Algebra und Diskrete Strukturen für

Grundschullehramt

WS 2018/2019

Christian Sevenheck

Fakultät für Mathematik

TU Chemnitz

vorläufige Fassung, 19. Dezember 2018

Fehler und Bemerkungen bitte an : christian.sevenheck@mathematik.tu-chemnitz.de

Inhaltsverzeichnis

Kapitel 1

Einführung, Überblick und Vorbemerkungen

Einige Bemerkungen zum Ziel und zum Sinn der Vorlesung:

1.) Es geht hier um mathematische Grundlagen (Mengenlehre, Logik etc.), sowie um Algebra und Arithmetik (Zahlensysteme, Matrizen, Teilbarkeit etc.).

2.) Es geht nicht um Didaktik (eigene VL) und auch nicht um Stoff der Grundschule (der ist Ihnen hoffentlich schon bekannt).

3.) Hoffnung/Wunsch: Diese (und andere) Mathematik-Vorlesung gibt Ihnen einen kleinen Einblick in das Fach aus der Sicht eines „echten“ Wissenschaftlers. Es geht neben den konkreten Inhalten vor allem um mathematische Denkweisen und Strategien zur Lösung von Problemen. Idealerweise sollen Sie dies in Ihren späteren Unterricht einfließen lassen und damit Schülern abstraktes Denken, aber auch den Spaß an Mathematik näherbringen.

Warum brauchen wir Mathematik?

Mathematik kommt überall vor! 3 (originelle) Beispiele:

1.) allgemeine Relativitätstheorie und GPS
Ohne Berücksichtigung der Raumkrümmung rechnet GPS ca. 10-50m falsch.

2.) algebraische Topologie und Stahlverarbeitung
Flüssiger Stahl wird häufig in Magnetfeldern gehalten. Hierfür wählt man oft die Form eines Torus ($\hat{=}$ Donut), weil ein Magnetfeld auf einer Kugeloberfläche einen Nullpunkt hat (Satz von Igel) $\Rightarrow$ Stahl läuft aus.

3.) Polynomringe und CD-Player
Eine CD kann Kratzer bekommen. Dann springt aber nicht einfach die Wiedergabe (wie bei einer Schallplatte), sondern es fehlen Informationen, da Musik ja digitalisiert abgespeichert wird. Trotzdem spielt der CD-Player weiter (wenn der Kratzer nicht zu groß ist). Warum?
Idee: Musik wird in sogenannten fehlertoleranten oder selbstkorrigierenden Codes abgespeichert. Hierzu verwendet man z. B. Polynomdivision.

Grundsätzlich gilt: Alle Naturwissenschaften, fast alle Sozialwissenschaften, alle Ingenieurwissenschaften sind ohne Mathematik verloren (meistens sehr alte/klassische Mathematik, aber nicht immer, siehe oben). Daher ist guter Mathematikunterricht in der Schule essentiell für die Zukunft der Gesellschaft.

Bereiche der Mathematik im Lehramtsstudium in Chemnitz

- Analysis: Konstruktion der reellen Zahlen, Folgen, Reihen, Grenzwerte, Stetigkeit, Differenzierbarkeit
- Geometrie: axiomatischer Aufbau der Geometrie, ebene und räumliche Geometrie, Konstruktionen
- Stochastik: Wahrscheinlichkeitsrechnung, Kombinatorik
- Algebra: Grundlagen (Mengen + Logik), Zahlbereiche ($\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$), Teilbarkeit, Gruppen, Ringe, Körper, lineare Algebra (Matrizen etc.)

Beispiele zur Algebra

1.) Primzahlen: Eine natürliche Zahl $p > 1$ heißt Primzahl, falls sie nur von 1 und sich selbst geteilt wird. Welche/wieviele Primzahlen gibt es? Wie findet man sie etc.

$$2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$$

Wieviele: unendlich viele (Euklid, Antike)
Wie verteilt: schwer/ungelöst
Wie findet man sie: viele Methoden/Tests für Perfomance von Computern

2.) Teilbarkeit: Natürliche Zahlen kann man mit Rest durcheinander teilen. a und b heißen kongruent modulo m (geschrieben $a \equiv b \quad (m)$), falls sie den gleichen Rest bei Division durch m haben. Wenn wir Reste r, p und Zahlen m, n vorgeben, gibt es dann eine Zahl a mit $a \equiv r \quad (m)$ und $a \equiv p \quad (n)$?
Antwort: ja, falls m, n teilerfremd sind (Chinesischer Restsatz).

3.) Lineare Gleichungssysteme:
lineare Gleichung: $a \cdot x = b$
Lösung: $x = \frac{b}{a}$ (einfach)
Gegeben zwei oder mehr lineare Gleichungen, z. B. $ax+by = c, dx+ey = f$. Fragen: Lösungen? Wieviele (endlich/unendlich)? Wie finden?
Idee: Matrizengleichung $\begin{pmatrix} a & b \\ d & e \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} c \\ f \end{pmatrix} \ldots$

Einige organisatorische Bemerkungen:

Jede Woche 2×90min Vorlesung. Hier werden Konzepte und allgemeine Aussagen vorgestellt und erläutert. Es kommen häufig vor: Definitionen, hier wird für ein bestimmtes Objekt oder eine Klasse von Objekten ein Name festgelegt, d. h., bei einer Definition muss man nicht begründen, dass sie wahr ist. Aussagen werden formuliert als Satz (sehr wichtig), Proposition (nicht ganz so wichtig) oder Lemma (eher eine Nebenaussage, welche eventuell für einen späteren Satz oder eine Proposition gebraucht wird). Alle diese Aussagen sollen wahr sein, und dies muss man (nach der Aussage) in einem Beweis begründen. In diesem darf nur streng logisch vorgegangen werden. Aus der Voraussetzung der Aussage muss durch den Beweis zweifelsfrei die Konklusion hergeleitet werden. Falls eine (kleinere) Aussage direkte Konsequenz eines Satzes oder einer Proposition ist, wird sie auch als Korollar bezeichnet.

In der Vorlesung werden auch (einige) Beispiele vorgerechnet. Hauptsächlich ist hierfür die Übung zuständig. Es gibt jede Woche ein Übungsblatt, welches Sie bitte bis zur nächsten Woche lösen und abgeben. Die Aufgaben werden korrigiert und in der übernächsten Woche in der Übung besprochen. Wichtig: Bearbeiten der Aufgaben ist essentiell, nur „Hören“ der Vorlesung bringt (fast) nichts. Es wird eventuell handschriftliche Notizen zur Vorlesung geben, aber nur mit Zeitverzögerung, also bitte mitschreiben!

Prüfungen finden mündlich statt, Termine werden am Ende der Vorlesungszeit vereinbart.

Kapitel 2

Logik, Mengenlehre und Abbildungen

In diesem Abschnitt werden einige grundlegende Notationen und Konzepte eingeführt. Wir beginnen mit Mengen:

Definition 2.1. *Eine Menge M (oder A oder B oder irgendein anderer Buchstabe) ist eine vorgegebene (wohldefinierte) Sammlung von Objekten, dies sind die Elemente der Menge. Man schreibt:*

$$x \in M : x \text{ ist Element von } M$$

$$x \notin M : x \text{ ist nicht Element von } M$$

Beispiele:

- $\mathbb{N} = \{1, 2, 3, \ldots\}$ ({} sind die Mengenklammern): Die Menge der natürlichen Zahlen.
- explizit gegebene endliche Mengen: $M_1 = \{a, b, c\}, M_2 = \{1, 2, 3\}$ oder $M_3 = \{a, 4, *, \circ, \smiley\}$.
- $\mathbb{Z} = \{0, 1, -1, 2, -2, \ldots\}$: Die Menge der ganzen Zahlen.
- $\mathbb{Q} = \{0, \pm 1, \pm\frac{1}{2}, \pm\frac{1}{3}, \pm\frac{1}{4}, \ldots, \pm 2, \pm\frac{2}{3}, \pm\frac{2}{5}, \ldots\}$: Die Menge der rationalen Zahlen.
- $\mathbb{R}$ = Die Menge der reellen Zahlen ($2,7 \in \mathbb{R}$, $3,99\ldots \in \mathbb{R}$ etc. : Analysis-VL).
- Die Menge aller Studierenden der TU Chemnitz (~ 11000).
- Die Menge aller Atome im Weltall ($\sim 10^{80}$).
- $\mathbb{Q}_+ = \mathbb{Q}_{>0} := \{x \in \mathbb{Q} | x > 0\}, \mathbb{Q}_{\geq 0} := \{x \in \mathbb{Q} | x \geq 0\}$ ($:=$ heißt definiert durch)
- Intervalle $[a, b] := \{x \in \mathbb{R} | \overbrace{a \leq x \leq b}^{(*)}\}$ = Menge aller $x \in \mathbb{R}$, welche die Bedingung $(*)$ errfüllen,
  $(a, b] := \{x \in \mathbb{R} | a < x \leq b\}$, analog $[a, b)$ und (a, b).
- Die leere Menge $M = \{\}$, welche kein Element enthält. Man schreibt dann $M = \varnothing$.
- Mengen können Mengen enthalten: $M = \{\{1, 2, 3\}, \{1, 2, 3, 4\}\}$ hat 2 Elemente.
- Sei M eine gegebene Menge, dann definiert man die Potenzmenge $\mathcal{P}(M) := \{B | B \subset M\}$ ($B \subset M$ heißt B ist enthalten in oder Teilmenge von M).

  Beispiel: $M = \{a, b, c\}, \mathcal{P}(M) = ?$

  Bilde alle möglichen Teilmengen von M:
  $\mathcal{P} = \{\varnothing, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$

Neue Mengen entstehen vor allem durch Verknüpfung gegebener Mengen mithilfe der folgenden Operationen.

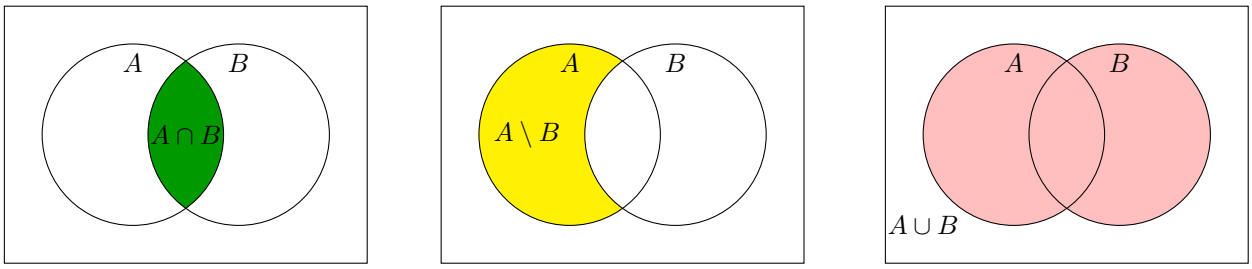
Definition 2.2. *Seien A, B Mengen, dann heißt*

$A \cup B := \{x | x \in A \text{ oder } x \in B\}$
die Vereinigung von A und B,

$A \cap B := \{x | x \in A \text{ und } x \in B\}$
der Durchschnitt von A und B,

$A \setminus B := \{x \in A | x \notin B\}$ *(gesprochen: A ohne B)*
das Komplement von B in A.

Man kann diese Operationen durch Diagramme veranschaulichen:



Beispiele:
$\mathbb{N}_0 = \mathbb{N} \cup \{0\}, \mathbb{N} = \mathbb{N}_0 \setminus \{0\}, \mathbb{Z} = \mathbb{N} \cup \{0\} \cup (-\mathbb{N})$, wobei $-\mathbb{N} := \{-n | n \in \mathbb{N}\}$, analog: $-\mathbb{N}_0$.
$\mathbb{N}_0 \cap (-\mathbb{N}_0) = \{0\}, \mathbb{N} \cap (-\mathbb{N}) = \varnothing$.

Bezeichnung (schon verwendet):
$A \subset B$ (A liegt in B, A ist Teilmenge von B): Falls $x \in A$, dann gilt auch $x \in B$.
$A \not\subset B$ (A liegt nicht in B): Es gibt ein $x \in A$, so dass $x \notin B$.
$A \subsetneq B$ (A ist echte Teilmenge von B): $A \subset B$ und $A \neq B$.

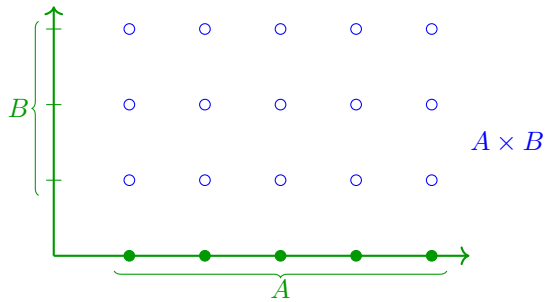
Beispiele:
$\mathbb{N} \subset \mathbb{N}_0, \mathbb{N}_0 \subset \mathbb{N}_0, \mathbb{N} \subsetneq \mathbb{N}_0,$ aber $\mathbb{N}_0 \not\subset \mathbb{N}$.

Eine wichtige Konstruktion, um neue Mengen aus Gegebenen zu erzeugen, ist das kartesische Produkt von Mengen.

Definition 2.3. *Seien A und B nicht-leere Mengen, dann definieren wir*

$$A \times B := \{(a, b) | a \in A, b \in B\}$$

Für endliche Mengen kann man das Produkt durch Punkte in der Ebene veranschaulichen:



Es gilt: $(a,b) = (a',b')$ genau dann, wenn $a = a'$ und $b = b'$.

Bemerkung: Will man Mengen präziser einführen, benutzt man gewisse Axiome (z. B. nach Zermelo-Fraenkel). Aus diesen folgt z. B. , dass es keine Menge aller Mengen gibt. Dies kann man auch so begründen: Sei M die Menge aller Mengen (angenommen, es gäbe sie). Sei $N := \{X \in M | X \notin X\}$. Dann folgt:

$$\left.\begin{array}{l} 1.) N \notin N \Rightarrow N \in N \\ 2.) N \in N \Rightarrow N \notin N \end{array}\right\} \text{sogenannte Russelsche Antinomie}$$

Also kann so eine Menge M nicht existieren.

Sehr viele Mengen kann man so bilden: Sei M eine Menge und sei für $x \in M$ eine logische Aussage $A(x)$ gegeben. Dann ist $N := \{x \in M | A(x) \text{ ist wahr}\}$ wieder eine Menge. Dies führt zur Definition logischer Aussagen.

Definition 2.4. *Eine logische Aussage ist eine Äußerung, die ohne jeden Zweifel entweder wahr oder falsch ist, z. B. :*

- *Heute ist Mittwoch* — *wahr (nur heute)*
- $2 > 1$ — *wahr*
- $1 < -2$ — *falsch*
- $\sqrt{2} \in \mathbb{Q}$ — *falsch (später genauer)*

Sehr wichtig zur Formulierung von Aussagen sind Quantoren, welche festlegen, für welche Objekte eine Aussage gilt:

- $\forall$ bedeutet „für alle“
- $\exists$ bedeutet „es gibt ein“
- $\exists!$ bedeutet „es gibt genau ein“
- $\nexists$ bedeutet „es gibt kein“

Beispiele:
-$\forall x \in \mathbb{N} : x > 0$,
-$\exists x \in \mathbb{N}_0 : x \in -\mathbb{N}_0$ (nämlich $x = 0$), sogar: $\exists! x \in \mathbb{N}_0 : x \in -\mathbb{N}_0$, aber: $\nexists x \in \mathbb{N} : x \in -\mathbb{N}$.

Neue Aussagen entstehen durch logische Verknüpfungen.

Definition 2.5. *Seien A und B Aussagen, dann schreiben wir:*

- $A \Rightarrow B$*: aus A folgt B.*
- $A \Leftrightarrow B$*: A genau dann, wenn B oder A ist äquivalent zu B.*
- $A \vee B$*: A oder B.*
- $A \wedge B$*: A und B.*
- $\neg A$*: nicht A.*

Solche oder kompliziertere Verknüpfungen (z. B. $\neg(A \wedge B) \vee C$) kann man durch Wahrheitstafeln überprüfen.

A	B	$A \wedge B$	$A \vee B$	$A \Rightarrow B$	$A \Leftrightarrow B$	$\neg A$
w	w	w	w	w	w	f
w	f	f	w	f	f	f
f	w	f	w	w	f	w
f	f	f	f	w	w	w

Damit kann man die folgenden logischen Aussagen beweisen.

Satz 2.6. *Die folgenden Aussagen sind unabhängig vom Wahrheitswert der Aussagen A, B und C immer wahr:*

1.) $A \vee \neg A$

2.) $\neg\neg A \Leftrightarrow A$

3.) $A \wedge B \Leftrightarrow B \wedge A$,
$A \vee B \Leftrightarrow B \vee A$

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

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

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

Beweis. Hier nur 4.):

A	B	$\neg(A \wedge B)$	$\neg A \vee \neg B$
w	w	f	f
w	f	w	w
f	w	w	w
f	f	w	w

Rest: Übung

□

Bemerkung: Negation von quantifizierten Aussagen: Die Quantoren $\exists, \forall$ werden durch Negation ausgetauscht, z. B. : Seien A, B Mengen. Aussage: $A \subset B$. Anders formuliert: $\forall x \in A : x \in B$. Die Negation ist $A \not\subset B$. Dies schreibt sich mit Quantoren: $\exists x \in A : x \notin B$. Analog andersherum, d. h.z.B:

Aussage: $\exists m \in \mathbb{Z} : m^2 < 0$ (falsche Aussage)
Negation: $\forall m \in \mathbb{Z} : m^2 \geq 0$ (wahre Aussage)

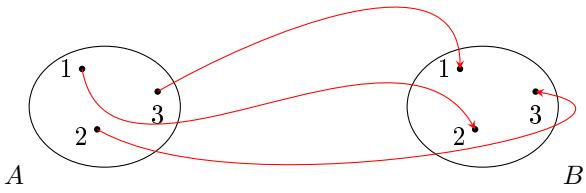
Nun wollen wir den in der ganzen Mathematik fundamentalen Begriff der Abbildung diskutieren.

