$\det(A) = \sum_{\sigma \in S_n} \text{sign}(\sigma) \cdot a_{1,\sigma(1)} \cdot \dots \cdot a_{n,\sigma(n)}$$

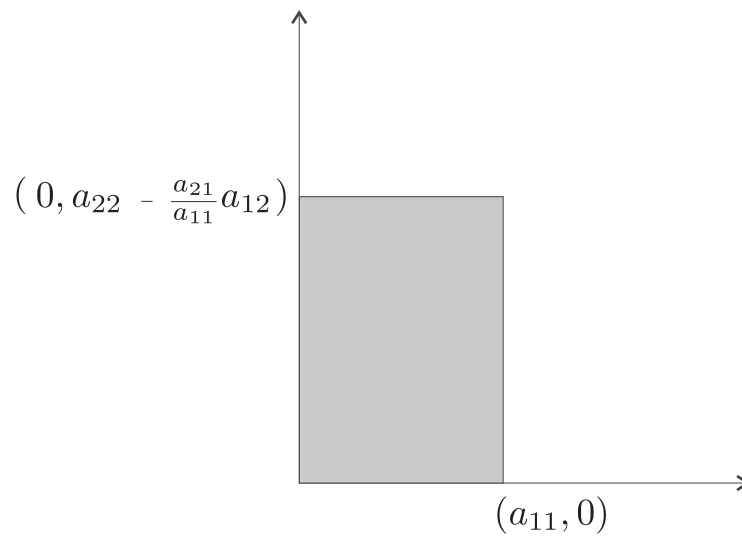


Abbildung 5.12: Zum Parallelogramm flächengleiches Rechteck

Lemma 5.14.2 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 $i = 1, \dots, n$ und jedes $\lambda \in K$ gilt

$$\det \begin{pmatrix} a_1 \\ \vdots \\ a_{i-1} \\ \mathbf{a}_i + \mathbf{b}_i \\ a_{i+1} \\ \vdots \\ a_n \end{pmatrix} = \det \begin{pmatrix} a_1 \\ \vdots \\ a_{i-1} \\ \mathbf{a}_i \\ a_{i+1} \\ \vdots \\ a_n \end{pmatrix} + \det \begin{pmatrix} a_1 \\ \vdots \\ a_{i-1} \\ \mathbf{b}_i \\ a_{i+1} \\ \vdots \\ a_n \end{pmatrix}$$

und

$$\det \begin{pmatrix} a_1 \\ \vdots \\ a_{i-1} \\ \lambda \cdot \mathbf{a}_i \\ a_{i+1} \\ \vdots \\ a_n \end{pmatrix} = \lambda \cdot \det \begin{pmatrix} a_1 \\ \vdots \\ a_{i-1} \\ \mathbf{a}_i \\ a_{i+1} \\ \vdots \\ a_n \end{pmatrix}$$

(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

$$\begin{aligned} & \sum_{\sigma \in S_n} \text{sign}(\sigma) \cdot a_{1,\sigma(1)} \cdot \dots \cdot (\mathbf{a}_{i,\sigma(i)} + \mathbf{b}_{i,\sigma(i)}) \cdot \dots \cdot a_{n,\sigma(n)} \\ &= \sum_{\sigma \in S_n} \text{sign}(\sigma) \cdot a_{1,\sigma(1)} \cdot \dots \cdot \mathbf{a}_{i,\sigma(i)} \cdot \dots \cdot a_{n,\sigma(n)} \\ &+ \sum_{\sigma \in S_n} \text{sign}(\sigma) \cdot a_{1,\sigma(1)} \cdot \dots \cdot \mathbf{b}_{i,\sigma(i)} \cdot \dots \cdot a_{n,\sigma(n)} \end{aligned}$$

und

$$\begin{aligned} & \sum_{\sigma \in S_n} \text{sign}(\sigma) \cdot a_{1,\sigma(1)} \cdot \dots \cdot (\lambda \cdot \mathbf{a}_{i,\sigma(i)}) \cdot \dots \cdot a_{n,\sigma(n)} \\ &= \lambda \cdot \sum_{\sigma \in S_n} \text{sign}(\sigma) \cdot a_{1,\sigma(1)} \cdot \dots \cdot \mathbf{a}_{i,\sigma(i)} \cdot \dots \cdot a_{n,\sigma(n)} \end{aligned}$$

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 $S_n/A_n = \{\text{id}, A_n \cdot \tau\}$), also

$$\begin{aligned} \det(A) &= \sum_{\sigma \in A_n} a_{1,\sigma(1)} \cdot \dots \cdot a_{n,\sigma(n)} \\ &\quad - \sum_{\sigma \in A_n} a_{1,\sigma(\tau(1))} \cdot \dots \cdot a_{n,\sigma(\tau(n))} \end{aligned}$$

wobei wir verwenden, dass sign ein Gruppenhomomorphismus ist, also

$$\text{sign}(\sigma \circ \tau) = \text{sign}(\sigma) \cdot \text{sign}(\tau) = -\text{sign}(\sigma).$$

Angenommen die i -te und j -te Zeile sind gleich, d.h. $a_i = a_j$. Dann ist

$$\begin{aligned} & a_{1,\sigma(\tau(1))} \cdot \dots \cdot a_{i,\sigma(\tau(i))} \cdot \dots \cdot a_{j,\sigma(\tau(j))} \cdot \dots \cdot a_{n,\sigma(\tau(n))} \\ &= a_{1,\sigma(1)} \cdot \dots \cdot a_{i,\sigma(j)} \cdot \dots \cdot a_{j,\sigma(i)} \cdot \dots \cdot a_{n,\sigma(n)} \\ &= a_{1,\sigma(1)} \cdot \dots \cdot a_{i,\sigma(i)} \cdot \dots \cdot a_{j,\sigma(j)} \cdot \dots \cdot a_{n,\sigma(n)}. \end{aligned}$$

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 5.14.3 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:

$$\det(A) = \lambda_1 \cdot \dots \cdot \lambda_n$$

4) Es gilt

$$A \text{ invertierbar} \iff \det(A) \neq 0$$

Beweis.

1) Mit (D1) und (D2) gilt für $i \neq j$

$$\underbrace{\det \begin{pmatrix} \vdots \\ \mathbf{a}_i + \mathbf{a}_j \\ \vdots \\ \mathbf{a}_i + \mathbf{a}_j \\ \vdots \end{pmatrix}}_0 = \underbrace{\det \begin{pmatrix} \vdots \\ \mathbf{a}_i \\ \vdots \\ \mathbf{a}_i \\ \vdots \end{pmatrix}}_0 + \underbrace{\det \begin{pmatrix} \vdots \\ \mathbf{a}_j \\ \vdots \\ \mathbf{a}_j \\ \vdots \end{pmatrix}}_0 \\ + \det \begin{pmatrix} \vdots \\ \mathbf{a}_i \\ \vdots \\ \mathbf{a}_j \\ \vdots \end{pmatrix} + \det \begin{pmatrix} \vdots \\ \mathbf{a}_j \\ \vdots \\ \mathbf{a}_i \\ \vdots \end{pmatrix}$$

2) Mit (D1) und (D2) gilt für $i \neq j$

$$\det \begin{pmatrix} a_1 \\ \vdots \\ a_{i-1} \\ \mathbf{a}_i + \lambda \cdot \mathbf{a}_j \\ a_{i+1} \\ \vdots \\ a_n \end{pmatrix} = \det \begin{pmatrix} a_1 \\ \vdots \\ a_{i-1} \\ \mathbf{a}_i \\ a_{i+1} \\ \vdots \\ a_n \end{pmatrix} + \underbrace{\lambda \cdot \det \begin{pmatrix} a_1 \\ \vdots \\ a_{i-1} \\ \mathbf{a}_j \\ a_{i+1} \\ \vdots \\ a_n \end{pmatrix}}_0$$

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 $\lambda_1 \cdot \dots \cdot \lambda_n$ 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

$$\begin{pmatrix} \lambda_1 & & & & * \\ & \ddots & & & \\ & & \lambda_{i-1} & & \\ & & & 0 & \dots & \dots & 0 \\ & & & & \lambda_{i+1} & & * \\ & & & & & \ddots & \\ 0 & & & & & & \lambda_n \end{pmatrix}$$

Aus der Definition der Determinante folgt, dass $\det(A) = 0$, denn jeder Summand enthält einen Faktor aus der i -ten Zeile.

4) Mit Bemerkung 5.5.10 und Satz 5.8.4 gilt: A invertierbar $\Leftrightarrow \text{rk } A = \dim \text{Bild } A = n \Leftrightarrow$ Zeilenstufenform von A ist

$$\begin{pmatrix} \lambda_1 & & * \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$$

mit $\lambda_1, \dots, \lambda_n \neq 0$.

■

Das Corollar gibt uns Algorithmus 5.6 zur Bestimmung der Determinanten.

Algorithmus 5.6 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** $\det(A) = (-1)^v \det(D) = (-1)^v \cdot \lambda_1 \cdot \dots \cdot \lambda_n$.
-

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 5.14.4 Für die Determinante von

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

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):
 $A := \langle\langle 1, 1, 2 \rangle \langle -1, -1, -1 \rangle \langle -1, 1, 0 \rangle\rangle$;
Determinant(A);
 -2

Satz 5.14.5 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 5.14.3 und (D1) gilt

$$\det(T \cdot B) = \det(T) \cdot \det(B)$$

falls $T \in \text{GL}(n, K)$ eine elementare Zeilenoperation darstellt. Mit Algorithmus 5.5 ist $A = T_1 \cdot \dots \cdot T_s$ das Produkt solcher Matrizen, also

$$\det(A \cdot B) = \det(T_1) \cdot \dots \cdot \det(T_s) \cdot \det(B)$$

Insbesondere für $B = E$ folgt

$$\det(A) = \det(T_1) \cdot \dots \cdot \det(T_s)$$

und damit die Behauptung. ■

Mit $\det(E) = 1$ erhalten wir:

Corollar 5.14.6 Für $A \in \text{GL}(n, K)$ ist

$$\det(A^{-1}) = \frac{1}{\det(A)}.$$

Beispiel 5.14.7 Als Illustration des Corollars bestimmen wir die Inverse für A aus Beispiel 5.14.4 und beobachten wie sich in jedem Schritt die Determinante ändert

$$\begin{array}{lcl}
 \det(A) = & \det \begin{pmatrix} 1 & -1 & -1 \\ 1 & -1 & 1 \\ 2 & -1 & 0 \end{pmatrix} & | & 1 = \det \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\
 & = \det \begin{pmatrix} 1 & -1 & -1 \\ 0 & 0 & 2 \\ 0 & 1 & 2 \end{pmatrix} & & = \det \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ -2 & 0 & 1 \end{pmatrix} \\
 & = -\det \begin{pmatrix} 1 & -1 & -1 \\ 0 & 1 & 2 \\ 0 & 0 & 2 \end{pmatrix} & & = -\det \begin{pmatrix} 1 & 0 & 0 \\ -2 & 0 & 1 \\ -1 & 1 & 0 \end{pmatrix} \\
 & = -2 \cdot \det \begin{pmatrix} 1 & -1 & -1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} & & = -2 \cdot \det \begin{pmatrix} 1 & 0 & 0 \\ -2 & 0 & 1 \\ -\frac{1}{2} & \frac{1}{2} & 0 \end{pmatrix} \\
 & = -2 \cdot \det \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} & & = -2 \cdot \det \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 0 \\ -1 & -1 & 1 \\ -\frac{1}{2} & \frac{1}{2} & 0 \end{pmatrix} \\
 & = -2 \cdot \det \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} & & = -2 \cdot \det \begin{pmatrix} -\frac{1}{2} & -\frac{1}{2} & 1 \\ -1 & -1 & 1 \\ -\frac{1}{2} & \frac{1}{2} & 0 \end{pmatrix} \\
 & = & -2 & | & = -2 \cdot \det(A^{-1})
 \end{array}$$