Definition 2.7. *Seien A, B Mengen. Eine Abbildung f ist eine Zuordnung, welche jedem $x \in A$ genau ein Element aus B, genannt $f(x)$ zuordnet. Wir schreiben:*

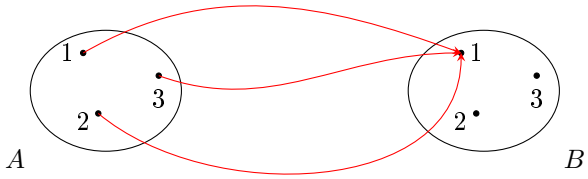
$$\begin{aligned} f : A &\to B \\ x &\mapsto f(x) \end{aligned}$$

Beispiele:

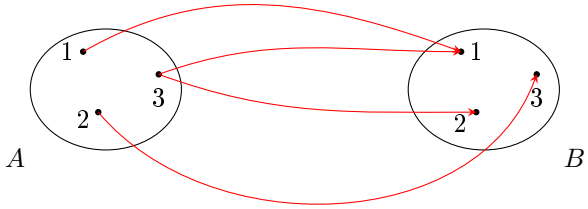
- Abbildungen zwischen endlichen Mengen kann man explizit angeben: $A = B = \{1, 2, 3\}, f : A \to B : f(1) = 2, f(2) = 3, f(3) = 1$.
  graphisch:



oder $f(1) = f(2) = f(3) = 1$



Aber: das folgende Bild gehört zu keiner Abbildung



(hier ist $f(3)$ nicht eindeutig bestimmt.)

- $f : \mathbb{N}_0 \to \mathbb{N}; x \mapsto x + 1$
- $f : \mathbb{R} \to \mathbb{R}; x \mapsto x^3$
- $f : \mathbb{R} \to \mathbb{R}_+; x \mapsto x^2$ (Erinnerung: $\mathbb{R}_+ = \{x \in \mathbb{R} | x \geq 0\}$)
- M beliebige Menge, $f : M \to M; x \mapsto x$, (identische Abbildung oder Identität), geschrieben id_M

Wichtig sind häufig spezielle Arten von Abbildungen

Definition 2.8. *Eine Abbildung $f : A \to B$ heißt*

1.) injektiv genau dann, wenn gilt

$$\forall x, y \in A : x \neq y \Rightarrow f(x) \neq f(y).$$

(Äquivalent: $\forall x, y \in A : f(x) = f(y) \Rightarrow x = y$)

2.) surjektiv genau dann, wenn gilt

$$\forall b \in B : \exists a \in A : f(a) = b.$$

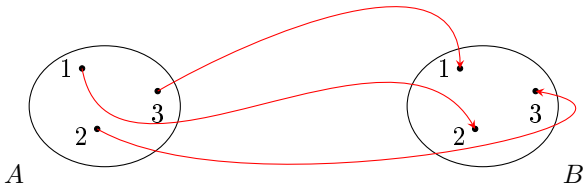
Für eine beliebige Abbildung $f : A \to B$ heißt $f(A)$ das Bild von f, geschrieben $\mathrm{im}(f)$. *Also gilt*

$$f \text{ surjektiv} \Leftrightarrow \mathrm{im}(f) = B.$$

3.) bijektiv genau dann, wenn f injektiv und surjektiv ist.

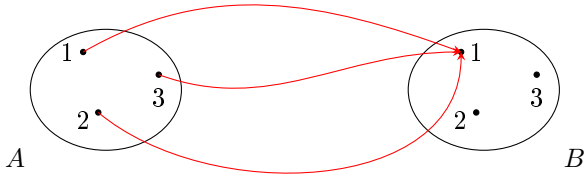
Beispiele:

-



ist bijektiv.

-



ist nicht injektiv ($f(1) = f(2) = f(3) = 1$) und nicht surjektiv ($\nexists a \in A = \{1, 2, 3\} : f(a) = 2$). (Also auch nicht bijektiv.)

- $f : \mathbb{N}_0 \to \mathbb{N}; x \mapsto x + 1$ ist bijektiv. (Achtung: $\mathbb{N} \subsetneq \mathbb{N}_0$, aber f ist trotzdem bijektiv. So etwas kann bei endlichen Mengen nicht passieren.)
- $f : \mathbb{R} \to \mathbb{R}; x \mapsto x^3$ ist bijektiv.
- $\exp : \mathbb{R} \to \mathbb{R}; x \mapsto e^x$ ist injektiv, nicht surjektiv.
- $f : \mathbb{R} \to \mathbb{R}_+; x \mapsto x^2$ ist surjektiv, nicht injektiv.

Manchmal kann man Abbildungen verknüpfen oder umkehren.

Definition 2.9. *Es seien Abbildungen $f : A \to B$ und $g : B \to C$ gegeben, dann definieren wir $g \circ f : A \to C$ durch*

$$(g \circ f)(a) \coloneqq \overbrace{g(\underbrace{f(a)}_{\in B})}^{\in C} \forall a \in A.$$

Übung:

f, g injektiv (surjektiv, bijektiv) $\Rightarrow g \circ f$ injektiv (surjektiv, bijektiv).

$g \circ f$ surjektiv $\Rightarrow g$ surjektiv.

$g \circ f$ injektiv $\Rightarrow f$ injektiv.

Satz 2.10. *Sei $f : A \to B$ eine bijektive Abbildung. Dann gibt es genau eine Abbildung $g : B \to A$, so dass $g \circ f = id_A$ und $f \circ g = id_B$ gilt.*

Beweis. $\forall b \in B : \exists! a \in A : f(a) = b$ (da f bijektiv: Existenz von a, da f surjektiv, Eindeutigkeit, da f injektiv) Setze daher: $g(b) := a$, dies definiert $g : A \to B$ und es gilt: $(f \circ g)(b) = f(g(b)) = f(a) = b$. Also ist $f \circ g = id_B$. Und $(g \circ f)(a) = g(f(a)) = g(b) = a$, also ist $g \circ f = id_A$.

Da g wie oben definiert werden muss (um $g \circ f = id_A$ und $f \circ g = id_B$ zu erreichen), ist es eindeutig und wird mit f^{-1} bezeichnet und Umkehrabbildung genannt.

□

Anwendung: Kardinalität von Mengen.

Definition 2.11. *Sei A eine Menge. Die Kardinalität von A (oder die Mächtigkeit von A), geschrieben* $\mathrm{card}(A), |A|$ *oder auch $\#A$ oder $\overline{A}$ ist die Anzahl der Elemente von A, falls A endlich ist. Falls A unendlich ist, setzen wir $|A| := \infty$. Es gilt also* $\mathrm{card}(A) \in \mathbb{N}_0 \cup \{\infty\}$ *(denn* $\mathrm{card}(\varnothing) = 0 \in \mathbb{N}_0$*).*

Zwei Mengen A und B haben per Definition die gleiche Kardinalität (oder sind gleichmächtig), falls es eine Bijektion $f : A \to B$ gibt.

Bemerkungen:

- Falls $|A| < \infty, |B| < \infty$ (d. h. A und B sind endliche Mengen), dann gilt:
  A und B sind gleichmächtig $\Leftrightarrow |A| = |B|$.
- Für unendliche Mengen können interessante Phänomene auftreten, z. B. (siehe oben): $\mathbb{N} \subsetneq \mathbb{N}_0$, aber die Abbildung $f : \mathbb{N}_0 \to \mathbb{N}; n \mapsto n + 1$ ist bijektiv. d. h., $\mathbb{N}$ und $\mathbb{N}_0$ sind gleichmächtig. Veranschaulichen kann man dies mit dem Gedankenexperiment des „Hilberthotels“ (nach David Hilbert), siehe Übungen.

Kapitel 3

Die klassischen Zahlbereiche

Wir kennen alle aus der Schule die natürlichen Zahlen, und zwar schreiben wir

$$\mathbb{N} = \{1, 2, 3, 4, \ldots\}$$

Es ist relativ schwierig, die natürlichen Zahlen mathematisch präzise einzuführen (dies machen wir später), aber es ist intuitiv klar, wie wir mit natürlichen Zahlen rechnen: für $n, m \in \mathbb{N}$ können wir $n+m$ und $n \cdot m \in \mathbb{N}$ bilden.
Wir nennen $\mathbb{N}_0 := \{0\} \cup \mathbb{N} = \{0, 1, 2, \ldots\}$ die Menge der natürlichen Zahlen mit Null. Die Null ist wichtig, um Zahlen im Dezimalsystem schreiben zu können: $156 = 100 + 50 + 6$.
Wir können natürliche Zahlen nicht immer subtrahieren: die Gleichung $x + 5 = 3$ hat keine Lösung $x \in \mathbb{N}$, aber natürlich die Lösung $x = -2$. Dies führt zu den ganzen Zahlen:

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

Aber auch in $\mathbb{Z}$ können wir z. B. die Gleichung $x \cdot 3 = 5$ nicht lösen, hierfür brauchen wir Brüche oder rationale Zahlen:

$$\mathbb{Q} := \left\{ \frac{a}{b} \middle| a \in \mathbb{Z}, b \in \mathbb{N} \right\}$$

Wir bemerken, dass wir in $\mathbb{Q}$ nun alle vier Grundrechenarten: $+$ (Plus oder Addition), $-$ (Minus oder Subtraktion), $\cdot$ (Mal oder Multiplikation) und / (Teilen oder Division) durchführen können, außer natürlich der Division durch 0. Die folgenden Rechenregeln gelten in $\mathbb{Q}$ (und sind intuitiv klar):

Für die Addition:

A1) $\forall x, y, z \in \mathbb{Q} : (x + y) + z = x + (y + z)$
Assoziativität der Addition.

A2) $\forall x, y \in \mathbb{Q} : x + y = y + x$
Kommutativität der Addition.

A3) $\forall x \in \mathbb{Q} : 0 + x = x + 0 = x$
0 ist das neutrale Element bezüglich $+$.

A4) $\forall x \in \mathbb{Q} : \exists y \in \mathbb{Q} : x + y = 0$
y ist das Negative von x oder das zu x bezüglich$+$ inverse Element.

Für die Multiplikation:

M1) $\forall x, y, z \in \mathbb{Q} : (x \cdot y) \cdot z = x \cdot (y \cdot z)$
Assoziativität der Multiplikation.

M2) $\forall x, y \in \mathbb{Q} : x \cdot y = y \cdot x$
Kommutativität der Multiplikation.

M3) $\forall x \in \mathbb{Q} : 1 \cdot x = x \cdot 1 = x$
1 ist das neutrale Element bezüglich $\cdot$.

M4) $\forall x \in \mathbb{Q}, x \neq 0 : \exists y \in \mathbb{Q} : x \cdot y = 1$
y ist das zu x bezüglich $\cdot$ inverse Element.

Verträglichkeit von Addition und Multiplikation:

D) $\forall x, y, z \in \mathbb{Q} : (x + y) \cdot z = x \cdot z + y \cdot z$
Distributivgesetz.

In der Algebra (und eigentlich in der gesamten Mathematik) benutzt man Mengen mit zwei Verknüpfungen, welche genau diese Rechenregeln erfüllen. Deshalb gibt man solchen Objekten einen Namen.

Definition 3.1. *Eine Menge K, welche mindestens zwei verschiedene Elemente, geschrieben 0 und 1, enthält, und auf der zwei Rechenoperationen $+$ und $\cdot$ definiert sind, welche die oben stehenden Regeln A1-A4,M1-M4 und D erfüllen, heißt Körper. Diese Regeln heißen Körperaxiome.*

Beispiele:

- oben gesehen: $\mathbb{Q}$ ist ein Körper.
- analog: die reellen Zahlen $\mathbb{R}$ sind ein Körper.
- Es gibt Körper mit endlich vielen Elementen, z. B. sei $K = \{0, 1\}$. Wir definieren die Operationen $+$ und $\cdot$ durch Tabellen:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Achtung: Hier gilt $1 + 1 = 0$!

Übungsaufgabe:

i) Überprüfe die Regeln A1-A4,M1-M4,D.

ii) Finde ähnliche Tabellen, welche die Mengen $K = \{0, 1, 2\}$ und $K = \{0, 1, 2, 3\}$ zu Körpern machen.

Endliche Körper mit k Elementen heißen $\mathbb{F}_k$. Da jeder Körper Elemente $1 \neq 0$ enthält, ist $\mathbb{F}_2$ der kleinstmögliche Körper. Man kann beweisen, dass nur für $k = p^r$ mit p Primzahl und $r \in \mathbb{N}$ ein Körper $\mathbb{F}_k$ existiert (also gibt es z. B. nicht $\mathbb{F}_6$). Aus den Körperaxiomen kann man viele weitere Regeln ableiten, z. B. :

1.) Angenommen, für $x, y, y' \in K$ gelte $x + y = 0$ und $x + y' = 0$. Dann folgt aus A1,A2 und A3, dass

$$y' = y' + 0 = y' + (x + y) = (y' + x) + y = (x + y') + y = 0 + y = y$$

ist. Also ist für gegebenes x das Element y, so dass $x + y = 0$ gilt (also das Negative von x) eindeutig bestimmt und wird $-x$ geschrieben.

2.) Analog sieht man, dass das Inverse von x $(\neq 0)$ aus M4 eindeutig bestimmt ist. Es wird $\frac{1}{x}$ oder x^{-1} geschrieben.

3.) Falls gilt $b = x + a$, dann ist

$$b + (-a) = x + a + (-a) \overset{A1}{=} x + (a + (-a)) \overset{A4}{=} x + 0 \overset{A3}{=} x,$$

also gilt $x = b + (-a)$, wofür wir kürzer $x = b - a$ schreiben.

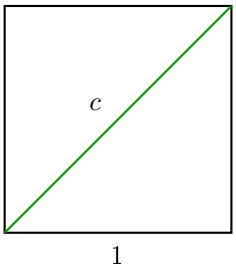
4.) Analog: $a \cdot x = b \xrightarrow{\text{M1,M3,M4}} x = \frac{b}{a} := b \cdot \frac{1}{a}$

5.) Aus A3) folgt $0 + 0 = 0$, daraus folgt

$$0 \cdot x = (0 + 0) \cdot x \overset{D)}{=} 0 \cdot x + 0 \cdot x$$
$$\text{also: } 0 \cdot x = (0 \cdot x) - (0 \cdot x) = 0.$$

Achtung: Diese Regeln sind für das Rechnen z. B. in $\mathbb{Q}$ ganz selbstverständlich und bedürfen keiner weiteren Erklärung. Aber der Punkt ist, dass man sie ohne weitere Annahmen aus den Körperaxiomen ableiten kann und sie daher für alle Körper gelten, z. B. für die Körper $\mathbb{F}_2, \mathbb{F}_3, \ldots$

Aus der Geometrie kann man ganz leicht sehen, dass es noch andere als rationale Zahlen geben muss. Betrachte den Satz von Pythagoras:



$$c = \sqrt{1^2 + 1^2} = \sqrt{2}$$

Frage: Kann man $\sqrt{2}$ als Bruch schreiben?
Antwort: Nein!

Satz 3.2. *$\sqrt{2} \notin \mathbb{Q}$, d. h., es gibt kein $x \in \mathbb{Q}$ mit $x^2 = 2$.*

Beweis. Wir führen einen sogenannten indirekten oder Widerspruchsbeweis durch. Wir nehmen an, das Gegenteil der Behauptung, welche wir beweisen wollen, würde gelten. Dann ziehen wir daraus Schlüsse, bis wir auf eine offensichtlich falsche Behauptung, Widerspruch genannt, kommen. Da diese Konsequenz also unmöglich ist, muss die ursprüngliche Behauptung wahr sein.

Zum Beweis des Satzes nehmen wir also an: $\exists x \in \mathbb{Q} : x^2 = 2$. Solch ein x kann man immer als Bruch schreiben, es gibt also Zahlen $a \in \mathbb{Z}, b \in \mathbb{N} : x = \frac{a}{b}$ und zwar so, dass a und b nicht beide gerade Zahlen sind. Falls nämlich a und b gerade sind, kann man durch Kürzen erreichen, dass eine von beiden nicht mehr von 2 geteilt wird. Es gilt also: $x = \frac{a}{b}, x^2 = 2 \Rightarrow \left(\frac{a}{b}\right)^2 = \frac{a^2}{b^2} = 2$, also: $2b^2 = a^2$.

Allgemein gilt nun: Ist n eine gerade Zahl ($n = 2m$), so ist auch $n^2 = 4m^2$ gerade. Ist n ungerade ($n = 2m+1$), so ist auch $n^2 = 4m^2 + 4m + 1$ ungerade. Aus letzter Aussage folgt: n^2 gerade $\Rightarrow n$ gerade. Also haben wir: n gerade $\Leftrightarrow n^2$ gerade.

Kommen wir zur Gleichung $a^2 = 2b^2$ zurück: Es ist a^2 gerade, also auch a, d. h., $\exists k \in \mathbb{Z} : a = 2k$. Dann folgt: $2b^2 = (2k)^2$, also $2b^2 = 4k^2$, und daraus folgt $b^2 = 2k^2$. Also ist auch b gerade. Dies ist der Widerspruch, denn wir hatten vorausgesetzt, dass nicht a und b gleichzeitig gerade sein sollen. Also kann es kein $x \in \mathbb{Q}$ mit $x^2 = 2$ geben, d. h., $\sqrt{2} \notin \mathbb{Q}$. □

Frage: Wie groß ist $\sqrt{2}$? Taschenrechner: $\sqrt{2}$ „=“1,4142136 $= \frac{14142136}{10000000} \in \mathbb{Q}$
Näherungsverfahren: Finde eine Folge von rationalen Zahlen, welche $\sqrt{2}$ annähern.

z. B. : Ist $\frac{a}{b}$ eine Näherung für $\sqrt{2}$, so ist $\frac{a+2b}{a+b}$ eine bessere Näherung (Theon von Smyrna ca. 100 n.u.Z.). Probieren mit Startwert $a = b = 1$:

$$\frac{1}{1}, \frac{3}{2}, \frac{7}{5}, \frac{17}{12}, \frac{41}{29} = 1,413793\ldots, \frac{99}{70} = 1,414285\ldots$$

Man stellt fest, dass die Werte dieser Folge abwechselnd größer oder kleiner als $\sqrt{2}$ sind.

In der Analysis werden die reellen Zahlen genau auf diese Art und Weise durch Hinzunehmen aller „Grenzwerte“ solcher „konvergenter“ Folgen von Brüchen konstruiert. In $\mathbb{R}$ hat man viele wichtige nicht-rationale Zahlen, wie π, e oder eben $\sqrt{c}$ mit $c \in \mathbb{N}$ zur Verfügung (aber z. B. nicht $\sqrt{-1}$, später). Wollen wir mit $\sqrt{2}$ rechnen, brauchen wir gar nicht alle reellen Zahlen. Wir kommen mit viel weniger aus.