5.15 Anwendung: Eigenvektoren und Page-Rank

5.15.1 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 5.15.1 *Als Beispiel betrachten wir den Graphen in Abbildung 5.13.*

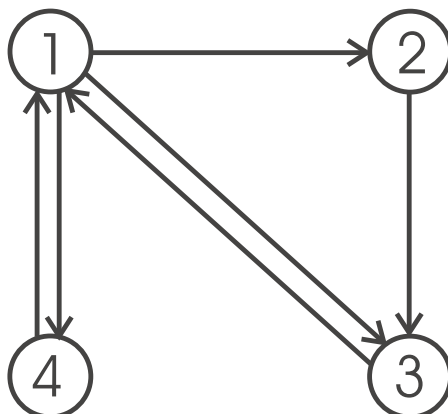


Abbildung 5.13: Gerichteter Graph von Links zwischen Internetseiten.

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

$$B = \begin{pmatrix} \frac{1}{n} & \dots & \frac{1}{n} \\ \vdots & \ddots & \vdots \\ \frac{1}{n} & \dots & \frac{1}{n} \end{pmatrix}.$$

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 definiert, dass alle Spaltensummen gleich 1 sind. Allgemein definiert man:

Definition 5.15.2 Eine Matrix $A = (a_{i,j}) \in \mathbb{R}^{n \times n}$ heißt **Markovmatrix**, falls $a_{ij} \geq 0$ für alle i, j und

$$\sum_{j=1}^n a_{i,j} = 1$$

für alle i .

Beispiel 5.15.3 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:

5.15.2 Eigenwerte und Eigenvektoren

Definition 5.15.4 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

$$\text{Eig}(A, \lambda) = \text{Ker}(\lambda E - A) \subset K^n$$

der **Eigenraum** von A zum Eigenwert λ .

Als Kern ist $\text{Eig}(A, \lambda)$ ein Untervektorraum. Bis auf den 0-Vektor sind die Elemente von $\text{Eig}(A, \lambda)$ genau die Eigenvektoren von A zum Eigenwert λ .

Satz 5.15.5 Für $A \in K^{n \times n}$ gilt

$$\text{Eig}(A, \lambda) \neq \{0\} \iff \det(\lambda E - A) = 0$$

Beweis. Mit Satz 5.8.4 und Corollar 5.14.3.(4) gilt

$$\begin{aligned} \text{Eig}(A, \lambda) \neq \{0\} &\iff \dim \text{Ker}(\lambda E - A) > 0 \\ &\iff \lambda E - A \text{ ist nicht invertierbar} \\ &\iff \det(\lambda E - A) = 0 \end{aligned}$$

■

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:

$$\begin{array}{ccc} K^n & \xrightarrow{A} & K^n \\ T \uparrow & & \uparrow T \\ K^n & \xrightarrow{D} & K^n \end{array}$$

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 5.36.

Definition und Satz 5.15.6 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 $T \in \text{GL}(n, K)$ 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 $T \in \text{GL}(n, K)$ 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, \dots, t_n die Basis aus Eigenvektoren und $T = (t_1 \mid \dots \mid t_n)$. Dann gilt $A \cdot t_i = t_i \cdot \lambda_i$, also

$$A \cdot T = T \cdot D.$$

■

Definition und Satz 5.15.7 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 4.2.10 (Einsetzen in Polynome ist ein Ringhomomorphismus) und Satz 5.15.5 gilt

$$\chi_A(\lambda) = 0 \Leftrightarrow \det(\lambda \cdot E - A) = 0 \Leftrightarrow \text{Eig}(A, \lambda) \neq \{0\}$$

■

Bemerkung 5.15.8 Ist A diagonalisierbar, dann gilt mit Satz 5.14.5 und Corollar 5.14.6, dass

$$\begin{aligned} \chi_A(t) &= \det(t \cdot E - A) = \det(T \cdot (t \cdot E - D) \cdot T^{-1}) \\ &= \det(T) \cdot \det(t \cdot E - D) \cdot \det(T)^{-1} \\ &= \chi_D(t) = \prod_{i=1}^s (t - \mu_i)^{n_i} \end{aligned}$$

mit den paarweise verschiedenen Eigenwerten $\mu_1, \dots, \mu_s \in K$ 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 5.15.9 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** $\dim \text{Eig}(A, \mu_i)$ mit den algebraischen Vielfachheiten n_i übereinstimmen, d.h.

$$\dim \text{Ker}(\mu_i E - A) = n_i \quad \forall i = 1, \dots, s.$$

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 $v_i \in \text{Eig}(A, \mu_i)$ zeigen wir mit Induktion nach s

$$v_1 + \dots + v_s = 0 \implies v_1 = \dots = v_s = 0.$$

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 $v_i = 0$ $\forall i = 1, \dots, s - 1$, also auch $v_s = 0$. ■

Man sagt dann auch: Die Summe der Eigenräume

$$\sum_{i=1}^s \text{Eig}(A, \mu_i) = \left\{ \sum_{i=1}^s v_i \mid v_i \in \text{Eig}(A, \mu_i) \right\} = K^n$$

ist eine **direkte Summe** und schreibt $\bigoplus_{i=1}^s \text{Eig}(A, \mu_i)$.