Definition 3.3. *Wir definieren die Menge* $\mathbb{Q}(\sqrt{2})$ *als Teilmenge von* $\mathbb{R}$ *durch:*

$$\mathbb{Q}(\sqrt{2}) := \{a + b \cdot \sqrt{2} | a, b \in \mathbb{Q}\} \subset \mathbb{R}$$

Also ist z. B. $\frac{1}{4} + \frac{2}{7} \cdot \sqrt{2}$ ein Element von $\mathbb{Q}(\sqrt{2})$. Die folgenden Formeln zeigen, dass Summe und Produkt von zwei Zahlen aus $\mathbb{Q}(\sqrt{2})$ wieder in $\mathbb{Q}(\sqrt{2})$ sind.

$$\begin{aligned}(a + b\sqrt{2}) + (c + d\sqrt{2}) &= (a + c) + (b + d)\sqrt{2}\\ (a + b\sqrt{2}) \cdot (c + d\sqrt{2}) &= (ac + 2bd) + (ad + bc)\sqrt{2}\end{aligned}$$

Es gilt aber noch mehr: Für alle $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ existiert ein Inverses, falls nicht $a = b = 0$ ist, d. h.

$$\forall a + b \in \mathbb{Q}(\sqrt{2}) \setminus \{0\} : \exists c, d \in \mathbb{Q} : (a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = 1,$$

nämlich: $c := \frac{a}{a^2-2b^2}$ und $\frac{-b}{a^2-2b^2}$. Dies müssen wir beweisen:
Zunächst gilt: $a^2 - 2b^2 = 0 \Rightarrow a = b = 0$ (sonst wäre $\sqrt{2} \in \mathbb{Q}$, siehe Satz 3.2). Also sind für $a \neq 0$ oder $b \neq 0$ die Zahlen $c, d \in \mathbb{Q}$. Außerdem:

$$\begin{aligned}&(a + b\sqrt{2}) \cdot \left(\frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}\right)\\ =&\underbrace{(a + b\sqrt{2}) \cdot (a - b\sqrt{2})}_{a^2-2b^2} \cdot \frac{1}{a^2 - 2b^2} = 1.\end{aligned}$$

Also ist $\mathbb{Q}(\sqrt{2})$ abgeschlossen unter $+$ und $\cdot$, jedes Element $a + b\sqrt{2}$ besitzt ein Negatives, nämlich $-a - b\sqrt{2}$ und jedes Element außer 0 besitzt ein Inverses. Außerdem ist $\mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$, also gelten alle Axiome A1-A4, M1-M4, D. Wir erhalten also:

Satz 3.4. $\mathbb{Q}(\sqrt{2})$ *ist ein Körper.*

Wichtig an der obigen Konstruktion ist, dass wir mit Elementen aus $\mathbb{Q}(\sqrt{2})$ rechnen können, ohne die Dezimalbruchentwicklung von $\sqrt{2}$ zu kennen.

Kapitel 4

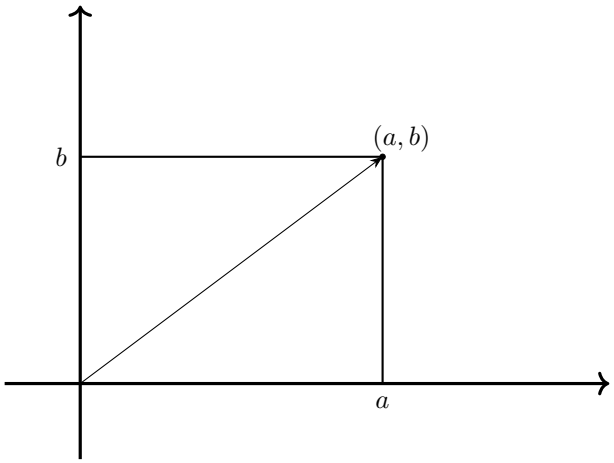
Der Körper der komplexen Zahlen

Wie wir schon gesehen haben, gibt es auch in $\mathbb{R}$ Gleichungen, welche keine reellen Lösungen haben, nämlich z. B. $x^2+1=0$. Wir hatten die Konstruktion von $\mathbb{R}$ (oder vorher auch von $\mathbb{Q}(\sqrt{2})$) damit motiviert, dass wir einen Körper konstruieren wollten, welcher $\mathbb{Q}$ und eine Nullstelle von $x^2-2=0$ enthält. Dies imitieren wir nun: Wir konstruieren den Körper $\mathbb{C}$ so, dass er eine Zahl i mit $i^2=-1$ enthält (dann muss auch $(-i)^2=-1$ gelten. Wir benutzen dabei die folgende geometrische Konstruktion, welche auf Hamilton zurückgeht.

Definition 4.1. *Sei $\mathbb{C}=\mathbb{R}\times\mathbb{R}(=\mathbb{R}^2)$, d. h., Elemente von $\mathbb{C}$ sind Paare (a,b) von rellen Zahlen. Setze*

$$\begin{array}{rcll} 0 & \coloneqq & (0,0) & \text{(die komplexe 0)} \\ 1 & \coloneqq & (1,0) & \text{(die komplexe 1)} \\ i & \coloneqq & (0,1) & \text{(die imaginäre Einheit)} \end{array}$$

Wir nennen ein Element $(a,b)\in\mathbb{C}$ eine komplexe Zahl und $\mathbb{C}$ die komplexe oder Gaußsche Zahlenebene. Wir können also $(a,b)\in\mathbb{C}$ durch einen Punkt in der Ebene darstellen.



Wir definieren nun zwei Operationen $+$ und $\cdot$ auf $\mathbb{C}$ durch die folgenden Formeln

$$\begin{aligned} (a,b)+(c,d) &\coloneqq (a+c,b+d) \\ (a,b)\cdot(c,d) &\coloneqq (ac-bd,ad+bc) \end{aligned} \tag{$*$}$$

Damit können wir den folgenden Satz formulieren.

Satz 4.2. $\mathbb{C}$ *ist ein Körper.*

Beweis. Wir müssen alle Axiome A1-A4, M1-M4 sowie D überprüfen. Das ist fast alles Fleißarbeit, z. B. M2 (Kommutativität der Multiplikation):

$$(a,b)\cdot(c,d) = (ac-bd, ad+bc) = (ca-db, cb+da) = (c,d)\cdot(a,b)$$

$$\uparrow$$

Axiome M2 und A2 für den Körper $\mathbb{R}$

Interessant ist nur das Axiom M4: Wie finden wir ein inverses Element für $(a,b) \in \mathbb{C}\setminus\{0\}$ (d. h., a und b sind nicht gleichzeitig gleich Null)? Um dies zu beantworten, führen wir erst eine vereinfachte Schreibweise für komplexe Zahlen ein . Eine reelle Zahl a können wir mit der komplexen Zahl $(a,0)$ identifizieren, und da $(b,0)\cdot\underbrace{(0,1)}_{i} = (0,b)$ und $(a,b) = (a,0)+(0,b)$ gilt, können wir (a,b) auch als

$$(a,b) = a+bi$$

schreiben. Dann lassen sich die Rechenregeln (∗) viel natürlicher schreiben als:

$$\begin{aligned}(a+bi)+(c+di) &= (a+c)+i(b+d)\\ (a+bi)\cdot(c+di) &= (ac+i^2\cdot bd)+i(ad+bc)\end{aligned}$$

Jetzt ist aber $i^2 = (0,1)\cdot(0,1) = (-1,0) = -1$, also

$$(a+bi)\cdot(c+di) = (ac-bd)+i(ad+bc),$$

und wir sehen, dass i tatsächlich eine Quadratwurzel aus -1 ist. Nun zum Axiom M4: Wir haben $(a+bi)\cdot(a-bi) = a^2+b^2$, und falls a und b nicht beide gleich Null sind, dann ist $a^2+b^2 \neq 0$. Dann gilt:

$$(a+bi)\cdot\left(\frac{a}{a^2+b^2} - i\cdot\frac{b}{a^2+b^2}\right) = \frac{(a+bi)\cdot(a-bi)}{a^2+b^2} = 1$$

Die Zahl $\frac{a}{a^2+b^2} - i\frac{b}{a^2+b^2} = \left(\frac{a}{a^2+b^2}, -\frac{b}{a^2+b^2}\right)$ ist also das Inverse der komplexen Zahl $a+ib \in \mathbb{C}\setminus\{0\}$.

□

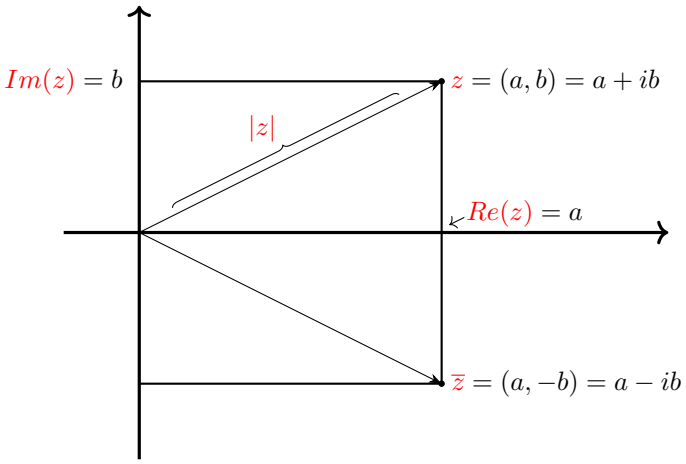
Übung: Prüfen Sie die verbleibenden Körperaxiome nach!

Beispiele für das Rechnen in $\mathbb{C}$:

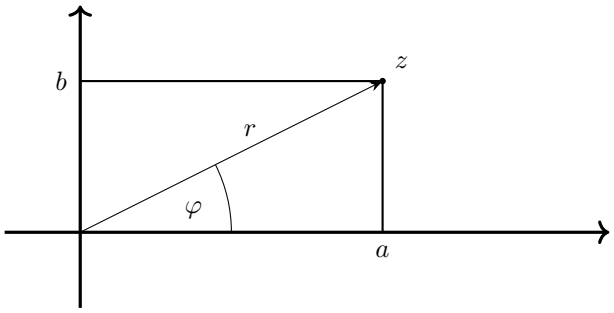
- $\frac{1}{3+4i} = \frac{3-4i}{(3-4i)(3+4i)} = \frac{3-4i}{3^2+4^2} = \frac{3}{25} - i\frac{4}{25}$.
- Es gilt: $(1+i)(1+i) = 1+2i-1 = 2i$, also $i = \frac{1}{2}(1+i)^2 = \left(\frac{1+i}{\sqrt{2}}\right)^2$. Somit ist also $\frac{1}{2}(1+i)$ eine Quadratwurzel von i.
- Sei $c \coloneqq \frac{1}{2}\left(-1+i\cdot\sqrt{3}\right)$. Dann gilt:
  $c^3 = c\cdot c^2 = \frac{1}{8}\left(-1+i\cdot\sqrt{3}\right)\cdot\left(1-2i\cdot\sqrt{3}-3\right) = \frac{1}{8}\left(-1+i\cdot\sqrt{3}\right)(-2)\left(1+i\cdot\sqrt{3}\right) = -\frac{1}{4}(-3-1) = 1$,
  also ist c eine dritte Wurzel von 1.
- Übung: Prüfen Sie, dass für $c = \frac{1}{2}\left(-1+i\cdot\sqrt{3}\right)$ auch $c^2+c+1 = 0$ gilt!

Wir führen nun einige weitere wichtige Begriffe rund um komplexe Zahlen ein.

Definition 4.3. *Für eine komplexe Zahl $z = a + ib \in \mathbb{C}$ heißt a der* Realteil *(geschrieben $Re(z)$) und b der* Imaginärteil *(geschrieben $Im(z)$). Außerdem heißt $\overline{z} := a - ib \in \mathbb{C}$ die zu z* konjugierte *komplexe Zahl. Dann ist $z \cdot \overline{z} = (a+ib)(a-ib) = a^2 + b^2 \in \mathbb{R}$ und man definiert den* Betrag *von z als $|z| := \sqrt{z\overline{z}} = \sqrt{a^2+b^2}$. Man kann dies wieder graphisch veranschaulichen:*



Wir möchten die Operationen $+$ und $\cdot$ auch geometrisch in der komplexen Zahlenebene verstehen. Hierzu benötigen wir eine neue Darstellung komplexer Zahlen, die sogenannte Polardarstellung:
Sei $z = a + ib \in \mathbb{C}$ gegeben, mit $r := |z| = \sqrt{a^2 + b^2}$. Dann ist (wie aus dem Bild ersichtlich): $a = r \cdot \cos(\varphi)$ und $b = r \cdot \sin(\varphi)$, sodass $z = r(\cos(\varphi) + i\sin(\varphi))$ gilt.



Definition 4.4. *(r, φ) heißen* Polarkoordinaten *der komplexen Zahl z, dabei heißt $r = |z|$ der Betrag und $\varphi =: \arg(z)$ das Argument von z. Wir wählen φ immer im Intervall $[0, 2\pi)$.*

Damit können wir die Multiplikation sehr viel einfacher verstehen: Seien $z := r(\cos(\varphi) + i\sin(\varphi))$ und $w := s(\cos(\psi) + i\sin(\psi))$ gegeben (also $r, s \in \mathbb{R}_+; \varphi, \psi \in [0, 2\pi)$), dann ist

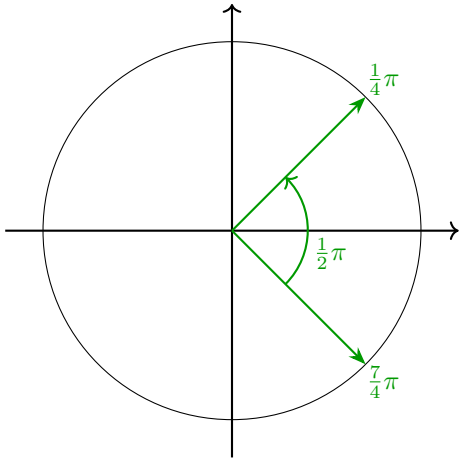
$$\begin{aligned} z \cdot w &= rs(\cos(\varphi) + i\sin(\varphi))(\cos(\psi) + i\sin(\psi)) \\ &= rs(\cos(\varphi)\cos(\psi) - \sin(\varphi)\sin(\psi) + i(\cos(\varphi)\sin(\psi) + \sin(\varphi)\cos(\psi))) \\ &\overset{(*)}{=} rs(\cos(\varphi + \psi) + i\sin(\varphi + \psi)). \end{aligned}$$

Additionstheoreme: $\cos(\varphi + \psi) = \cos(\varphi)\cos(\psi) - \sin(\varphi)\sin(\psi)$
$\sin(\varphi + \psi) = \cos(\varphi)\sin(\psi) + \sin(\varphi)\cos(\psi)$.

Damit haben wir folgenden Satz bewiesen:

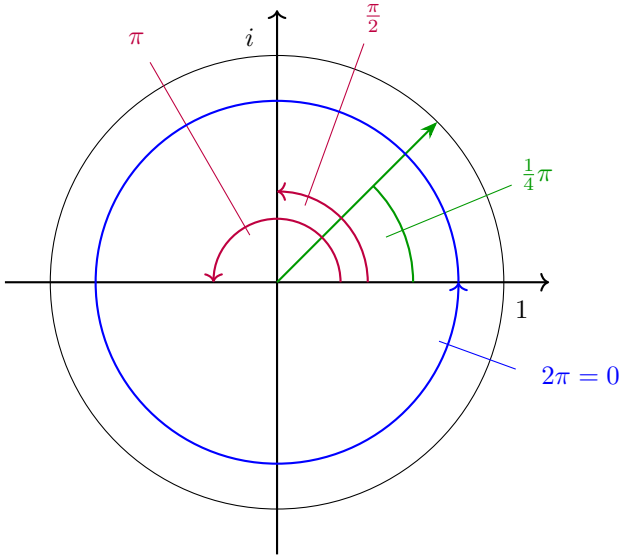
Satz 4.5. *Bei der Multiplikation komplexer Zahlen werden die Beträge multipliziert und die Argumente addiert, letzteres bis auf Vielfache von* 2π.

Zum Beispiel würde man als Summe von $\frac{7}{4}\pi$ und $\frac{1}{2}\pi$ die Zahl $\frac{1}{4}\pi$ ansehen, denn
$\frac{7}{4}\pi + \frac{1}{2}\pi = \frac{7+2}{4}\pi = \frac{9}{4}\pi = \frac{1}{4}\pi + 2\pi$.

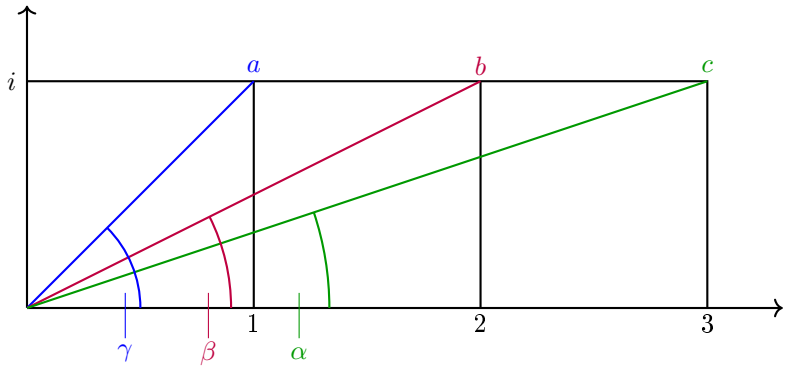


Beispiele:

- Wir wissen natürlich, dass $(-1)\cdot(-1) = 1$ ist. Wie sieht das aus, falls man $-1 = -1 + i\cdot 0$ als komplexe Zahl auffasst:
  $\arg(-1) = \pi$, also ist $\arg((-1)\cdot(-1)) = \arg(-1) + \arg(-1) = \pi + \pi = 2\pi = 0 + 2\pi$, und $\arg(1) = 0$.
- Klar: $\arg(i) = \frac{\pi}{2} \Rightarrow \arg(i^2) = 2 \cdot \frac{\pi}{2} = \pi$, und wegen $|i|^2 = 1^2 = 1$ folgt erneut $i^2 = -1$.
- Wir hatten oben gesehen, dass $z := \frac{1}{\sqrt{2}}(1+i)$ eine Quadratwurzel von i ist. Es gilt $\arg(\frac{1}{\sqrt{2}}(1+i)) = \frac{\pi}{4}$, also ist $\arg((\frac{1}{\sqrt{2}}(1+i))^2) = 2 \cdot \frac{\pi}{4} = \frac{\pi}{2}$.
- Geometrische Darstellung dieser Beispiele:



- Anwendungsbeispiel der Polardarstellung:



Was ist die Summe der Winkel α, β und γ? Dies ist a priori schwer, aber ganz leicht bei Benutzung der Multiplikation komplexer Zahlen:

$$a = 1 + i,\ b = 2 + i,\ c = 3 + i$$

$$\begin{aligned} a \cdot b \cdot c &= (1+i)(2+i)(3+i) \\ &= (2 - 1 + 3i)(3+i) \\ &= (1+3i)(3+i) \\ &= (3 - 3 + 10i) = 10i \end{aligned}$$

Also $\alpha + \beta + \gamma = \arg(a \cdot b \cdot c) = \frac{\pi}{2}$.

- Berechnung des Inversen: Falls $z = a + bi = |z| \cdot (\cos\varphi + i \sin\varphi)$ ist, dann muss für $w := z^{-1} = |w| \cdot (\cos\psi + i\sin\psi)$ gelten

$$|1| = 1 = |z \cdot w| = |z| \cdot |w| \Rightarrow |w| = \frac{1}{|z|}, \text{ sowie}$$

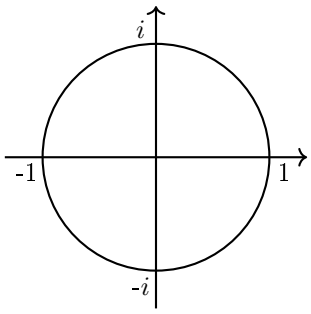
$$\arg(1) = 0 = \arg(z \cdot w) = \varphi + \psi \Rightarrow \psi = -\varphi$$

Also erhalten wir:

$$\begin{aligned} z^{-1} &= \frac{1}{|z|}(\cos(-\varphi) + i\sin(-\varphi)) \\ &= \frac{1}{|z|}(\cos\varphi - i\sin\varphi) \\ &= \frac{a}{a^2+b^2} - i\frac{b}{a^2+b^2} = \frac{1}{\sqrt{a^2+b^2}}\left(\frac{a}{\sqrt{a^2+b^2}} - i\frac{b}{\sqrt{a^2+b^2}}\right), \end{aligned}$$

da $\cos\varphi = \frac{a}{|z|}$, $\sin\varphi = \frac{b}{|z|}$.

Von besonderer Bedeutung sind komplexe Zahlen mit Betrag 1. Klar ist, dass aus $|z| = 1$ folgt, dass $z = \cos\varphi + i\sin\varphi$ für ein $\varphi \in [0, 2\pi)$ ist. Dies sind genau die Zahlen auf dem Einheitskreis $S^1 := \{z \in \mathbb{C} : |z| = 1\}$



Man sieht leicht, dass die folgenden Aussagen gelten:

1.) $1 \in S^1$

2.) $z, w \in S^1 \Rightarrow z \cdot w \in S^1$ (klar, weil $|z \cdot w| = |z| \cdot |w|$)

3.) $z \in S^1 \Rightarrow z^{-1} \in S^1$ (klar, weil $|z^{-1}| = |z| = 1$)

Man kann dies formalisieren zu der Aussage, dass S^1 zusammen mit „$\cdot$“ eine Gruppe ist, später mehr davon. Gleich benötigen wir die sogenannten de Moivreschen Formeln

Lemma 4.6. *$\forall \varphi \in [0, 2\pi), \forall n \in \mathbb{N}$ gilt:*

$$(\cos\varphi + i\sin\varphi)^n = \cos(n\varphi) + i\sin(n\varphi)$$

Beweis. Klar ist $|\cos\varphi + i\sin\varphi| = 1$ und $\arg(\cos\varphi + i\sin\varphi) = \varphi$. Also ist nach der obigen Regel zur Multiplikation komplexer Zahlen (beachte: $(\cos\varphi + i\sin\varphi)^n = \underbrace{(\cos\varphi + i\sin\varphi) \cdot \ldots \cdot (\cos\varphi + i\sin\varphi)}_{\text{n-mal}}$)
$|(\cos\varphi + i\sin\varphi)^n| = 1$ und $\arg((\cos\varphi + i\sin\varphi)^n) = n\varphi$, also $(\cos\varphi + i\sin\varphi)^n = \cos(n\varphi) + i\sin(n\varphi)$

□

Als Anwendung erhalten wir Formeln für $\cos(n\varphi)$ und $\sin(n\varphi)$. Beispielsweise finden wir für $n = 3$:

$$\begin{aligned}
& \cos(3\varphi) + i\sin(3\varphi) \\
\overset{\text{Lemma 4.6}}{=} \quad & (\cos\varphi + i\sin\varphi)^3 \\
\overset{\text{Binomische Formel}}{=} \quad & \cos^3\varphi + 3i\cos^2\varphi\sin\varphi + 3i^2\cos\varphi\sin^2\varphi + i^3\sin^3\varphi \\
= \quad & (\cos^3\varphi - 3\cos\varphi\sin^2\varphi) + i(3\cos^2\varphi\sin\varphi - \sin^3\varphi)
\end{aligned}$$

Auf beiden Seiten dieser Gleichung stehen komplexe Zahlen, deren Real- und Imaginärteil sind also gleich. Daher gilt:

$$\begin{aligned}
\cos(3\varphi) &= \cos^3\varphi - 3\cos\varphi\sin^2\varphi \\
\sin(3\varphi) &= 3\cos^2\varphi\sin\varphi - \sin^3\varphi
\end{aligned}$$

Definition 4.7. *Eine komplexe Zahl $z \in \mathbb{C}$ heißt n-te Einheitswurzel, falls gilt $z^n - 1 = 0$. Man schreibt auch $\mu_n \coloneqq \{z \in \mathbb{C} : z^n - 1 = 0\}$ für die Menge der n-ten Einheitswurzeln.*

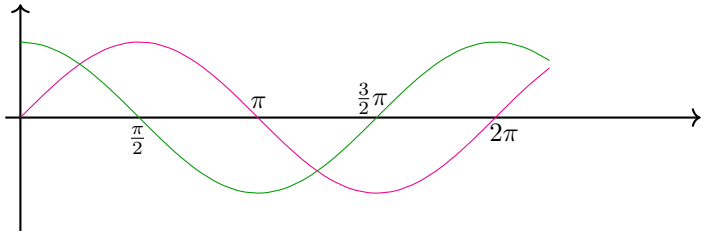
Es gilt: $\mu_n \subset S^1$, denn für alle $z \in \mu_n$ gilt $z^n = 1$, also auch $|z^n| = |1| = 1$. Aber wieder nach der Regel für das Multiplizieren von komplexen Zahlen ist $|z^n| = |z|^n$, also $|z|^n = 1$, also wegen $|z| \in \mathbb{R}_+$ folgt $|z| = 1$, d. h. $z \in S^1$.
Wir können nun sofort folgende Aussage zeigen:

Proposition 4.8. *Es gilt $|\mu_n| = n$, d. h., es gibt genau n Stück n-te Einheitswurzeln, nämlich die Zahlen $1, \zeta, \zeta^2, \zeta^3, \ldots, \zeta^{n-1}$, wobei $\zeta := \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right)$ ist.*

Beweis. Die Zahl $z = \cos\varphi + i\sin\varphi$ ist genau dann eine n-te Einheitswurzel, wenn gilt:

$$1 = z^n = (\cos\varphi + i\sin\varphi)^n = \cos(n\varphi) + i\sin(n\varphi)$$

Es muss also gelten: $\cos(n\varphi) = 1$ und $\sin(n\varphi) = 0$
Erinnerung: Graphen von cos und sin:



Also folgt: $n\varphi = 0 + 2k\pi$ für ein $k \in \mathbb{Z}$. Da wir das Argument von komplexen Zahlen immer im Intervall $[0, 2\pi)$ wählen, gilt also $\varphi = \frac{k}{n} \cdot 2\pi$ für $k \in \{0, 1, \ldots, n-1\}$. Daher sind die Zahlen

$$\cos\left(\frac{2k\pi}{n}\right) + i\sin\left(\frac{2k\pi}{n}\right), \qquad k = 0, 1, \ldots, n-1$$

die n-ten Einheitswurzeln und es gibt keine anderen. Nach der Formel von de Moivre gilt:

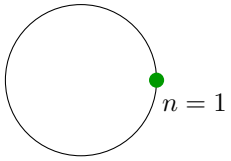
$$\cos\left(\frac{2k\pi}{n}\right) + i\sin\left(\frac{2k\pi}{n}\right) = \left(\cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)\right)^k = \zeta^k,$$

also ist $\mu_n = \{1 = \zeta^0, \zeta, \zeta^2, \ldots, \zeta^{n-1}\}$.

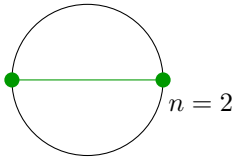
□

Beispiele:

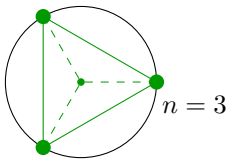
- Es gibt nur eine erste Einheitswurzel, nämlich 1 ($z^1 = 1 \Leftrightarrow z = 1$)



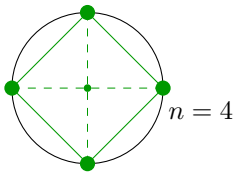
- 1 und -1 sind die zweiten Einheitswurzeln



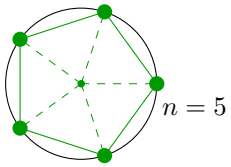
- Die 3 dritten Einheitswurzeln sind 1, $\cos\left(\frac{2}{3}\pi\right) + i\sin\left(\frac{2}{3}\pi\right) = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$, sowie $\cos\left(\frac{4}{3}\pi\right) + i\sin\left(\frac{4}{3}\pi\right) = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$

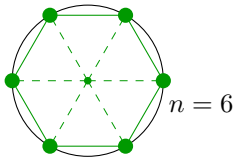


- Die 4 vierten Einheitswurzeln sind 1, i, -1, $-i$



- Hier noch die entsprechenden Bilder für $n = 5, 6$:





An den Bildern erkennt man:

1.) Die n-ten Einheitswurzeln bilden die Ecken eines regelmäßigen n-Ecks, welches in den Einheitskreis S^1 einbeschrieben ist.

2.) Eine n-te Einheitswurzel ist auch eine $2n$-te, $3n$-te etc., anders ausgedrückt: $\mu_n \subset \mu_{k\cdot n}$ für alle $k \in \mathbb{N}$.

Natürlich kann man diese zwei Beobachtungen auch sofort durch Nachrechnen mit Hilfe von Proposition 4.8 verifizieren.
Wir wollen jetzt die komplexen Zahlen benutzen, um Lösungsformeln für gewisse polynomiale Gleichungen anzugeben. Wir beginnen mit einem besonders einfachen Fall.

Satz 4.9. *Sei w eine komplexe Zahl ungleich 0, dann gibt es genau n verschiedene Lösungen der Gleichung $z^n = w$, diese sind Eckpunkte eines regulären n-Ecks.*

Beweis. Wir schreiben in Polarkoordinaten $w = r(\cos\varphi + i\sin\varphi)$. Eine mögliche Lösung von $z^n = w$ ist die Zahl $z_0 = \sqrt[n]{r}(\cos\frac{\varphi}{n} + i\sin\frac{\varphi}{n})$, denn $z_0^n = r(\cos(n\frac{\varphi}{n}) + i\sin(n\frac{\varphi}{n})) = w$. Falls für eine Zahl $z_1 \in \mathbb{C}$ auch die Gleichung $z_1^n = w$ erfüllt ist, dann gilt $\frac{z_1^n}{z_0^n} = \frac{w}{w} = 1$, also $\left(\frac{z_1}{z_0}\right)^n = 1$. Also ist $\frac{z_1}{z_0}$ eine n-te Einheitswurzel, also sind alle Lösungen gegeben durch $\{\zeta^k \cdot z_0 : \zeta = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right), k = 0, 1, \ldots, n-1\}$. Diese Punkte liegen auf einem regelmäßigen n-Eck, welches dem Kreis mit Radius $\sqrt[n]{r} = |z_0|$ einbeschrieben ist.

□

Ein praktischer Algorithmus, um die Gleichung $z^n = w$ zu lösen ist also:

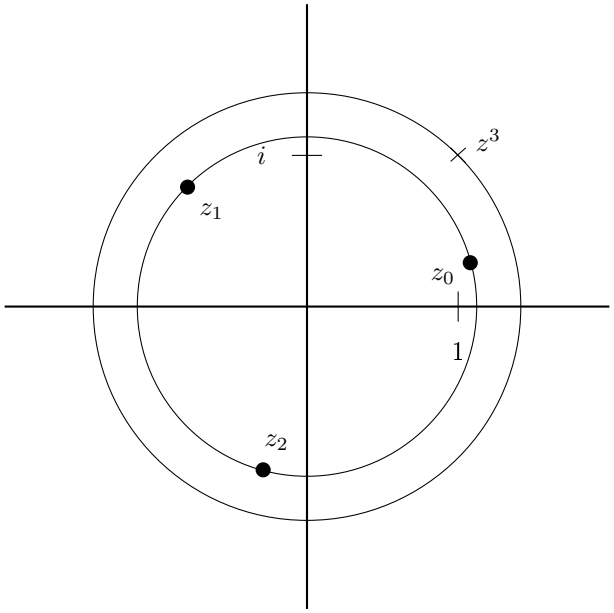
1. Gegeben $w = a + ib \in \mathbb{C}$
2. Bestimme $r := |w| = \sqrt{a^2 + b^2}$ und $\varphi := \arg(w) = \arccos\left(\frac{a}{r}\right)$

3. Bestimme $\sqrt[n]{r}$, $\frac{\varphi}{n}$ und $\cos\left(\frac{\varphi}{n}\right), \sin\left(\frac{\varphi}{n}\right)$, dann ist die Zahl $z_0 = \sqrt[n]{r} \cdot \left(\cos\left(\frac{\varphi}{n}\right) + i \sin\left(\frac{\varphi}{n}\right)\right.$ eine Lösung.

4. Berechne die n-ten Einheitswurzeln $1 = \zeta^0, \zeta^1, \zeta^2, \ldots, \zeta^{n-1}$. Dann sind alle Lösungen gegeben durch $z_0, \zeta \cdot z_0, \zeta^2 \cdot z_0, \ldots, \zeta^{n-1} \cdot z_0$.

Beispiel (Lösung mit Taschenrechner): $z^3 = 1 + i = 1 + i \cdot 1$
$\Rightarrow r = \sqrt{1^2 + 1^2} = \sqrt{2} = 1,4142\ldots, \qquad \varphi = \arccos\left(\frac{1}{\sqrt{2}}\right) = 0,7856\ldots,$
$\sqrt[3]{r} = 1,1225\ldots, \qquad \frac{\varphi}{3} = 0,2595\ldots, \qquad \cos\left(\frac{\varphi}{3}\right) = 0,9569\ldots, \qquad \sin\left(\frac{\varphi}{3}\right) = 0,2565\ldots,$ also
$z_0 = 1,1225\ldots \cdot (0,9569\ldots + i \cdot 0,2565\ldots) = 1,08\ldots + i \cdot 0,29\ldots,$
$\zeta = \cos\left(\frac{2\pi}{3}\right) + i \sin\left(\frac{2\pi}{3}\right) = -\frac{1}{2} + i\frac{\sqrt{3}}{2} = -0,5 + i \cdot 0,8660\ldots,$
$\zeta^2 = \cos\left(\frac{4\pi}{3}\right) - i \sin\left(\frac{4\pi}{3}\right) = -\frac{1}{2} - i\frac{\sqrt{3}}{2} = -0,5 - i \cdot 0,8660\ldots$

Also ist $z_1 = \zeta \cdot z_0 = -0,79\ldots + i \cdot 0,79\ldots, \quad z_2 = \zeta^2 \cdot z_0 = \zeta \cdot z_1 = -0,29\ldots\ldots - i \cdot 1,08\ldots$



Wir kommen nun zu quadratischen und kubischen Gleichungen. Erstere kennen Sie bereits aus der Schule.

Satz 4.10. *Die Gleichung $x^2 + px + q = 0$ hat die zwei Lösungen*

$$x_{1,2} = \frac{-p \pm \sqrt{p^2 - 4q}}{2} \quad \forall p, q \in \mathbb{C}$$

Die Zahl $D := \frac{p^2}{4} - q$ heißt Diskriminante der Gleichung $x^2 + px + q = 0$. Falls $p, q \in \mathbb{R}$, hat die Gleichung

$$\begin{aligned} \text{2 reelle Lösungen (d. h. } x_1, x_2 \in \mathbb{R}) &\Leftrightarrow D > 0 \\ \text{1 reelle Lösung } x = -\frac{p}{2} &\Leftrightarrow D = 0 \\ \text{2 konjugiert komplexe Lösungen (d. h. } x_1 = \overline{x_2} \in \mathbb{C} \setminus \mathbb{R}) &\Leftrightarrow D < 0 \end{aligned}$$

Beweis. Dieser Beweis ist wahrscheinlich wohlbekannt, aber er ist instruktiv, daher wiederholen wir ihn hier. Wir betrachten die sogenannte quadratische Ergänzung:

$$
\begin{aligned}
& x^2 + px + q = (x + \frac{1}{2}p)^2 - \frac{1}{4}p^2 + q = 0 \\
\Leftrightarrow \quad & (x + \frac{1}{2}p)^2 = \frac{1}{4}p^2 - q \\
\Leftrightarrow \quad & x_{1,2} + \frac{1}{2}p = \pm\sqrt{\underbrace{\frac{1}{4}p^2 - q}_{D}} \\
\Leftrightarrow \quad & x_{1,2} = \frac{1}{2}(-p \pm \sqrt{p^2 - 4q})
\end{aligned}
$$

Falls $p, q \in \mathbb{R}$:
$D = 0 \Leftrightarrow \exists!$ Lösung $x_1 = x_2 = -\frac{p}{2} \in \mathbb{R}$
$D > 0 \Leftrightarrow$ Es existieren zwei reelle Lösungen, da $\sqrt{D} \in \mathbb{R}$
$D < 0 \Leftrightarrow Re(x_1) = Re(x_2), Im(x_1) = -Im(x_2) \Rightarrow x_1 = \overline{x_2}$

□

In ähnlicher Art wollen wir jetzt eine Lösungsformel für Gleichungen dritten Grades herleiten. Diese wurde im 16. Jahrhundert von italienischen Mathematikern entdeckt: nämlich unabhängig voneinander durch Scipione del Ferro und Niccolo Fontana (genannt Tartaglia), welche die Lösung aber geheim hielten. Die Methode von Tartaglia wurde von Girolamo Cardano in seinem Buch „Ars Magna“ publiziert. Seitdem spricht man von der Cardanoschen Formel. Diese wollen wir jetzt herleiten. Wir betrachten also Gleichungen der Form

$$y^3 + ay^2 + by + c = 0 \qquad (*)$$

und wir starten wieder mit einer (diesmal kubischen) Ergänzung:
Sei $x := y + \frac{1}{3}a$, d. h., $y = x - \frac{1}{3}a$, dann finden wir durch Einsetzen in die Gleichung $(*)$, dass $(x - \frac{1}{3}a)^3 + a(x - \frac{1}{3}a)^2 + b(x - \frac{1}{3}a) + c = 0$ gelten muss. Dies formen wir um zu:

$$x^3 - 3x^2 \cdot \frac{1}{3}a + 3x \cdot \frac{1}{9}a^2 - \frac{1}{27}a^3 + ax^2 - 2a^2x\frac{1}{3} + \frac{1}{9}a^3 + bx - \frac{ab}{3} + c = 0$$

weiter umgeformt

$$x^3 + \frac{1}{3}a^2x - \frac{1}{27}a^3 - \frac{2}{3}a^2x + \frac{1}{9}a^3 + bx - \frac{ab}{3} + c = x^3 - (\underbrace{\frac{1}{3}a^2 - b}_{p})x - (\underbrace{\frac{ab}{3} - c + \frac{2}{27}a^3}_{q}) = 0$$

Damit haben wir die ursprüngliche Gleichung in eine Gleichung vom Typ $x^3 - px - q = 0$ transformiert. Allerdings können wir jetzt nicht wie im Fall von Gleichungen zweiten Grades daraus direkt die Lösung ableiten. Wir illustrieren dies an einem Beispiel:

Sei die Gleichung $y^3 + 3y^2 + 3y + 9 = 0$ gegeben. Dann setzen wir $x := y + 1$, also $y = x - 1$ und erhalten durch Einsetzen:

$$
\begin{aligned}
& (x-1)^3 + 3 \cdot (x-1)^2 + 3 \cdot (x-1) + 9 = 0 \\
\Leftrightarrow \quad & x^3 - 3x^2 + 3x - 1 + 3x^2 - 6x + 3 + 3x - 3 + 9 \\
\Leftrightarrow \quad & x^3 + 8 = 0 \\
\Leftrightarrow \quad & x^3 = -8
\end{aligned}
$$

Und damit sehen wir, dass -2 eine Lösung der ursprünglichen Gleichung ist (und nach Satz 4.9 sind die beiden Lösungen $-2\zeta, -2\zeta^2$, mit $\zeta = \cos\left(\frac{2\pi}{3}\right) + i\sin\left(\frac{2\pi}{3}\right)$).