Bemerkung: Es gilt stets $\dim \text{Eig}(A, \mu_i) \leq n_i$ (Übung).

Beispiel 5.15.10 Für

$$A = \begin{pmatrix} 4 & 0 & 2 \\ -2 & 2 & -2 \\ -4 & 0 & -2 \end{pmatrix}$$

ist

$$\begin{aligned} \chi_A(t) &= \det(tE - A) = \det \begin{pmatrix} t-4 & 0 & -2 \\ 2 & t-2 & 2 \\ 4 & 0 & t+2 \end{pmatrix} \\ &= \det \begin{pmatrix} t-4 & 0 & -2 \\ 0 & t-2 & 2 + \frac{2}{t-4} \cdot 2 \\ 0 & 0 & t+2 + \frac{4}{t-4} \cdot 2 \end{pmatrix} \\ &= t^3 - 4t^2 + 4t \\ &= t(t-2)^2 \end{aligned}$$

Man beachte, dass wir hier mit rationalen Funktionen in $\mathbb{Q}(t) = \mathbb{Q}(\mathbb{Q}[t])$ 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

$$\begin{aligned} \text{Eig}(A, 0) &= \text{Ker}(A) = \left\langle \left(\begin{array}{c} -\frac{1}{2} \\ \frac{1}{2} \\ 1 \end{array} \right) \right\rangle \\ \text{Eig}(A, 2) &= \text{Ker}(2E - A) = \left\langle \left(\begin{array}{c} 0 \\ 1 \\ 0 \end{array} \right), \left(\begin{array}{c} -1 \\ 0 \\ 1 \end{array} \right) \right\rangle \end{aligned}$$

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

$$T = \begin{pmatrix} 0 & -1 & -\frac{1}{2} \\ 1 & 0 & \frac{1}{2} \\ 0 & 1 & 1 \end{pmatrix} \quad \text{und} \quad T^{-1} = \begin{pmatrix} -1 & 1 & -1 \\ -2 & 0 & -1 \\ 2 & 0 & 2 \end{pmatrix}$$

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 5.34.

Bemerkung 5.15.11 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

$$\text{Eig}(A, 1) = \left\langle \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\rangle,$$

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 5.35.

5.15.3 Markovmatrizen

Satz 5.15.12 Jede Markovmatrix hat den Eigenwert 1.

Beweis. Sei A eine Markovmatrix. Mit Übung 5.32 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 5.15.7 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 5.15.13 Für die Matrix A in Beispiel 5.15.3 erhalten wir mit dem Gaußalgorithmus

$$\begin{aligned} E - A &= \begin{pmatrix} 1 & 0 & -1 & -1 \\ -\frac{1}{3} & 1 & 0 & 0 \\ -\frac{1}{3} & -1 & 1 & 0 \\ -\frac{1}{3} & 0 & 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & -1 & -1 \\ 0 & 1 & -\frac{1}{3} & -\frac{1}{3} \\ 0 & -1 & \frac{2}{3} & -\frac{1}{3} \\ 0 & 0 & -\frac{1}{3} & \frac{2}{3} \end{pmatrix} \\ &\mapsto \begin{pmatrix} 1 & 0 & -1 & -1 \\ 0 & 1 & -\frac{1}{3} & -\frac{1}{3} \\ 0 & 0 & \frac{1}{3} & -\frac{1}{3} \\ 0 & 0 & -\frac{1}{3} & \frac{2}{3} \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & -1 & -1 \\ 0 & 1 & -\frac{1}{3} & -\frac{1}{3} \\ 0 & 0 & 1 & -2 \\ 0 & 0 & 0 & 0 \end{pmatrix} \\ &\mapsto \begin{pmatrix} 1 & 0 & -1 & -1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -2 \\ 0 & 0 & 0 & 0 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 & -3 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -2 \\ 0 & 0 & 0 & 0 \end{pmatrix} \end{aligned}$$

also

$$\text{Eig}(A, 1) = \text{Ker}(E - A) = \left\langle \left(\begin{array}{c} 3 \\ 1 \\ 2 \\ 1 \end{array} \right) \right\rangle$$

Das Ranking der Internetseiten mit dem Linkgraphen aus Abbildung 5.13 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.

5.16 Übungsaufgaben

Übung 5.1 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 5.16.1 Bestimmen Sie jeweils die Lösungsmenge $V \subset \mathbb{Q}^5$ für folgende Gleichungssysteme und eine Basis von V :

1)

$$\begin{array}{rcccccc} x_1 & + & 2x_2 & + & 2x_3 & - & 2x_4 & - & x_5 & = & 0 \\ -2x_1 & - & 3x_2 & - & x_3 & + & 8x_4 & + & x_5 & = & 0 \\ x_1 & + & 4x_2 & + & 8x_3 & + & 8x_4 & - & 4x_5 & = & 0 \\ 2x_1 & + & 5x_2 & + & 7x_3 & + & 2x_4 & - & 4x_5 & = & 0 \end{array}$$

2)

$$\begin{array}{rcccccc} x_1 & + & x_2 & + & x_3 & + & x_4 & - & x_5 & = & 0 \\ x_1 & + & 2x_2 & + & 3x_3 & + & 4x_4 & - & 5x_5 & = & 0 \\ x_1 & + & 4x_2 & + & 9x_3 & + & 16x_4 & - & 25x_5 & = & 0 \\ x_1 & + & 8x_2 & + & 27x_3 & + & 64x_4 & - & 125x_5 & = & 0 \end{array}$$