Wenn wir dieses Beispiel allerdings ein wenig ändern und stattdessen die Gleichung

$$y^3 + 3y^2 + 9 = 0$$

betrachten (welche eigentlich einfacher aussieht), dann erhalten wir durch kubische Ergänzung

$$(x-1)^3 + 3(x-1)^2 + 9 = x^3 - 3x^2 + 3x - 1 + 3x^2 - 6x + 3 + 9 = x^3 - 3x + 11 = 0,$$

und diese Gleichung können wir nicht einfach auflösen.

Um also die Gleichung $x^3 = px+q$ aufzulösen, nehmen wir $p \neq 0$ an, denn sonst liefert Satz 4.9 alle Lösungen. Der erstaunliche Trick, mit dem man auf die Lösung kommt, ist, $x = u + v$ zu setzen. Damit erhalten wir

$$(u+v)^3 = u^3 + 3u^2v + 3uv^2 + v^3 = 3uv(u+v) + u^3 + v^3 = 3uv \cdot x + u^3 + v^3.$$

Weil aber $x^3 = px + q$ gilt, reicht es aus, das Gleichungssystem

$$\begin{aligned} 3uv &= p \\ u^3 + v^3 &= q \end{aligned}$$

zu lösen (d. h., bei gegebenen Zahlen p und q die Zahlen u und v zu bestimmen). Wir hatten $p \neq 0$ angenommen, daher ist $u \neq 0$ und $v \neq 0$, also erhalten wir aus der ersten Gleichung $v = \frac{p}{3u}$, was wir in die zweite Gleichung einsetzen. Dies gibt

$$u^3 + \left(\frac{p}{3u}\right)^3 = q.$$

Wir multiplizieren mit u^3, dann folgt:

$$(u^3)^2 - qu^3 + \frac{p^3}{27} = 0.$$

Wenn wir jetzt $r := u^3$ setzen, haben wir die folgende quadratische Gleichung in r:

$$r^2 - qr + \frac{p^3}{27} = 0, \text{ also ist}$$

$$r_{1,2} = \frac{q}{2} \pm \sqrt{\frac{q^2}{4} - \frac{p^3}{27}} = \frac{q \pm \sqrt{q^2 - \frac{4}{27}p^3}}{2}$$

Also gilt $u^3 = \frac{1}{2}(q \pm \sqrt{q^2 - \frac{4}{27}p^3})$. Wir wählen zunächst die Lösung $u^3 = \frac{1}{2}(q + \sqrt{q^2 - \frac{4}{27}p^3})$, dann haben wir folgenden Satz (Cardanosche Formel):

Satz 4.11. *Sei die Gleichung $x^3 - px - q = 0$ mit $p \neq 0$ gegeben. Dann ist $x = u + \frac{p}{3u}$ mit*

$$u = \sqrt[3]{\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3}}$$

eine Lösung. Die beiden anderen Lösungen sind gegeben durch $x = u + \frac{p}{3u}$ mit

$$u = \zeta \cdot \sqrt[3]{\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3}},$$

sowie $x = u + \frac{p}{3u}$ mit

$$u = \zeta^2 \cdot \sqrt[3]{\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3}}.$$

Hierbei ist wieder $\zeta = \cos(\frac{2\pi}{3}) + i\sin(\frac{2\pi}{3})$ eine dritte Einheitswurzel.

Beweis. Aus Satz 4.9 folgt, dass die Gleichung $u^3 = \frac{1}{2}(q + \sqrt{q^2 - \frac{4}{27}p^3})$ die drei Lösungen $u = \zeta^i \sqrt[3]{\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3}}$ mit $\zeta = \cos(\frac{2\pi}{3}) + i\sin(\frac{2\pi}{3})$ und $i = 0, 1, 2$ hat. Es bleibt noch zu begründen, warum wir nicht die Gleichung $u^3 = \frac{1}{2}(q - \sqrt{q^2 - \frac{4}{27}p^3})$ betrachtet haben. Wir hatten aus den Gleichungen

$$3uv = p$$
$$u^3 + v^3 = q$$

abgeleitet, dass u die Gleichung $(u^3)^2 - qu^3 + \frac{p^3}{27} = 0$ erfüllen muss, aber genauso erhält man, dass $(v^3)^2 - qv^3 + \frac{p^3}{27} = 0$ gilt. Also ist auch $v^3 = \frac{1}{2}(q \pm \sqrt{q^2 - \frac{4}{27}p^3})$ und daher ist $v^3 = \frac{1}{2}(q + \sqrt{q^2 - \frac{4}{27}p^3})$, falls wir $u^3 = \frac{1}{2}(q - \sqrt{q^2 - \frac{4}{27}p^3})$ wählen. Da aber $x = u + v$ ist, ändert sich an der Lösung für x der Gleichung $x^3 = px + q$ nichts, egal, ob wir $u^3 = \frac{1}{2}(q + \sqrt{q^2 - \frac{4}{27}p^3})$ oder $u^3 = \frac{1}{2}(q - \sqrt{q^2 - \frac{4}{27}p^3})$ wählen.

□

Wir diskutieren einige Beispiele zu den Cardanoschen Formeln:

1.) $x^3 = 9x + 28$. Wir haben $p = 9$ und $q = 28$. Wir erhalten für u:

$$u = \sqrt[3]{14 + \sqrt{14^2 - 3^3}} = \sqrt[3]{14 + \sqrt{196 - 27}}$$
$$= \sqrt[3]{14 + \sqrt{169}} = \sqrt[3]{27} = 3.$$

Damit erhalten wir als Lösung

$$x = u + \frac{p}{3u} = 3 + \frac{9}{9} = 4.$$

Die beiden anderen Lösungen bekommt man aus $\zeta u, \zeta^2 u$, mit $\zeta = \cos(\frac{2\pi}{3}) + i\sin(\frac{2\pi}{3})$. Sie sind nicht reell.

2.) $x^3 = -3x + 4 \quad \Rightarrow \quad p = -3, q = 4$. Hier ist

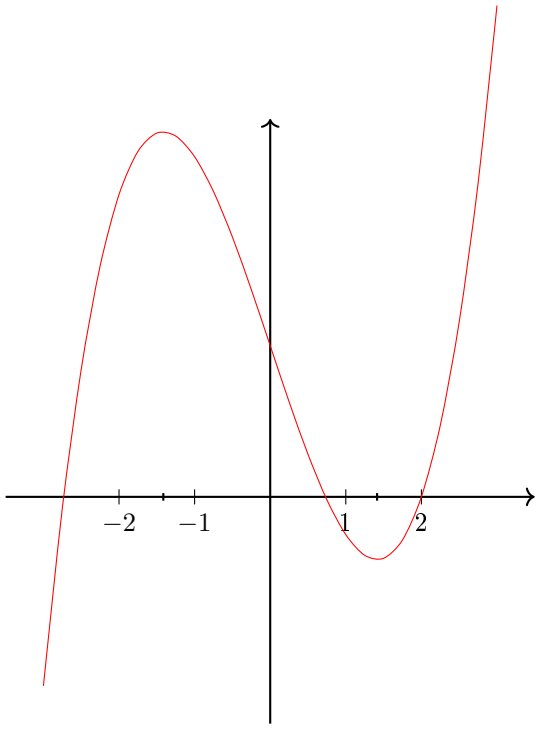
$$u = \sqrt[3]{2 + \sqrt{4 - (-1)^3}} = \sqrt[3]{2 + \sqrt{5}}$$

Dies lässt sich nicht leicht ausrechnen, in der Tat ist $u \notin \mathbb{Q}$. Der Taschenrechner sagt: $u \approx 1,61803\ldots$, und wegen $\frac{p}{3u} = -\frac{1}{u}$ ist hier $x = u - \frac{1}{u}$, also haben wir $\frac{1}{u} \approx 0,61803\ldots$. Dies zeigt, dass $x \approx 1$ gilt. Tatsächlich stellen wir durch Einsetzen fest, dass $1^3 = -3 \cdot 1 + 4$ gilt, also ist $x = 1$ eine exakte Lösung der Gleichung. Damit ist bewiesen, dass gilt

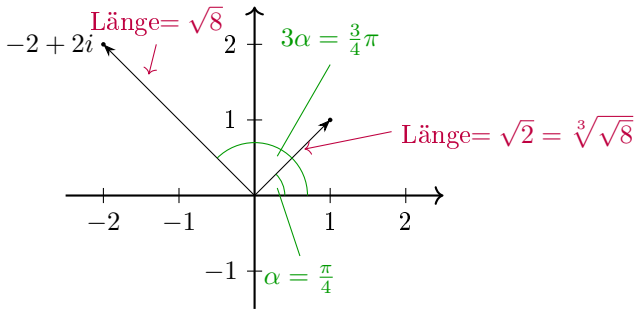
$$\sqrt[3]{2 + \sqrt{5}} - \frac{1}{\sqrt[3]{2 + \sqrt{5}}} = 1.$$

Übungsaufgabe: Rechne dies (exakt, d. h.ohne Taschenrechner) nach!

3.) Sei nun die Gleichung $x^3 = 6x - 4$ gegeben. Hier kann man mittels Kurvendiskussion feststellen, dass es 3 reelle Lösungen geben muss: Betrachte die Funktion $f(x) = x^3 - 6x + 4$, dann ist $f'(x) = 3x^2 - 6$ also $f'(x) = 0$ für $x = \pm\sqrt{2}$. Außerdem stellt man durch Einsetzen fest, dass $x = 2$ eine Lösung der gegebenen Gleichung, also eine Nullstelle von f ist. Damit sieht eine qualitatives Bild von f (d. h., wir wissen nur, dass es drei Nullstellen geben muss, aber nicht, wo diese genau liegen) so aus:



Was liefert uns die Cardanosche Formel? Es ist $x = u + \frac{2}{u}$ und $u = \sqrt[3]{-2+\sqrt{-4}}$. Hierbei beobachten wir ein neues Phänomen: Wir wissen, dass alle drei Lösungen reell sind, aber um diese mit Hilfe der Cardanoschen Formel ausrechnen zu können, müssen wir mit komplexen Zahlen rechnen. Um $u = \sqrt[3]{-2+\sqrt{-4}} = \sqrt[3]{-2+i\cdot 2}$ zu bestimmen, zeichnen wir diese Zahl in der Gaußschen Zahlenebene:



Das Bild zeigt, dass $\sqrt[3]{-2+2i} = 1+i$ gilt, und in der Tat rechnet man nach
$(1+i)^3 = 1 + 3\cdot 1^2\cdot i + 3\cdot 1\cdot i^2 + i^3 = 1 + 3i - 3 - i = -2 + 2i$
Dann ist $x = u + \frac{p}{3u} = 1 + i + \frac{6}{3(1+i)} = 1 + i + \frac{2}{1+i} = 1 + i + \frac{2(1-i}{1-i^2} = 1 + i + 1 - i = 2$, und damit liefert die Cardanosche Formel also tatsächlich die Lösung $x = 2$.
Wollen wir die anderen beiden Lösungen bestimmen, so verwenden wir, dass $u = \zeta(1+i)$ und $u = \zeta^2(1+i)$ auch Lösungen von $u^3 = -2 + 2i$ sind, mit $\zeta = \cos\left(\frac{2\pi}{3}\right) + i\sin\left(\frac{2\pi}{3}\right) = -\frac{1}{2} + i\frac{1}{2}\sqrt{3}$.

Dann ist für $u = \zeta(1+i)$

$$\begin{aligned} x = u + \frac{2}{u} &= \left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right)(1+i) + \frac{2}{1+i}\overbrace{\left(-\frac{1}{2} - i\frac{\sqrt{3}}{2}\right)}^{\zeta^2=\overline{\zeta}=\zeta^{-1}} \\ &= \left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right)(1+i) + (1-i)\left(-\frac{1}{2} - i\frac{\sqrt{3}}{2}\right) \\ &= \frac{1}{2}\left[(-1+i\sqrt{3})(1+i) + (-1-i\sqrt{3})(1-i)\right] \\ &= \frac{1}{2}\left(-1-\sqrt{3}+i(\sqrt{3}-1) - 1 - \sqrt{3} + i(1-\sqrt{3})\right) \\ &= \frac{1}{2}(-2-2\sqrt{3}) = -1-\sqrt{3} \end{aligned}$$

und analog findet man für $u = \zeta^2(1+i)$, dass

$$x = -1 + \sqrt{3}$$

gilt.

Der Fundamentalsatz der Algebra:

Wir haben in den letzten Kapiteln die Zahlenbereiche immer weiter ausgeweitet, nämlich:

$$\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R} \subsetneq \mathbb{C}$$

Jede dieser Erweiterungen haben wir vorgenommen, um bestimmte Gleichungen lösen zu können. Die Erweiterung $\mathbb{R} \subsetneq \mathbb{C}$ diente z. B. dazu, die Gleichung $x^2 + 1 = 0$ zu lösen. Wir haben gesehen, dass auch für die Gleichungen $x^n = c$ oder allgemeiner für Gleichungen 2. oder 3. Grades immer Lösungen existieren, und es gibt sogar explizite Formeln dafür. Solche Formeln existieren auch für Gleichungen vom Grad 4, aber nicht mehr ab Grad ≥ 5 (Galois). Trotzdem gilt der folgende berühmte Satz:

Satz 4.12 (Fundamentalsatz der Algebra)**.** *Jede Gleichung der Form*

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0,$$

wobei a_i feste komplexe Zahlen sind, hat mindestens eine Lösung in $\mathbb{C}$.

Einen Beweis werden wir in dieser Vorlesung nicht führen, da man Methoden aus der Analysis braucht. Interessant ist, dass man relativ leicht ein etwas verbessertes Ergebnis ableiten kann (der Beweis dazu kommt später und benutzt Polynomdivision).

Satz 4.13 (Fundamentalsatz der Algebra, 2. Version)**.** *Sei $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$. Dann kann man f schreiben als*

$$f(x) = (x - \lambda_1) \cdot \ldots \cdot (x - \lambda_n),$$

wobei $\lambda_i \in \mathbb{C}$ sind (hierbei kann $\lambda_i = \lambda_j$ für $i \neq j$ vorkommen).

Wir sehen also, dass wir in $\mathbb{C}$ alle möglichen Polynomgleichungen vollständig lösen können, und tatsächlich ist $\mathbb{C}$ in gewisser Weise der größtmögliche Körper.

Kapitel 5

Die natürlichen Zahlen und das Prinzip der vollständigen Induktion

Wir haben bis jetzt die natürlichen Zahlen als gegeben betrachtet und daraus die rationalen, reellen und komplexen Zahlen konstruiert. Hier wollen wir den Aufbau der natürlichen Zahlen etwas genauer studieren. Das folgende Problem zeigt, dass auch die natürlichen Zahlen schon schwierige Probleme hervorbringen können.

Collatz-Ulam-Problem: Sei $n \in \mathbb{N}$ eine natürliche Zahl. Dann definieren wir:

$$T(n) := \begin{cases} 3n+1, & \text{falls } n \text{ ungerade ist} \\ \frac{n}{2}, & \text{falls } n \text{ gerade ist} \end{cases}$$

Jetzt betrachten wir die Folge von Zahlen

$$n, T(n), T(T(n)), T(T(T(n))), \ldots, T^k(n), \ldots$$

Man sagt auch, diese Folge werde rekursiv durch $T^k(n) := T(T^{k-1}(n))$ definiert.
Hier sind einige Beispiele für vorgegebene Startwerte für n:

$n = 1 \to T(n) = 4 \to T(T(n)) = T^2(n) = 2 \to T^3(n) = 1$

$n = 3 \to T(n) = 10 \to T^2(n) = 5 \to T^3(n) = 16 \to T^4(n) = 8 \to T^5(n) = 4 \to T^6(n) = 2 \to T^7(n) = 1$

$n = 6 \to T(n) = 3 \to T^2(n) = 10 \to T^3(n) = 5 \to \ldots \to T^8(n) = 1$

Es stellt sich nun die Frage:
Existiert immer ein N, so dass $T^N(n) = 1$ ist?
In den Beispielen oben ist das so, z. B. ist $N = 7$ für $n = 3$ und $N = 8$ für $n = 6$ (und für $n = 1$ kann man natürlich $N = 0$ oder auch $N = 3$ wählen). Tatsächlich ist dies ein ungelöstes Problem, obwohl man vermutet, dass die Antwort ja ist.

Wir wollen jetzt die offen gebliebene Frage aufgreifen, wie man die Menge $\mathbb{N}$ eigentlich genau definieren kann. Eine Möglichkeit geht auf Giuseppe Peano zurück. Zur Veranschaulichung stellen wir uns die natürlichen Zahlen als eine unendlich lange Kette vor, welche mit 1 beginnt:

Dies kann man mathematisch so formulieren:

- Das Anfangselement 1 ist ein spezielles Element von $\mathbb{N}$.
- Es gibt eine Abbildung $\nu : \mathbb{N} \to \mathbb{N}$, welche ein Element auf seinen Nachfolger abbildet.

Hat man 1 und die Abbildung ν gegeben, dann definiert man: $2 \coloneqq \nu(1), 3 \coloneqq \nu(2), 4 \coloneqq \nu(3)$. Wir erzeugen also aus 1 und der Nachfolgerabbildung ν die gesamte Menge.

Bemerkung: Falls wir das spezielle Element 1 durch Null ersetzen, so können wir genauso $\mathbb{N}_0$ erzeugen.

Für die so erzeugte Menge $\mathbb{N}$ und die Abbildung ν gelten folgende Axiome:

P1) Das Element 1 ist kein Nachfolger, d. h.

$$\forall n \in \mathbb{N} : \nu(n) \neq 1.$$

P2) Unterschiedliche natürliche Zahlen haben unterschiedliche Nachfolger, d. h.

$$\forall n, m \in \mathbb{N} : n \neq m \Rightarrow \nu(n) \neq \nu(m).$$

P3) Sei $S \subset \mathbb{N}$ eine Teilmenge, welche die folgenden Eigenschaften erfüllt:

- $1 \in S$
- $n \in S \Rightarrow \nu(n) \in S$

Dann gilt: $S = \mathbb{N}$.

Die Bedeutung dieser Axiome ist folgende Aussage:

Satz 5.1. *Sei M eine Menge mit einem fest gewählten Element $1 \in M$ und einer Abbildung $\nu : M \to M$, welche die Axiome P1,P2 und P3 erfüllt. Dann existiert eine bijektive Abbildung $\alpha : M \to \mathbb{N}$.*

Dieser Satz gibt eine Antwort auf die Frage nach der Definition der natürlichen Zahlen: Die Peano-Axiome charakterisieren die Menge $\mathbb{N}$ eindeutig, d. h., bis auf Bijektionen gibt es nur eine Menge, welche diese Axiome erfüllt. Dies ist ganz anders als z. B. bei den Körperaxiomen, denn es gibt viele verschiedene Körper, wie wir gesehen haben.

Bemerkung: Man kann eine Menge M, welche P1-P3 erfüllt, wie folgt aus der leeren Menge aufbauen (nach John von Neumann):

$$1 \coloneqq \varnothing, \quad 2 \coloneqq \{\varnothing\}, \quad 3 \coloneqq \{\varnothing, \{\varnothing\}\}, \ldots,$$

allgemein:

$$\nu(n) = n \cup \{n\}.$$

Wir wollen nun zwei wichtige Prinzipien kennenlernen, welche auf der Definition der natürlichen Zahlen basieren, nämlich das Rekursionsprinzip und die Beweismethode der vollständigen Induktion. Wir diskutieren zunächst ersteres. Rekursive Definitionen werden vor allem für Folgen benutzt: Eine Folge ist eine Hintereinanderreihung von Zahlen (z. B. natürliche, ganze, rationale oder komplexe Zahlen), welche man z. B. mit $a_1, a_2, a_3, \ldots$ oder auch mit $(a_n)_{n \in \mathbb{N}}$ bezeichnet. Zum Beispiel haben wir die Folge der geraden natürlichen Zahlen: $a_1 = 2, a_2 = 4, a_3 = 6, \ldots$, also $a_n = 2n \forall n \in \mathbb{N}$. Analog bilden die ungeraden Zahlen eine Folge: $a_1 = 1, a_2 = 3, a_3 = 5, \ldots$, also $a_n = 2n - 1 \forall n \in \mathbb{N}$. Formal definiert man dies so:

Definition 5.2.

1.) Eine Folge ist eine Abbildung $a : \mathbb{N} \to M$, wobei M eine beliebige Menge ist. Man schreibt dann a_n für das Folgenelement $a(n)$.

2.) Sei $\nu : \mathbb{N} \to \mathbb{N}$ die Nachfolgerfunktion der natürlichen Zahlen (d. h. $\nu(n) = n + 1$, siehe weiter oben). Eine rekursive Definition einer Folge $(a_n)_{n\in\mathbb{N}}$ (oder $a : \mathbb{N} \to M$) besteht aus den folgenden Daten:

- *dem Folgenelement $a_1 = a(1)$.*
- *einer Vorschrift, wie $a(\nu(n))$ aus $a(n)$ bestimmt werden kann, und zwar für alle $n \in \mathbb{N}$.*

Dadurch wird $a(n)$ eindeutig festgelegt.

Für die obigen Beispiele der geraden bzw. ungeraden Zahlen wären die rekursiven Definitionen wie folgt:

gerade Zahlen: $a_1 \coloneqq 2, a_{n+1} \coloneqq a_n + 2$

ungerade Zahlen: $a_1 \coloneqq 1, a_{n+1} \coloneqq a_n + 2$

Weitere Beispiele:

1.) Sei $a \in \mathbb{C}, a \neq 0$. Wir definieren die Zahl a^n rekursiv durch: $a_1 \coloneqq a, a^{n+1} \coloneqq a^n \cdot a$.

2.) Wir definieren $n!$ (gesprochen „n Fakultät“) durch: $0! \coloneqq 1, n! \coloneqq n \cdot (n-1)!$.

3.) Seien Zahlen $a_1, \ldots, a_n$ vorgegeben. Wir können rekursiv eine präzise Definition der Summe $\sum_{i=1}^{n} a_i$ oder des Produkts $\prod_{i=1}^{n} a_i$ geben:

$$\text{Summe :} \quad \sum_{i=1}^{1} a_i \coloneqq a_1, \qquad \sum_{i=1}^{n} a_i \coloneqq \sum_{i=1}^{n-1} a_i + a_n$$

$$\text{Produkt :} \quad \prod_{i=1}^{1} a_i \coloneqq a_1, \qquad \prod_{i=1}^{n} a_i \coloneqq \left(\prod_{i=1}^{n-1} a_i\right) \cdot a_n$$

In diesen Beispielen haben haben wir eine schon bekannte Definition nur in rekursiver Weise umformuliert. Aber es gibt auch Folgen, welche man leicht rekursiv definieren kann, bei denen eine direkte Formel bzw. Definition nicht einfach zu finden ist. Die folgende Definition ist das berühmteste Beispiel.

Definition 5.3 (Fibonacci-Zahlen)**.**
Sei $F(1) \coloneqq 1, F(2) \coloneqq 1$ und

$$F(n+2) \coloneqq F(n) + F(n+1).$$

(anders geschrieben: $F(\nu(\nu(n))) \coloneqq F(n) + F(\nu(n))$)

Nach ihrem Erfinder Leonardo Pisano Fibonacci beschreibt diese Folge die Vermehrung einer Kaninchenpopulation, beginnend mit einem Elternpaar. Die ersten Elemente dieser Folge sehen so aus:

n	1	2	3	4	5	6	7	8	9	10
$F(n)$	1	1	2	3	5	8	13	21	34	55

Mathematisch ist vor allem die direkte Formel für $F(n)$ interessant, nämlich

$$F(n) = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right)$$

Man erhält hier trotz des mehrfachen Auftretens von $\sqrt{5}$ immer eine natürliche Zahl!

Nun kommen wir zum Beweisprinzip der vollständigen Induktion, welches an vielen Stellen der Mathematik verwendet wird.

Satz 5.4. *Sei für alle natürlichen Zahlen $n \in \mathbb{N}$ eine Aussage $A(n)$ gegeben (d. h., der Wahrheitswert der Aussage hängt von der Zahl n ab). Angenommen, es würde gelten:*

1.) $A(1)$ ist wahr.

2.) Falls $A(n)$ wahr ist, dann ist auch $A(n+1)$ wahr, anders geschrieben: $A(n) \Rightarrow A(n+1)$.

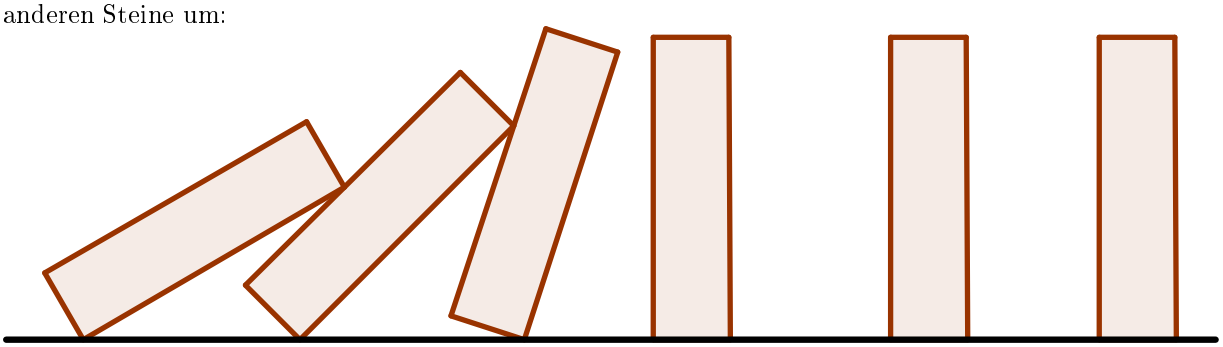
Dann ist $A(n)$ wahr für alle $n \in \mathbb{N}$.

Beweis. Wir führen den Beweis unter Verwendung der Peano-Axiome für die natürlichen Zahlen. Wir definieren die Menge

$$S := \{n \in \mathbb{N} | A(n) \text{ ist wahr}\}.$$

S ist offensichtlich eine Teilmenge von $\mathbb{N}$ und es gilt $1 \in S$. Außerdem gilt folgendes: Falls $n \in S$ ist, dann ist $A(n)$ wahr (dies war die Definition von S), dann ist wegen Annahme 2. im zu beweisenden Satz aber auch $A(n+1)$ wahr, also $n+1 \in S$. Wir erhalten also, dass immer gilt $n \in S \Rightarrow n+1 \in S$. Nach dem Axiom P3 schlussfolgern wir dann: $S = \mathbb{N}$, d. h., die Aussage $A(n)$ ist wahr für alle $n \in \mathbb{N}$. □

Die Bedeutung dieses Satzes besteht darin, dass man die Aussage eines Satzes, welche von einer natürlichen Zahl n abhängt, nicht direkt beweisen muss, sondern man muss nur beweisen, dass sie für $n = 1$ gilt und, dass aus der Gültigkeit für n auch die Gültigkeit für $n+1$ folgt. Anschaulich kann man sich dies vorstellen wie eine Reihe von hintereinander aufgestellten Dominosteinen: fällt der erste Stein um, so fallen auch alle anderen Steine um:



Wie führt man einen Beweis mittels vollständiger Induktion nun praktisch durch? Es gibt drei Schritte:

1.) Induktionsanfang: Die Gültigkeit der Aussage für $n = 1$ wird verifiziert.

2.) Induktionsvorraussetzung: Für eine beliebige, aber feste Zahl n wird die Aussage als wahr angenommen.

3.) Induktionsschritt: Hier wird durch logische Schlüsse aus der Induktionsvoraussetzung hergeleitet, dass die Aussage auch für $n+1$ wahr ist.

Kann man diese drei Schritte ausführen, dann besagt Satz 5.4, dass die zu beweisende Aussage für alle $n \in \mathbb{N}$ gilt. Vorsicht: Falls man die drei Schritte nicht ausführen kann, dann kann man daraus nichts schlussfolgern, d. h., die zu beweisende Aussage könnte trotzdem richtig sein.
Wir diskutieren jetzt einige Beispiele:

1.) Wir betrachten die folgenden Rechnungen:

$$\begin{array}{lcll} 1 & = & 1 & = & 1^2 \\ 1+3 & = & 4 & = & 2^2 \\ 1+3+5 & = & 9 & = & 3^2 \\ 1+3+5+7 & = & 16 & = & 4^2 \end{array}$$

Man kann vermuten, dass die Summe von aufeinanderfolgenden ungeraden Zahlen immer eine Quadratzahl ist, genauer, dass gilt:

$$1 + 3 + 5 + \ldots + 2n - 1 = n^2 \tag{5.1}$$

Dies wollen wir durch vollständige Induktion beweisen. Wir führen also die drei Schritte aus:

Induktionsanfang: Für $n = 1$ lautet die Aussage (5.1) einfach: $1 = 1^2$, was offensichtlich richtig ist.

Induktionsvoraussetzung: Wir nehmen an, dass für ein festes $k \in \mathbb{N}$ die Aussage (5.1) richtig ist, d. h., für dieses k (aber a priori erst einmal nur für dieses) gilt:

$$1 + 3 + 5 + \ldots + (2k - 1) = k^2 \tag{5.2}$$

Induktionsschritt: Wir formen die Gleichung (5.2) um, wir addieren $2k + 1$ auf beiden Seiten:

$$1 + 3 + 5 + \ldots + (2k - 1) + (2k + 1) = k^2 + 2k + 1$$

Dies ist aber das gleiche, wie

$$\begin{aligned} & 1 + 3 + 5 + \ldots + (2k - 1) + (2k + 1) = (k + 1)^2 \\ \Leftrightarrow \quad & 1 + 3 + \ldots + (2(k + 1) - 1) = (k + 1)^2 \end{aligned}$$

Dies ist aber genau die Gleichung (5.1), wenn wir für n die Zahl $k + 1$ einsetzen. Damit ist der Induktionsschritt vollzogen und die gewünschte Aussage (also die Richtigkeit von Formel (5.1)) bewiesen.

2.) Als zweites Beispiel wollen wir eine Formel für komplexe Zahlen beweisen: Sei $x \in \mathbb{C}$, aber $x \neq 1$. Dann gilt für alle $n \in \mathbb{N}$:

$$1 + x + x^2 + \ldots + x^{n-1} = \frac{1 - x^n}{1 - x} \tag{5.3}$$

Induktionsanfang: Sei $n = 1$, dann sagt Formel (5.3):

$$1 = \frac{1 - x}{1 - x} \overset{x \neq 1}{=} 1$$

und das ist ganz offensichtlich richtig.

Induktionsvoraussetzung: Angenommen, für festes $k \in \mathbb{N}$ gelte

$$1 + x + x^2 + \ldots + x^{k-1} = \frac{1 - x^k}{1 - x}. \tag{5.4}$$

Induktionsschritt: Wir addieren x^k auf beiden Seiten von (5.4)

$$\begin{aligned} & 1 + x + x^2 + \ldots + x^{k-1} + x^k = \frac{1 - x^k}{1 - x} + x^k \\ \Leftrightarrow \quad & 1 + x + x^2 + \ldots + x^{k-1} + x^k = \frac{1 - x^k}{1 - x} + \frac{(1 - x)x^k}{1 - x} \\ \Leftrightarrow \quad & 1 + x + x^2 + \ldots + x^{k-1} + x^{(k+1)-1} = \frac{1 - x^k + x^k - x^{k+1}}{1 - x} \\ \Leftrightarrow \quad & 1 + x + x^2 + \ldots + x^{k-1} + x^{(k+1)-1} = \frac{1 - x^{k+1}}{1 - x} \end{aligned}$$

Dies ist genau Gleichung (5.3) für $n = k + 1$.

Bemerkung: Es gibt viele Varianten der vollständigen Induktion, z. B. können wir in Satz 5.4 statt der Menge $\mathbb{N}$ auch die Menge $\mathbb{N}_0$ betrachten, und eine Aussage $A(n)$, welche für alle $n \in \mathbb{N}_0$ definiert ist. Dann müssen wir nur die 1.) ersetzen durch

1.)′ $A(0)$ ist wahr

und Bedingung 2.) bleibt gleich. Analog betrachten wir die ganzen Zahlen $\mathbb{Z}$, wählen ein festes $m \in \mathbb{Z}$ und untersuchen eine Aussage, welche für alle Zahlen $n \geq m$ definiert ist. Dann ersetzen wir einfach 1.) durch

1.)″ $A(m)$ ist wahr.

Genauso gibt es die absteigende Induktion: Falls eine Aussage $A(n)$ wahr ist für ein $m \in \mathbb{Z}$ und falls man statt 2.) die modifizierte Version

2.)′ $A(n) \Rightarrow A(n-1)$

beweisen kann, dann gilt die Aussage $A(n)$ für alle Elemente der Menge $\{n \in \mathbb{Z} | n \leq m\}$. Schlussendlich verwendet man häufig die die folgende Variante von Satz 5.4: Es gelte

1.) Die Aussagen $A(1)$ und $A(2)$ sind wahr.

2.) Falls $A(n)$ und $A(n+1)$ wahr sind, dann auch $A(n+2)$.

Dann ist $A(n)$ für alle $n \in \mathbb{N}$ wahr. Damit wollen wir die Formel für die Fibonacci-Zahlen beweisen. Sei also $F(1) = F(2) = 1$ und $F(n+2) = F(n) + F(n+1)$. Wir wollen zeigen, dass dann $\forall n \in \mathbb{N}$ gilt:

$$F(n) = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right)$$

Induktionsanfang: Für $n = 1, 2$ ist diese Formel erfüllt: Es ist

$$F(1) = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2} \right) = \frac{1}{2\sqrt{5}} (1 + \sqrt{5} - 1 + \sqrt{5}) = 1$$

$$F(2) = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^2 - \left(\frac{1-\sqrt{5}}{2} \right)^2 \right) = \frac{1}{4\sqrt{5}} (1 + 2\sqrt{5} + 5 - (1 - 2\sqrt{5} + 5)) = \frac{1}{4\sqrt{5}} (4\sqrt{5}) = 1$$

Induktionsvoraussetzung: Für festes $n \in \mathbb{N}$ gilt:

$$F(n) = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right) \text{ und}$$

$$F(n+1) = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^{n+1} - \left(\frac{1-\sqrt{5}}{2} \right)^{n+1} \right)$$

Induktionsschritt: Wir wollen aus der Induktionsvoraussetzung die Formel

$$F(n+2) = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^{n+2} - \left(\frac{1-\sqrt{5}}{2} \right)^{n+2} \right)$$

ableiten. Nach Definition gilt $F(n+2) = F(n) + F(n+1)$, also

$$\begin{aligned}
F(n+2) &= \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n + \left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}\right] \\
&= \frac{1}{2^n\sqrt{5}}\left[(1+\sqrt{5})^n + \frac{1}{2}(1+\sqrt{5})^{n+1} - (1-\sqrt{5})^n - \frac{1}{2}(1-\sqrt{5})^{n+1}\right] \\
&= \frac{1}{2^{n+1}\sqrt{5}}\left[(1+\sqrt{5})^n(2+1+\sqrt{5}) - (1-\sqrt{5})^n(2+1-\sqrt{5})\right] \\
&= \frac{1}{2^{n+1}\sqrt{5}}\left[(1+\sqrt{5})^n(3+\sqrt{5}) - (1-\sqrt{5})^n(3-\sqrt{5})\right]
\end{aligned}$$

Wollen wir also zeigen, dass gilt

$$F(n+2) = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n+2} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+2}\right),$$

dann müssen wir die Gleichheit

$$F(n+2) = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n+2} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+2}\right) = \frac{1}{2^{n+1}\sqrt{5}}\left[(1+\sqrt{5})^n(3+\sqrt{5}) - (1-\sqrt{5})^n(3-\sqrt{5})\right]$$

zeigen. Dies ist äquivalent zu:

$$\begin{aligned}
& \frac{1}{2^{n+1}\sqrt{5}}\frac{1}{2}\left[(1+\sqrt{5})^{n+2} - (1-\sqrt{5})^{n+2}\right] = \frac{1}{2^{n+1}\sqrt{5}}\left[(1+\sqrt{5})^n(3+\sqrt{5}) - (1-\sqrt{5})^n(3-\sqrt{5})\right] \\
\Leftrightarrow \quad & \frac{1}{2}\left[(1+\sqrt{5})^{n+2} - (1-\sqrt{5})^{n+2}\right] = \left[(1+\sqrt{5})^n(3+\sqrt{5}) - (1-\sqrt{5})^n(3-\sqrt{5})\right] \\
\Leftrightarrow \quad & (1-\sqrt{5})^n \underbrace{\left[(3-\sqrt{5}) - \frac{1}{2}(1-\sqrt{5})^2\right]}_{\substack{=3-\sqrt{5}-\frac{1}{2}(1-2\sqrt{5}+5) \\ =3-\frac{1}{2}6-\sqrt{5}+\frac{1}{2}2\sqrt{5} \\ =0}} = (1+\sqrt{5})^n \underbrace{\left[(3+\sqrt{5}) - \frac{1}{2}(1+\sqrt{5})^2\right]}_{\substack{=3+\sqrt{5}-\frac{1}{2}(1+2\sqrt{5}+5) \\ =3-\frac{1}{2}6+\sqrt{5}-\frac{1}{2}2\sqrt{5} \\ =0}}
\end{aligned}$$

Binomialkoeffizienten: Wir haben schon mehrfach binomische Formeln verwendet, hier diskutieren wir dies noch einmal systematisch.