Beispiel 5.16.2 Bestimmen Sie für jedes $t \in \mathbb{Q}$ eine Basis des Lösungsraums $V_t \subset \mathbb{Q}^3$ des homogenen linearen Gleichungssystems

$$\begin{array}{rccccrcr} -x_1 & + & & x_2 & - & & 2x_3 & = & 0 \\ & x_1 & + & (t-1) \cdot x_2 & + & & 2x_3 & = & 0 \\ 2x_1 & + & (t-2) \cdot x_2 & + & (t^2 - t + 4) \cdot x_3 & = & 0 \end{array}$$

Übung 5.2 Sei

$$\begin{array}{l} l_1 = a_{1,1}x_1 + \dots + a_{1,n}x_n = 0 \\ \vdots \\ l_r = a_{r,1}x_1 + \dots + a_{r,n}x_n = 0 \end{array}$$

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 5.3 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:

$$\begin{array}{l} U_1 = \{f \in \mathbb{R}[x]_{\leq d} \mid f(0) = 0\} \\ U_2 = \{f \in \mathbb{R}[x]_{\leq d} \mid f(0) = 1\} \\ U_3 = \{f \in \mathbb{R}[x]_{\leq d} \mid f(1) = 0\} \\ U_4 = \left\{f \in \mathbb{R}[x]_{\leq d} \mid \int_0^1 f(x) dx = 0\right\} \\ U_5 = \{f \in \mathbb{R}[x]_{\leq d} \mid f'(0) + f''(0) = 0\} \\ U_6 = \{f \in \mathbb{R}[x]_{\leq d} \mid f'(0) \cdot f''(0) = 0\} \end{array}$$

- 2) Bestimmen Sie bei den Untervektorräumen U_i jeweils eine Basis.

Übung 5.4 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 5.5 Zeigen Sie: Für jedes $b \in \mathbb{R}$ bilden die $d+1$ Polynome

$$1, (x-b), (x-b)^2, \dots, (x-b)^d \in \mathbb{R}[x]_{\leq d}$$

eine Basis von $\mathbb{R}[x]_{\leq d}$.

Übung 5.6 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 5.7 Bestimmen Sie welche Teilmengen von

$$\{x^3 + x, x^2, x^3, x^2 + 1, x, 1\}$$

Basen von $\mathbb{R}[x]_{\leq 3}$ bilden.

Übung 5.8 Sei K ein Körper, und seien $U, V \subset K^n$ Untervektorräume gegeben durch Basen u_1, \dots, u_s von U und v_1, \dots, 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

$$U = \left\langle \begin{pmatrix} 4 \\ 0 \\ 2 \\ 4 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ 1 \\ 1 \end{pmatrix} \right\rangle \quad V = \left\langle \begin{pmatrix} 2 \\ 0 \\ 3 \\ 1 \end{pmatrix}, \begin{pmatrix} 4 \\ 3 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 2 \\ 2 \\ 3 \\ 1 \end{pmatrix} \right\rangle$$

von \mathbb{Q}^4 an.

Übung 5.9 Sei

$$A = \begin{pmatrix} 1 & -2 & 3 & -4 \\ -3 & 2 & -1 & 0 \end{pmatrix} \quad \text{und} \quad B = \begin{pmatrix} 0 & -2 \\ 1 & -1 \\ 2 & 0 \\ 3 & 1 \end{pmatrix}$$

Berechnen Sie AB und BA . Wie können Sie $AB \neq BA$ auch ohne Rechnung sofort sehen? Bestimmen Sie den Rang von BA .

Übung 5.10 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

$$A \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_5 \end{pmatrix} = \begin{pmatrix} 2 \\ -7 \\ -7 \end{pmatrix} \quad B \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$$

Übung 5.11 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 5.12 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

$$\Omega = (1, x-1, (x-1)^2, (x-1)^3)$$

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

$$\frac{d}{dx} = \text{lc}_{\Delta} \circ A \circ \text{co}_{\Omega}.$$

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 $\varepsilon = (e_1, \dots, e_4)$ von \mathbb{Q}^4 . Können Sie die Matrix im Sinne von Ableitungen interpretieren?

Übung 5.13 Sei $d \in \mathbb{N}$, $t_1, \dots, t_{d+1} \in \mathbb{R}$ und

$$F: \mathbb{R}[x]_{\leq d} \rightarrow \mathbb{R}^{d+1}$$

$$p \mapsto \begin{pmatrix} p(t_1) \\ \vdots \\ p(t_{d+1}) \end{pmatrix}$$

- 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 $\Omega = (1, x, \dots, x^d)$ von $\mathbb{R}[x]_{\leq d}$ und der Standardbasis $\Delta = (e_1, \dots, e_{d+1})$ 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 4.18.

Übung 5.14 Seien V und W zwei K -Vektorräume mit Basen $\Omega = (v_1, \dots, v_n)$ und $\Delta = (w_1, \dots, w_m)$. Zeigen Sie: Die Menge $\text{Hom}_K(V, W)$ der Homomorphismen $V \rightarrow W$ und die Menge $K^{n \times m}$ der $n \times m$ -Matrizen sind K -Vektorräume und die Abbildung

$$\begin{aligned} \text{Hom}_K(V, W) &\rightarrow K^{n \times m} \\ F &\mapsto M_{\Delta}^{\Omega}(F) \end{aligned}$$

ist ein Isomorphismus.

Übung 5.15 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 5.16 Bestimmen Sie jeweils eine Basis von $\text{Ker } A$ und $\text{Bild } A$ für folgende Matrizen:

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \\ 3 & 4 & 5 \end{pmatrix} \in \mathbb{Q}^{3 \times 3} \quad A = \begin{pmatrix} 1 & 2 \\ 2 & 1 \\ 0 & 0 \\ 1 & 2 \end{pmatrix} \in (\mathbb{F}_3)^{4 \times 2}$$

$$A = \begin{pmatrix} 1 & 2 & 2 & -2 & -1 \\ -2 & -3 & -1 & 8 & 1 \\ 1 & 4 & 8 & 8 & -4 \\ 2 & 5 & 7 & 2 & -4 \end{pmatrix} \in \mathbb{Q}^{4 \times 5}$$

Dabei bezeichnet $\mathbb{F}_3 = \mathbb{Z}/3$ den Körper mit 3 Elementen.

Übung 5.17 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 5.18 Sei

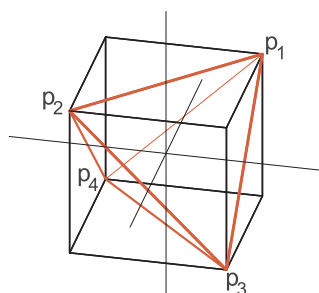
$$A = \begin{pmatrix} 1 & 2 & 2 & -2 \\ -2 & -3 & -1 & 8 \\ 1 & 4 & 8 & 8 \\ 2 & 5 & 7 & 2 \end{pmatrix} \quad \text{und} \quad b = \begin{pmatrix} 1 \\ -1 \\ 4 \\ 4 \end{pmatrix}$$

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

$$\begin{aligned} \mathbb{Q}^4 / \text{Ker}(A) &\longrightarrow \text{Bild}(A) \\ \bar{x} &\longmapsto A \cdot x. \end{aligned}$$

Übung 5.19 Betrachten Sie den Tetraeder T



mit den Ecken

$$\begin{aligned} p_2 &= \begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix} & p_1 &= \begin{pmatrix} -1 \\ 1 \\ 1 \end{pmatrix} \\ p_4 &= \begin{pmatrix} -1 \\ -1 \\ -1 \end{pmatrix} & p_3 &= \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix} \end{aligned}$$

Jede Bewegung des \mathbb{R}^3 , die 0 festhält, ist ein Homomorphismus $\mathbb{R}^3 \rightarrow \mathbb{R}^3$. 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 5.20 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 5.21 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 5.22 Sei $K = \mathbb{Q}$. Schreiben Sie eine Funktion, die für eine Matrix $T \in K^{n \times n}$

- 1) prüft, ob $T \in \text{GL}(n, K)$, 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 5.12, die Matrix $A \in \mathbb{Q}^{4 \times 4}$ aus Aufgabe 5.21.(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 5.21.(2).

Übung 5.23 Implementieren Sie für eine Matrix $A \in \mathbb{Q}^{n \times m}$ eine Funktion zur Bestimmung von $T \in \text{GL}(n, \mathbb{Q})$, sodass $T \cdot A$ Zeilenstufenform hat. Schreiben Sie auch eine Funktion, die aus $T \cdot A$ eine Basis von $\text{Ker } A$ berechnet.

Hinweis: Verwenden Sie z.B. die Funktion `RowOperation` der MAPLE-Bibliothek `LinearAlgebra`. Vergleichen Sie mit den Funktionen `GaussianElimination` und `NullSpace`.

Übung 5.24 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 $L_{(1,x,x^2,x^3)}^{(1,x,x^2)}(A) : \mathbb{Q}[x]_{\leq 2} \rightarrow \mathbb{Q}[x]_{\leq 3}$?

Übung 5.25 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 $T \in \text{GL}(4, \mathbb{Q})$ und $S \in \text{GL}(5, \mathbb{Q})$, sodass $T \cdot A \cdot S$ die Normalform

$$T \cdot A \cdot S = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}$$

hat, wobei $r = \text{rang } A$ und E_r die $r \times r$ Einheitsmatrix ist.

Übung 5.26 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 $T \in \text{GL}(3, \mathbb{Q})$ und $S \in \text{GL}(4, \mathbb{Q})$ sodass $T \cdot A \cdot S$ Normalform hat.

Übung 5.27 Berechnen Sie für die Matrizen in Aufgabe 5.17 jeweils die Determinante.

Übung 5.28 Seien a_1, \dots, a_{d+1} Elemente eines Körpers K . Die Matrix

$$A = \begin{pmatrix} 1 & a_1 & a_1^2 & \cdots & a_1^d \\ 1 & a_2 & a_2^2 & \cdots & a_2^d \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_{d+1} & a_{d+1}^2 & \cdots & a_{d+1}^d \end{pmatrix}$$

nennt man eine Vandermondsche Matrix. Zeigen Sie

$$\det A = \prod_{1 \leq i < j \leq d+1} (a_j - a_i)$$

Übung 5.29 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 5.30 Der ISBN-Code ist gegeben durch eine Identifikationsnummer aus 9 nichtnegativen ganzen Zahlen a_1, \dots, a_9 und einer zehnten Zahl $a_{10} \in \{1, \dots, 9, X\}$, wobei X für 10 steht, mit

$$\sum_{j=1}^{10} j a_j \equiv 0 \pmod{11}$$

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 5.31 Sei $s \geq 2$. Implementieren Sie Codierung, Fehlererkennung und Dekodierung für den Hamming-Code mit s Kontrollbits, z.B. in MAPLE.

Übung 5.32 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 $A \in \text{GL}(n, K)$ gilt

$$(A^t)^{-1} = (A^{-1})^t$$

4) Sei R ein kommutativer Ring. Überprüfen Sie, dass obige Aussagen auch für Matrizen mit Koeffizienten in R sinnvoll sind.