Definition 5.5. *Seien $n, k \in \mathbb{N}_0$, dann setzen wir*

$$\begin{aligned}
\binom{n}{k} &:= \frac{n\cdot(n-1)\cdot(n-2)\cdot\ldots\cdot(n-k+1)}{k\cdot(k-1)\cdot\ldots\cdot 2\cdot 1} \\
&= \frac{n\cdot(n-1)\cdot(n-2)\cdot\ldots\cdot(n-k+1)\cdot(n-k)\cdot(n-k-1)\cdot\ldots\cdot 2\cdot 1}{k\cdot(k-1)\cdot\ldots\cdot 2\cdot 1\cdot(n-k)\cdot(n-k-1)\cdot\ldots\cdot 2\cdot 1} \\
&= \frac{n!}{(n-k)!\cdot k!}
\end{aligned}$$

Der Ausdruck $\binom{n}{k}$ heißt Binomialkoeffizient und wird „n über k“ oder „k aus n“ gesprochen. Falls $k > n$ ist, setzen wir $\binom{n}{k} := 0$.

Beispiele:
$$\binom{4}{2} = \frac{4\cdot 3\cdot \cancel{2}\cdot \cancel{1}}{\cancel{2}\cdot\cancel{1}\cdot 2\cdot 1} = \frac{4\cdot 3}{2} = \frac{12}{2} = 6.$$
$$\binom{5}{3} = \frac{5!}{3!\cdot 2!} = \frac{5\cdot 4\cdot \cancel{3}\cdot \cancel{2}}{\cancel{3}\cdot\cancel{2}\cdot 2} = \frac{5\cdot 4}{2} = 10.$$
$$\binom{7}{5} = \binom{7}{2} = \frac{7\cdot 6}{2\cdot 1} = \frac{42}{2} = 21.$$

Es gelten die folgenden Regeln für die Binomialkoeffizienten:

Lemma 5.6.

$$\binom{n}{0} = \frac{n!}{n!\cdot 0!} = 1.$$
$$\binom{n}{1} = \frac{n!}{(n-1)!} = \frac{n\cdot \cancel{(n-1)}\cdot\ldots\cdot \cancel{2}\cdot\cancel{1}}{\cancel{(n-1)}\cdot\ldots\cdot\cancel{2}\cdot\cancel{1}} = n.$$
$$\binom{n}{2} = \frac{n!}{(n-2)!\cdot 2} = \frac{n\cdot(n-1)\cdot\cancel{(n-2)}\cdot\ldots\cdot\cancel{2}\cdot\cancel{1}}{\cancel{(n-2)}\cdot\ldots\cdot\cancel{2}\cdot\cancel{1}\cdot 2} = \frac{n\cdot(n-1)}{2}.$$
$$\binom{n}{k} = \frac{n!}{(n-k)!\cdot k!} = \frac{n!}{k!\cdot(n-k)!} = \binom{n}{n-k} \quad \textit{(schon bei Beispiel } \binom{7}{5} \textit{ benutzt).}$$

$$\begin{aligned}\binom{n}{k} + \binom{n}{k-1} &= \frac{n!}{(n-k)!\cdot k!} + \frac{n!}{(n-k+1)!\cdot(k-1)!} = \frac{n!}{(n-k)!\cdot(k-1)!}\cdot\left(\frac{1}{k} + \frac{1}{n-k+1}\right)\\ &= \frac{n!}{(n-k)!\cdot(k-1)!}\cdot\left(\frac{n-k+1+k}{k\cdot(n-k+1)}\right) = \frac{n!\cdot(n+1)}{(n-k)!\cdot(n-k+1)\cdot(k-1)!\cdot k}\\ &= \frac{(n+1)!}{(n+1-k)!\cdot k!} = \binom{n+1}{k}.\end{aligned}$$

Es gibt eine wichtige Interpretation der Zahl $\binom{n}{k}$:

Lotterie: Sei eine Menge von Kugeln, auf welche die Zahlen 1 bis n aufgedruckt sind, gegeben. Wieviele Möglichkeiten gibt es, k Zahlen daraus zu ziehen (z. B. $n = 49, k = 6$: „echtes Lotto“)?
Für die erste Kugel hat man n Möglichkeiten, für die Zweite nur noch $n-1$, für die Dritte $n-2$ usw. Die Anzahl der Möglichkeiten, k Zahlen aus n Zahlen auszuwählen, ergibt sich durch Multiplikation dieser „Einzelmöglichkeiten“, also hat man $n\cdot(n-1)\cdot(n-2)\cdot\ldots\cdot(n-k+1)$ viele Möglichkeiten. Als Beispiel betrachten wir den Fall $n = 4, k = 2$, dann kann man die Paare von Zahlen (oder Kugeln) $1|2, 1|3, 1|4, 2|1, 2|3, 2|4, 3|1, 3|2, 3|4, 4|1, 4|2, 4|3$ wählen, also gibt es $4\cdot 3 = 12$ Stück. Dies ist genau die Zahl $n\cdot(n-k+1) = n\cdot(n-1)$. Falls $k = n$ ist, erhält man also alle Möglichkeiten, n Zahlen anzuordnen, und dies ist dann $n!$.
Bei der Lotterie kommt es nun aber nicht auf die Reihenfolge der gezogenen Zahlen/Kugeln an, also ist die Anzahl der Möglichkeiten, k Zahlen/Objekte aus n Zahlen/Objekten auszuwählen, ohne auf die Reihenfolge zu achten, gleich

$$\frac{n\cdot(n-1)\cdot\ldots\cdot(n-k+1)}{k!}$$

und dies ist genau der Binomialkoeffizient $\binom{n}{k}$.

Der Name Binom bedeutet Zweiterm und führt zur binomischen Formel, welche wir schon in Spezialfällen verwendet haben. Zum Beispiel gilt:

$$\begin{aligned}(x+y)^0 &= 1\\ (x+y)^1 &= x+y\\ (x+y)^2 &= x^2+2xy+y^2\\ (x+y)^3 &= x^3+3x^2y+3xy^2+y^3\\ (x+y)^4 &= x^4+4x^3y+6x^2y^2+4xy^3+y^4\end{aligned}$$

Man sieht, dass sich alle vorkommenden Koeffizienten als Binomialkoeffizienten schreiben lassen, es ist $1=\binom{2}{2}, 2=\binom{2}{1}, 3=\binom{3}{1}, 4=\binom{4}{1}, 6=\binom{4}{2}$. Dies führt zu folgender allgemeinen binomischen Formel:

Satz 5.7. *Für beliebige komplexe Zahlen $x, y \in \mathbb{C}$ und für alle $n \in \mathbb{N}_0$ gilt:*

$$\begin{aligned}(x+y)^n &= x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \ldots + \binom{n}{n-1}xy^{n-1} + y^n\\ &= \sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k\end{aligned}$$

Beweis. Wir benutzen wieder vollständige Induktion.

Induktionsanfang: Für $n = 0$ ist $(x+y)^0 = 1$ und der Ausdruck $\sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k$ vereinfacht sich zu $\sum_{k=0}^{0}\binom{0}{0}x^0y^0 = 1$, also ist die Formel für $n = 0$ korrekt.

Induktionsvoraussetzung: Für eine feste Zahl $n \in \mathbb{N}_0$ gelte

$$(x+y)^n = \sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k \tag{5.5}$$

Induktionsschritt: Wir multiplizieren die Gleichung (5.5) auf beiden Seiten mit $(x+y)$ und erhalten:

$$
\begin{aligned}
& (x+y)^n \cdot (x+y) = \left(\sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k\right) \cdot (x+y) \\
\Leftrightarrow \quad & (x+y)^{n+1} = \left(\sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k\right) \cdot x + \left(\sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k\right) \cdot y \\
\Leftrightarrow \quad & (x+y)^{n+1} = \sum_{k=0}^{n} \binom{n}{k} x^{n-k+1} y^k + \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^{k+1} \\
\Leftrightarrow \quad & (x+y)^{n+1} = x^{n+1} + \sum_{k=1}^{n} \binom{n}{k} x^{n-k+1} y^k + \sum_{k=0}^{n-1} \binom{n}{k} x^{n-k} y^{k+1} + y^{n+1} \qquad \mid \text{ersetze } k \text{ durch } k-1 \\
\Leftrightarrow \quad & (x+y)^{n+1} = x^{n+1} + \sum_{k=1}^{n} \binom{n}{k} x^{n-k+1} y^k + \sum_{k=1}^{n} \binom{n}{k-1} x^{n-(k-1)} y^{(k-1)+1} + y^{n+1} \\
\Leftrightarrow \quad & (x+y)^{n+1} = x^{n+1} + \sum_{k=1}^{n} \binom{n}{k} x^{n-k+1} y^k + \sum_{k=1}^{n} \binom{n}{k-1} x^{n-k+1} y^k + y^{n+1} \\
\Leftrightarrow \quad & (x+y)^{n+1} = x^{n+1} + \sum_{k=1}^{n} \underbrace{\left(\binom{n}{k} + \binom{n}{k-1}\right)}_{\overset{\text{Lemma 5.6}}{=} \binom{n+1}{k}} x^{n-k+1} y^k + y^{n+1} \\
\Leftrightarrow \quad & (x+y)^{n+1} = x^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} x^{n-k+1} y^k + y^{n+1} \\
\Leftrightarrow \quad & (x+y)^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} x^{(n+1)-k} y^k
\end{aligned}
$$

Dies ist aber nichts anderes als Formel (5.5), bei welcher die Variable n durch die Variable $n+1$ ersetzt wurde. □

Wir können eine interessante Konsequenz der allgemeinen binomischen Formel ableiten:

Korollar 5.8.

$$
\begin{aligned}
\forall n \in \mathbb{N}: \qquad (1+x)^n &= \sum_{k=0}^{n} \binom{n}{k} x^k \\
\textit{Es gilt:} \qquad 2^n &= \binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{n} \\
0 &= \binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \ldots + (-1)^n \binom{n}{n} \\
2^{n-1} = \frac{1}{2}(2^n + 0) &= \binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \ldots
\end{aligned}
$$

(beachte: $\binom{n}{k} = 0 \; \forall k > n$, also bricht die Summe $+\ldots$ entweder bei $\binom{n}{n-1}$ oder bei $\binom{n}{n}$ ab)

Beweis. Die Gleichung $(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k$ folgt aus Satz 5.7, indem man in der binomischen Formel $y = 1$ setzt. Setzt man dann noch $x = 1$ oder $x = -1$, so erhält man die anderen Formeln im Korollar. □

Wir wollen jetzt einen letzten wichtigen Aspekt der natürlichen Zahlen studieren, nämlich

Primzahlen: Wir wiederholen folgende sicherlich bekannte Definition:

Definition 5.9. *Eine natürliche Zahl $p \in \mathbb{N}$ heißt Primzahl, falls sie von genau zwei Zahlen geteilt wird (nämlich 1 und sich selbst). Die Zahl 1 ist damit keine Primzahl. Wir bezeichnen die Menge der Primzahlen mit*

$$\mathbb{P} = \{2, 3, 5, 7, 11, 13, 17, \ldots\}$$

Seit der Antike hat man versucht, Verfahren zu entwickeln, um für eine gegebene Zahl zu testen, ob sie eine Primzahl ist. Eines der berühmtesten Verfahren ist das Folgende, welches alle Primzahlen von 2 bis zu einer vorgegebenen Zahl liefert:

Sieb des Eratosthenes: Man gibt sich eine feste Zahl n vor und schreibt alle Zahlen von 2 bis n auf. Dann streicht man alle Vielfachen von 2, dann alle Vielfachen von 3 usw. Hat man alle vorkommenden Vielfachen aller Zahlen gestrichen, dann bleiben genau die Primzahlen zwischen 2 und n übrig.

Beispiel: $n = 30$

	2	3	~~4~~	5	~~6~~
7	~~8~~	~~9~~	~~10~~	11	~~12~~
13	~~14~~	~~15~~	~~16~~	17	~~18~~
19	~~20~~	~~21~~	~~22~~	23	~~24~~
~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~

Die Zahlen in den Kästchen sind alle Primzahlen bis 30.

Warum sind Primzahlen wichtig? Unter anderem, weil man daraus alle anderen natürlichen Zahlen aufbauen kann, wie folgender Satz zeigt.

Satz 5.10. *Jede natürliche Zahl ist Produkt von Primzahlen.*

Beweis. Wir benutzen wieder vollständige Induktion, und zwar wollen wir für alle $n \in \mathbb{N}$ die folgende Aussage $A(n)$ beweisen:

$$A(n): \ n \text{ ist ein Produkt von Primzahlen}$$

Induktionsanfang: Wir müssen die Aussage $A(1)$ beweisen, also die Aussage: 1 ist ein Produkt von Primzahlen. Wir legen fest, dass das Produkt von 0 Zahlen immer gleich 1 sein soll (daher ist auch $x^0 = 1 \, \forall x$). Also ist 1 Produkt von 0 Primzahlen, d. h. $A(1)$ ist wahr.

Induktionsvoraussetzung: Wir wählen ein festes $n \in \mathbb{N}$ und nehmen an, dass $A(k)$ wahr ist für alle $k \leq n$. (Dies ist eine Variante des Prinzips der vollständigen Induktion, welche man analog zu Satz 5.4 beweisen kann.)

Induktionsschritt: Wir wollen zeigen, dass die Aussage $A(n+1)$ gilt. Es gibt zwei Möglichkeiten: Entweder die Zahl $n+1$ ist selbst eine Primzahl, dann ist sie natürlich ein Produkt von Primzahlen und die Aussage $A(n+1)$ ist wahr. Oder aber $n+1$ ist keine Primzahl, dann gibt es also eine Zahl a mit $1 < a < n+1$ so, dass a ein Teiler von $n+1$ ist, also gilt $n+1 = a \cdot b$, wobei auch $1 < b < n+1$ ist. Nach Induktionsvoraussetzung sind dann a und b Produkte von Primzahlen und damit ist (wegen $n+1 = a \cdot b$) auch die Zahl $n+1$ ein Produkt von Primzahlen, d. h. $A(n+1)$ ist auch in diesem Fall wahr. □

Mit diesem Satz wissen wir, dass sich jede Zahl als Produkt von Primzahlen schreiben lässt, aber es ist sehr schwierig, für eine gegebene Zahl diese Zerlegung zu finden. Wenn man z. B. zwei Primzahlen p und q hat, welche beide 100 Ziffern haben (d. h. p und q sind etwa so groß wie 10^{100}), dann kann man mit einem Computer leicht das Produkt $a := p \cdot q$ ausrechnen (a hat dann ca. 200 Ziffern). Aber: Wenn man nur die Zahl a kennt, ist es (derzeit) völlig unmöglich (auch mit den leistungsfähigsten Computern), die Zahlen p und q zu bestimmen. Auf diesem einfachen Prinzip basieren viele Verschlüsselungsvefahren.

Wieviele Primzahlen gibt es nun? Die erste und wichtigste Antwort ist der folgende klassische Satz.

Satz 5.11 (Euklid)**.** *Es gibt unendlich viele Primzahlen.*

Beweis. Wir führen einen indirekten Beweis: Angenommen, es gäbe nur endlich viele Primzahlen $p_1, \ldots, p_n$. Dann betrachten wir die Zahl

$$N := p_1 \cdot \ldots \cdot p_n + 1$$

Offensichtlich ist N nicht durch die Zahlen $p_1, \ldots, p_n$ teilbar (denn wenn man N durch eine der Zahlen p_i teilt, bleibt stets der Rest 1). Da N nach Satz 5.10 ein Produkt von Primzahlen ist, muss N selbst eine Primzahl sein. Dies ist ein Widerspruch zu unserer Annahme, dass $p_1, \ldots, p_n$ alle Primzahlen sind. Damit ist die Annahme falsch und es gibt also unendlich viele Primzahlen. □

Ebenso interessant ist die Frage, wieviele Primzahlen es gibt, welche kleiner als eine gegebene Zahl sind. Wir wollen ohne Beweise einige Bemerkungen hierzu machen. Definiere für alle $x \in \mathbb{R}$:

$$\Pi(x) := \text{Anzahl an Primzahlen} \leq x$$

Die ersten Werte von $\Pi(x)$ können wir ausrechnen: $\Pi(1) = 0, \Pi(2) = 1, \Pi(3) = \Pi(4) = 2, \ldots, \Pi(10) = 4$. Ein Computer berechnet: $\Pi(100) = 25, \Pi(1000) = 168, \Pi(10000) = 1229, \ldots$
Man stellt fest, dass die Zahl $\log_{10} x \cdot \frac{\Pi(x)}{x}$ für große x etwa 0,45 ist. Hierbei gibt $\log_{10} x$ die Anzahl der Dezimalstellen von x an. Genauer kann man folgendes zeigen:

Satz 5.12.

$$\lim_{x \to \infty} \frac{\Pi(x)}{x} \cdot \ln(x) = 1$$

$\ln(x)$ *bezeichnet den natürlichen Logarithmus von* x.