Übung 5.33 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 5.34 Diagonalisieren Sie

$$A = \begin{pmatrix} 5 & -5 & -5 \\ 1 & -1 & -1 \\ 3 & -3 & -3 \end{pmatrix} \in \mathbb{Q}^{3 \times 3} \quad \text{und} \quad B = \begin{pmatrix} 2 & 1 & 1 \\ 2 & 2 & 1 \\ -2 & 1 & 2 \end{pmatrix} \in \mathbb{Q}^{3 \times 3}$$

Übung 5.35 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 5.36 Für $a_{d-1}, \dots, a_0 \in \mathbb{R}$ sei V der Vektorraum der Folgen (b_n) , die der linearen Rekursionsgleichung

$$b_{n+d} = a_{d-1}b_{n+d-1} + \dots + a_0b_n \quad \forall n \geq 0$$

genügen. Zeigen Sie:

1) V ist ein d -dimensionaler \mathbb{R} -Vektorraum.

2) Die Indexshift-Abbildung $T : V \rightarrow V$, $(b_0, b_1, \dots) \mapsto (b_1, b_2, \dots)$ ist ein Endomorphismus. Bestimmen Sie die Matrixdarstellung von T bezüglich einer geeigneten Basis von V .

3) Das charakteristische Polynom von T ist

$$\chi_T(t) = t^d - (a_{d-1}t^{d-1} + \dots + a_1t + a_0)$$

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.

Index

- Äquivalenzrelation, 20
- linearer Code, 208
- Abbildung, 12
- abelsch, 50
- abzählbar, 168
- AES, 114
- affine Gerade, 180
- affine Unterräume, 180
- Algebra, 106
- algebraische Körpererweiterung, 109
- algebraische Vielfachheit, 232
- allgemeine lineare Gruppe, 198
- alternierende Gruppe, 59
- antisymmetrisch, 18
- Anzahl der Elemente, 7
- assoziativ, 17
- Assoziativität, 49
- assoziiert, 141
- aufgespannter Untervektorraum, 159
- Aufpunkt, 180
- Bahn, 66
- Bahngleichung, 80
- Basis, 161
- Basiswechsel, 201
- Bewegung, 63
- Bewegungsgruppe, 63
- bijektiv, 13
- Bild, 12, 56
- Cantor, Georg, 4
- Cardano, Geronimo, 3
- Charakteristik, 125
- charakteristisches Polynom, 231
- Chinesischer Restsatz, 131
- coprim, 130
- darstellende Matrix, 186
- Determinantenabbildung, 220
- diagonalisierbar, 231
- Diagonalmatrix, 224
- Diffie-Hellman key exchange, 119
- Dimension, 168
- direkte Summe, 232
- diskreter Logarithmus, 119
- Division mit Rest, 30, 126
- Dreiecksungleichung, 213
- Durchschnitt von Idealen, 130
- Eigenraum, 229
- Eigenvektor, 229
- Eigenwert, 229
- Einheit, 101, 110
- Einheitengruppe, 101, 110
- Einheitsmatrix, 193
- Einheitsvektoren, 162
- Einselement, 103
- Einsetzungshomomorphismus, 107
- Element, 4
- elementare Spaltentransformationen, 195
- elementare Zeilenoperationen, 189

- endlichdimensional, 168
- Endomorphismus, 230
- Epimorphismus, 57
- erweiterter Euklidischer Algorithmus, 36
- Erzeugendensystem, 121, 160
- Erzeuger, 60
- Euklidische Bewegungen, 63
- euklidische Norm, 126
- Euklidischer Algorithmus, 127
- euklidischer Ring, 126
- Euklids erster Satz, 34
- Euklids zweiter Satz, 34
- Eulersche Phi-Funktion, 111
- Exponentialfunktion, 58
- faktorieller Ring, 128
- fehlererkennend, 212
- fehlerkorrigierend, 213
- Fermat, Pierre de, 1
- Fermats letzter Satz, 1
- Ferrari, Lodovico, 3
- freie Gruppe, 52
- Fundamentalsatz der Algebra, 110
- Galois, Evariste, 3
- ganze Zahlen, 5
- Gaußalgorithmus, 148
- Gaußsche Zahlen, 109
- genau dann wenn, 5
- Generatormatrix, 207
- geometrische Vielfachheit, 232
- gerade Zahlen, 103
- größter gemeinsamer Teiler, 35, 127
- Grad, 105
- Graph, 82
- Graph einer Abbildung, 12
- Gruppe, 49
- Gruppe der Restklassen, 54
- Gruppe der Selbstabbildungen, 51, 62, 73
- Gruppentafel, 55
- Halbgruppe, 50
- Halbordnung, 18
- Hamming-Code, 214
- Hammingabstand, 212
- Hauptidealring, 128
- homogen, 146
- Ideal, 121
- identische Abbildung, 17
- Index, 76
- Indexformel, 76
- Induktionsanfang, 8
- Induktionsschritt, 9
- Induktionsvoraussetzung, 9
- inhomogenes lineares Gleichungssystem, 177
- injektiv, 13
- Integritätsring, 101, 123
- Inverses, 49
- invertierbar, 197
- ISBN-Nummer, 212
- isomorphe Graphen, 82
- Isomorphismus, 57
- Jordansche Normalform, 234
- Körper, 102, 110
- kanonische Abbildung, 20
- Kanten eines Graphen, 82
- Kartesisches Produkt von Gruppen, 53
- Kartesisches Produkt von Mengen, 7
- Kern, 56

- Kleiner Satz von Fermat, 111
 Kleinsche Vierergruppe, 90
 kleinstes gemeinsames Vielfaches, 35
 kommutativ, 50, 103
 kommutativer Ring, 103
 kommutativer Ring mit 1, 99
 Komplement, 5
 kongruent, 31
 Konjugation, 94
 Konjugationsklasse, 95
 Kontrollbits, 207
 Kontrollmatrix, 210
 Koordinatendarstellung, 172

 Lagrangepolynom, 136
 leere Menge, 4
 Leitkoeffizient, 147
 Leitmonom, 147
 Leitterm, 147
 Leitvariable, 147
 linear abhängig, 161
 linear unabhängig, 161
 lineares Gleichungssystem, 145
 Linearkombination, 159
 Linearkombinations-Abbildung, 172

 Mächtigkeit, 7
 Markovmatrix, 229
 Matrix, 174
 Matrixmultiplikation, 175
 Matrizenprodukt, 187
 Menge, 4
 Minimalabstand, 212
 Modul, 155
 Monoid, 50
 Monomorphismus, 57
 Moores Gesetz, 114
 multilinear, 221
 natürliche Zahlen, 5
 Nearest-Neighbour-Dekodierung, 213
 Nebenklassen, 75
 neutrales Element, 49
 Normalform, 203
 Normalteiler, 86
 Nullring, 103
 Nullteiler, 101, 123

 OE, 9
 ohne Einschränkung der Allgemeinheit, 9
 Operation, 62
 Orbit, 66
 Ordnung, 50
 Ordnung eines Gruppenelements, 61

 Parallelepipid, 220
 Paritybits, 207
 partitionieren, 20
 Peano-Axiome, 27
 perfect forward secrecy, 119
 Permutation, 51
 Pollard Faktorisierung, 118
 Pollard, John, 117
 Polynomring, 105
 Potenzmenge, 8
 prime Restklassen, 111
 prime Restklassengruppe, 111
 Primfaktor, 32
 Primfaktorzerlegung, 32
 Primzahl, 32
 Primzahlsatz, 34
 Probedivision, 37
 Public-Key-Kryptosystem, 114

 Quelle, 12
 Quotient, 67

- Quotientenabbildung, 67
 Quotientengruppe, 87
 Quotientenring, 121
 Quotientenvektorraum, 205

 Rang, 176
 rationale Funktionen, 124
 rationale Zahlen, 5
 reduzierte Spaltenstufenform, 196
 reduzierte Zeilenstufenform, 149, 193
 reflexiv, 18
 rekursiver Algorithmus, 11
 Relation, 11
 Repräsentant, 20
 Repräsentant einer Bahn, 67
 Restklasse, 32
 Restklassengruppe, 54, 100
 Ring, 102
 Ring mit 1, 103
 Ringhomomorphismus, 104
 RSA, 114

 Scherung, 218
 Schlüssel, öffentlicher, 114
 Schlüssel, privater, 114
 Sieb des Eratosthenes, 39
 Signatur, 59
 Signum, 59
 simultane Kongruenz, 40
 Skalarmultiplikation, 106
 Spaltenstufenform, 195
 sparse matrix, 201
 Stabilisator, 67
 Stammfunktion, 176
 Standardbasis, 162
 Substitutionshomomorphismus, 107
 Summe von Idealen, 130
 surjektiv, 13

 Symmetriegruppe, 63
 symmetrisch, 19
 symmetrische Gruppe, 51

 Tail, 147
 Tartaglia, Nicolo, 3
 teilerfremd, 31
 Teilmenge, 5
 teilt, 31
 Tetraeder, 79
 Totalordnung, 18
 transitiv, 18
 Transponierte, 209
 Transposition, 51
 Trapdoor-Einwegfunktion, 114

 Umkehrabbildung, 15
 Untergruppe, 53
 Unterring, 103
 Untervektorraum, 156
 Urbild, 12

 Vektor, 153
 Vektorraum, 153
 Vektorraumhomomorphismus, 173
 Vereinigung, 5
 Verknüpfung, 49
 Verknüpfungstafel, 73
 Vertex eines Graphen, 82
 vollständiges Repräsentantensystem, 67

 Wiles, Andrew, 2
 Wort, 52

 Zeilenstufenform, 149, 191
 Ziel, 12
 Zykel, 68
 zyklisch, 60

Literaturverzeichnis

- [1] M. Artin: Algebra, Birkhäuser (2003).
- [2] S. Bosch: Algebra, Springer (1993).
- [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] P. Bundschuh: Einführung in die Zahlentheorie, Springer (1998).
- [9] Decker, W.; Greuel, G.-M.; Pfister, G.; Schönemann, H.: SINGULAR 4-0-2 — *A computer algebra system for polynomial computations*. <http://www.singular.uni-kl.de> (2012).
- [10] G. Fischer: Lineare Algebra, Vieweg (2010).
- [11] G. Fischer, R. Sacher: Einführung in die Algebra, Teubner (1983).
- [12] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4.12*; <http://www.gap-system.org>, (2008).

- [13] G.H. Hardy, E.M. Wright: An introduction to the theory of numbers, Oxford (1956).
- [14] J. C. Jantzen, J. Schwermer: Algebra, Springer (2006).
- [15] C. Karpfinger, K. Meyberg: Algebra, Spektrum Akademischer Verlag (2008).
- [16] E. Kunz: Algebra, Vieweg (1994).
- [17] B. Kreußler, G. Pfister: Mathematik für Informatiker: Algebra, Analysis, Diskrete Strukturen, Springer (2009).
- [18] Maple (Waterloo Maple Inc.): Maple 16, <http://www.maplesoft.com/> (2012).
- [19] R. Remmert, P. Ullrich: Elementare Zahlentheorie, Birkhäuser (1987).
- [20] P. Ribenboim: Die Welt der Primzahlen, Springer (2006).
- [21] R. Schulze-Pillot: Einführung in die Algebra und Zahlentheorie, Springer (2008).
- [22] V. Shoup: A Computational Introduction to Number Theory and Algebra, Cambridge University Press (2005).
- [23] W. Willems: Codierungstheorie und Kryptographie, Birkhäuser (2008).
- [24] J. Wolfart: Einführung in die Algebra und Zahlentheorie, Vieweg (1996).
- [25] G. Wüstholtz: Algebra, Vieweg (2004).