Dies bedeutet, dass die Wahrscheinlichkeit, dass $x \in \mathbb{N}$ eine Primzahl ist, in etwa gleich $\frac{1}{\ln(x)}$ ist. Anders formuliert: Für gegebenes x ist der Abstand zur nächsthöheren Primzahl etwa $\ln(x)$. Damit kann man folgendermaßen (große) Primzahlen finden: Wähle eine beliebige (ungerade) Zahl N und betrachte die Folge $N, N+2, N+4, \ldots$ Nach ca. $\frac{\ln(N)}{2}$ Schritten werden wir in der Regel eine Primzahl finden.
Aber: $\forall N \in \mathbb{N}$ gilt: Keine der aufeinanderfolgenden Zahlen

$$(N+1)!+2, (N+1)!+3, (N+1)!+4, \ldots, (N+1)!+(N+1)$$

ist eine Primzahl (denn $(N+1)!+k$ ist durch k teilbar). Also gibt es beliebig lange Folgen aufeinanderfolgender Zahlen ohne Primzahlen.

Es gibt viele ungelöste Probleme, welche mit Primzahlen zu tun haben. Hier einige Beispiele:

1.) Seien n und $n+2$ Primzahlen, dann heißen sie Primzahlzwillinge, z. B.

$$3,5 \qquad 5,7 \qquad 11,13 \qquad 17,19 \qquad \ldots$$

Frage: Gibt es unendlich viele Primzahlzwillinge?

2.) Ist jede gerade Zahl (außer 2) Summe von zwei Primzahlen? Für alle Beispiele scheint es zu stimmen: $4 = 2+2, 6 = 3+3, 8 = 5+3, 10 = 3+7, 12 = 5+7, \ldots$ Tatsächlich hat man dies bis zur Zahl $4 \cdot 10^{18}$ überprüft. Es handelt sich um die sogenannte Goldbachsche Vermutung (nach Christian Goldbach, ∼1700).

3.) Gibt es unendlich viele Primzahlen der Form n^2+1 (z. B. : $2^2+1 = 5, 4^2+1 = 17, 6^2+1 = 37, \ldots$)?

Man sieht: Primzahlen verbergen noch viele Rätsel!

Kapitel 6

Teilung mit Rest

Wir wissen, dass $\mathbb{Z}$ im Gegensatz zu $\mathbb{Q}$ kein Körper ist: falls $a, b \in \mathbb{Z}$, $b \neq 0$, dann existiert der Quotient $\frac{a}{b}$ im Allgemeinen nicht als Element von $\mathbb{Z}$. Aber dafür können wir a durch b mit Rest teilen, genauer gilt folgendes:

Satz 6.1. *Seien $a, b \in \mathbb{N}$. Dann gibt es eindeutig bestimmte Zahlen $q, r \in \mathbb{N}_0$ so, dass gilt:*

$$a = q \cdot b + r \tag{6.1}$$

und so, dass $0 \leq r < b$ ist.

Beweis. Wir führen einen Beweis mit Induktion über a. Zuerst ist der Fall $b = 1$ klar, dann setzt man $q := a$ und $r = 0$. Dann ist (6.1) erfüllt und $r < b$.

Induktionsanfang: $a < b$ (Hier besteht also der Induktionsanfang nicht nur aus einem einzelnen Fall): Dann setzt man einfach: $q := 0$, $r := a$. Es gilt die Gleichung (6.1) und $r = a < b$.

Induktionsvoraussetzung: Wir nehmen an, dass die Aussage des Satzes für alle $a' \in \mathbb{N}$, welche kleiner als ein festes $a \in \mathbb{N}$ sind, bewiesen sei.

Induktionsschritt: Sei $a \geq b$ gegeben. Dann ist $a' := a - b$ kleiner als a, aber $a' \geq 0$, also können wir die Induktionsvoraussetzung für a' anwenden, d. h.

$$\exists q', r \in \mathbb{N}_0 : \; a' = q' \cdot b + r, \;\; r < b.$$

Es folgt, dass

$$a = a' + b = q'b + r + b = (q' + 1)b + r$$

gilt. Damit haben wir eine Darstellung von a wie in Gleichung (6.1). Es bleibt, die Eindeutigkeit zu zeigen. Seien $a = qb + r$ und $a = q'b + r'$ zwei solcher Darstellungen und sei $r \leq r'$. Durch Subtraktion der beiden Gleichungen folgt dann, dass $b(q - q') = r' - r$ ist. Aber aus $0 \leq r < b$, $0 \leq r' < b$ folgt, dass $0 \leq r' - r < b$ gilt, also haben wir $0 \leq q - q' < 1$. Also ist $q = q'$ und damit auch $r = r'$. Falls $r' < r$ ist, ziehen wir die Gleichungen einfach in umgekehrter Reihenfolge voneinander ab.

□

Definition 6.2. *Falls wie oben $a = bq + r$ mit $a, b, q \in \mathbb{N}_0$ und $0 \leq r < b$ gilt, dann schreiben wir*

$$a \equiv r \qquad \mod b,$$

(gesprochen „a kongruent r modulo b“). Außerdem ist $q = \lfloor \frac{a}{b} \rfloor$, hierbei wird für eine reelle Zahl x mit $\lfloor x \rfloor$ die größte Zahl, welche kleiner oder gleich x ist, bezeichnet.

Später wollen wir auch für ganze Zahlen Division mit Rest durchführen. Hierfür gilt die folgende Variante von Satz 6.1:

Satz 6.3. *Seien $a, b \in \mathbb{Z}$ und $b \neq 0$. Dann existieren eindeutig bestimmte Zahlen $q, r \in \mathbb{Z}$ mit*

$$a = qb + r$$

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

Man beachte, dass damit r tatsächlich in $\mathbb{N}_0$ liegt. Der Fall $b = 0$ ist ausgeschlossen, weil sonst $r = a$ und damit sicherlich nicht $r < |b|$ gelten würde. Der Beweis verläuft analog zum Beweis von Satz 6.1.

Aufbauend auf die Division mit Rest können wir nun den sehr wichtigen Euklidischen Algorithmus behandeln. Wir benötigen dazu einige Vorbereitungen.

Definition 6.4. *Sei $a \in \mathbb{N}$, definiere*

$$T(a) \coloneqq \{c \in \mathbb{N} \mid c|a\}$$

als die Menge aller positiven Teiler von a. Seien $a, b \in \mathbb{N}$, dann definiere

$$T(a, b) \coloneqq T(a) \cap T(b)$$

als die Menge der gemeinsamen Teiler von a und b. Setze weiterhin

$$\mathrm{ggT}(a, b) \coloneqq \max\{c \mid c \in T(a, b)\}.$$

$\mathrm{ggT}(a, b)$ *heißt der größte gemeinsame Teiler von a und b.*

Der Euklidische Algorithmus dient der Bestimmung des größten gemeinsamen Teilers. Hierzu formulieren und beweisen wir zunächst folgendes Lemma:

Lemma 6.5. *Seien $a, b \in \mathbb{N}$, $a \geq b$. Wir teilen a mit Rest durch b: $a = qb + r$, d. h. $r \equiv a \mod b$ und $r \in \{0, 1, 2, \ldots, b-1\}$. Dann gilt*

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

Beweis. Sei $c \in T(a, b)$, d. h. $c|a$ (gesprochen „c teilt a“) und $c|b$. Da $r = a - qb$ ist, muss dann auch $c|r$ gelten und damit ist $c \in T(r, b)$. Falls umgekehrt $c \in T(r, b)$ gilt, also $c|r$ und $c|b$, dann können wir $c|a$ schlussfolgern (wegen $a = qb + r$) und somit ist $c \in T(a, b)$. Also haben wir die Gleichheit von Mengen

$$T(a, b) = T(r, b)$$

bewiesen und dann gilt natürlich auch

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

□

Wir kommen jetzt zur Beschreibung des Euklidischen Algorithmus.

Satz 6.6 (Euklidischer Algorithmus)**.** *Gegeben seien zwei Zahlen $a, b \in \mathbb{N}$ mit $a \geq b$. Wir setzen*

- $a_1 \coloneqq a$, $a_2 \coloneqq b$.
- *Für $i = 3, 4, \ldots$ setzen wir $a_{i+2} \coloneqq a_i \mod a_{i+1}$, d. h. wir führen Division mit Rest durch:*

  $$a_i = q a_{i+1} + r$$

  und setzen $a_{i+2} \coloneqq r$.
- *Der Algorithmus stoppt, wenn $a_{k+1} = 0$ ist. Dann gilt*

1.) Der Algorithmus stoppt tatsächlich, d. h.: $\exists k \in \mathbb{N} : a_{k+1} = 0$.

2.) Es ist $\mathrm{ggT}(a, b) = a_k$.

Beweis. Zuerst zeigen wir, dass der Algorithmus wirklich nach endich vielen Schritten stoppt: Da a_{i+2} als Rest von a_i bei Division durch a_{i+1} definiert ist, gilt $a_{i+2} < a_{i+1}$, d. h.wir haben eine streng monoton fallende Folge von natürlichen Zahlen:

$$a_1 > a_2 > a_3 > \dots$$

Also ist nach spätestens a_1 Schritten die Zahl 0 erreicht (tatsächlich aber schon viel eher).

Es bleibt noch zu beweisen, dass tatsächlich $a_k = \mathrm{ggT}(a, b)$ gilt, wenn $a_{k+1} = 0$ ist, wenn also der Algorithmus bei a_{k+1} abbricht. Dafür verwenden wir Lemma 6.5, aus diesem folgt:

$$T(a, b) = T(a_1, a_2) = T(a_2, a_3) = \dots = T(a_{k-1}, a_k) = T(a_k, a_{k+1}) = T(a_k, 0) = T(a_k).$$

Also ist:

$$\mathrm{ggT}(a, b) = \mathrm{ggT}(a_1, a_2) = \mathrm{ggT}(a_2, a_3) = \dots = \mathrm{ggT}(a_k, 0) = a_k$$

□

Bemerkung: Dieser Beweis zeigt, dass a_k ein Teiler von a und b ist, nämlich der größte (eben der ggT), aber sogar noch mehr: wir haben gezeigt, dass jeder gemeinsame Teiler von a und b auch die Zahl $a_k = \mathrm{ggT}(a, b)$ teilt.

Eine Möglichkeit, den Euklidischen Algorithmus aufzuschreiben, ist die folgende Kette von Teilungen mit Rest:

$$\begin{aligned}
a = a_1 &= q_1 a_2 + a_3 = q_1 b + a_3 \\
a_2 &= q_2 a_3 + a_4 \\
a_3 &= q_3 a_4 + a_5 \\
&\vdots \\
a_{k-2} &= q_{k-2} a_{k-1} + a_k \\
a_{k-1} &= q_{k-1} a_k + 0, \quad a_k = \mathrm{ggT}(a, b)
\end{aligned}$$

Beispiele zum Euklidischen Algorithmus:

1.) $a = a_1 = 42$, $b = a_2 = 30$. Es ist dann

$$\begin{aligned}
42 &= 1 \cdot 30 + 12 \\
30 &= 2 \cdot 12 + 6 \\
12 &= 2 \cdot 6 + 0
\end{aligned}$$

$\Rightarrow \mathrm{ggT}(42, 30) = 6$.

2.) $a = a_1 = 175$, $b = a_2 = 20$. Es ist dann

$$\begin{aligned}
175 &= 8 \cdot 20 + 15 \\
20 &= 1 \cdot 15 + 5 \\
15 &= 3 \cdot 5 + 0
\end{aligned}$$

$\Rightarrow \mathrm{ggT}(175, 20) = 5$.

3.) $a = a_1 = 11220$, $b = a_2 = 5187$. Es ist dann

$$\begin{aligned} 11220 &= 2 \cdot 5187 + 846 \\ 5187 &= 6 \cdot 846 + 111 \\ 846 &= 7 \cdot 111 + 69 \\ 111 &= 1 \cdot 69 + 42 \\ 69 &= 1 \cdot 42 + 27 \\ 42 &= 1 \cdot 27 + 15 \\ 27 &= 1 \cdot 15 + 12 \\ 15 &= 1 \cdot 12 + 3 \\ 12 &= 4 \cdot 3 + 0 \end{aligned}$$

$\Rightarrow \text{ggT}(11220, 5187) = 3$.

Man kann den Euklidischen Algorithmus erweitern und damit folgende Aussage beweisen:

Satz 6.7. *Seien $a, b \in \mathbb{N}$, $a \geq b$. Dann gibt es Zahlen $A, B \in \mathbb{Z}$, so dass*

$$\text{ggT}(a, b) = Aa + Bb$$

ist.

Vor dem Beweis schauen wir uns zunächst einige Beispiele an:

Sei wie oben $a = a_1 = 42$, $b = a_2 = 30$. Dann hatten wir

$$\begin{aligned} 42 &= 1 \cdot 30 + 12 \\ 30 &= 2 \cdot 12 + 6 \\ 12 &= 2 \cdot 6 + 0 \end{aligned}$$

Wir können jetzt durch sukzessives Rückwärts-Einsetzen eine Darstellung für $6 = \text{ggT}(42, 30)$ konstruieren:

$$\begin{aligned} 6 &= 1 \cdot 30 - 2 \cdot 12 \\ &= 1 \cdot 30 - 2 \cdot (42 - 1 \cdot 30) \\ &= (-2) \cdot 42 + 3 \cdot 30 \end{aligned}$$

Damit sind in diesem Beispiel $A = -2$ und $B = 3$.

Sei erneut $a = a_1 = 175$, $b = a_2 = 20$, dann hatten wir oben berechnet:

$$\begin{aligned} 175 &= 8 \cdot 20 + 15 \\ 20 &= 1 \cdot 15 + 5 \\ 15 &= 3 \cdot 5 + 0 \\ \Rightarrow \quad 5 &= \text{ggT}(175, 20) \end{aligned}$$

Durch Zurück-Einsetzen erhalten wir:

$$\begin{aligned} 5 &= 20 - 1 \cdot 15 \\ &= 20 - 1 \cdot (175 - 8 \cdot 20) \\ &= 9 \cdot 20 - 1 \cdot 175 \end{aligned}$$

Hier ist also $A = 9$ und $B = -1$.

Beweis von Satz 6.7. Durch vollständige Induktion zeigen wir, dass es für alle Zahlen a_i, welche im Euklidischen Algorithmus vorkommen, ganze Zahlen A_i und B_i gibt, so dass

$$a_i = A_i a + B_i b$$

gilt. Wenn wie im Beweis von Satz 6.6 $a_k = \mathrm{ggT}(a,b)$ ist, dann sind $A := A_k$ und $B := B_k$ die gesuchten Zahlen.

Induktionsanfang: Setze $A_1 := 1$, $B_1 := 0$ und $A_2 := 0$, $B_2 := 1$, dann ist $a = a_1 = 1a$ und $b = a_2 = 1b$, also ist die Aussage für $i = 1, 2$ richtig.

Induktionvoraussetzung: Sei für $j = 1, 2, \ldots, i+1$ eine Darstellung $a_j = A_j a + B_j b$ gefunden.

Induktionsschritt: Nach Definition des Euklidischen Algorithmus ist $a_i = q_i a_{i+1} + a_{i+2}$, also $a_{i+2} = a_i - q_i a_{i+1}$. Dann erhalten wir durch Einsetzen:

$$\begin{aligned} a_{i+2} &= \overbrace{(A_i a + B_i b)}^{a_i} - q_i \overbrace{(A_{i+1} a + B_{i+1} b)}^{a_{i+1}} \\ &= (A_i - q_i A_{i+1})a + (B_i - q_i B_{i+1})b \end{aligned}$$

Wenn wir jetzt $A_{i+2} := A_i - q_i A_{i+1}$ und $B_{i+2} := B_i - q_i B_{i+1}$ definieren, dann gilt wie gewünscht $a_{i+2} = A_{i+2} a + B_{i+2} b$. □

Die Bestimmung der Koeffizienten A_i und B_i lässt sich praktisch mit dem erweiterten Euklidischen Algorithmus durchführen, welchen wir am Beispiel $a = 11220$, $b = 5187$ erläutern.

1.) Man legt eine Tabelle mit vier Spalten wie folgt an:

a_i	q_{i-1}	A_i	B_i
11220		1	0
5187	2	0	1

2.) In jedem Schritt entsteht eine Zeile nach folgender Regel: In jeder der Spalten a_i, A_i und B_i berechnet man ein neues Element nach der Formel:

(vorletztes Element dieser Spalte) − (letzte Zahl q) · (letztes Element dieser Spalte)

Im obigen Beispiel ergibt sich:

a_i	q_{i-1}	A_i	B_i
11220		1	0
5187	2	0	1
846	6	1	−2
111	7	−6	13
69	1	43	−93
42	1	−49	106
27	1	92	−199
15	1	−141	305
12	1	233	−504
3	4	−374	809

3.) In der letzten Zeile der Tabelle finden wir die Zahl $a_k = \mathrm{ggT}(a,b)$ sowie die Koeffizienten A und B. Für das obige Beispiel erhalten wir also:

$$3 = -374 \cdot 11220 + 809 \cdot 5187$$

Wir können nun eine wichtige Eigenschaft von Primzahlen beweisen.

Satz 6.8. *Sei p eine Primzahl, seien $a, b \in \mathbb{N}$ so, dass $p|ab$ gilt. Dann gilt $p|a$ oder $p|b$.*

Achtung: Dies schließt auch den Fall $p|a$ und $p|b$ ein. Es ist ein Unterschied, ob zwei Aussagen (hier „$p|a$“ sowie „$p|b$“) mit „oder“ verknüpft werden, oder mit „entweder oder“.

Beweis. Wir setzen $c := \mathrm{ggT}(a,p)$. Da p Primzahl ist, muss $c = 1$ oder $c = p$ gelten.

1.Fall: $c = p \Rightarrow p$ ist Teiler von $a \Rightarrow$ Satz bewiesen.

2.Fall: $c = 1$: Aus Satz 6.7 folgt dann, dass es $A, B \in \mathbb{Z}$ gibt mit $1 = Aa + Bp$. Wir multiplizieren diese Gleichung mit b und erhalten

$$b = Aab + Bpb.$$

Nach Voraussetzung gilt $p|ab$, also $p|Aab$ und natürlich haben wir $p|Bpb$. Daher folgt $p|(Aab + Bpb)$, also $p|b$. □

Korollar 6.9. *Sei p Primzahl, $a_1, \ldots, a_n \in \mathbb{N}$, dann gilt:*

$$p|a_1 \cdot \ldots \cdot a_n \quad \Rightarrow \quad \exists i \in \{1, \ldots, n\} : p|a_i$$

Beweis. Dies kann man einfach durch vollständige Induktion über n mit Hilfe von Satz 6.8 beweisen. □

Wir wollen jetzt einen der wichtigsten Sätze der Zahlentheorie beweisen. Es handelt sich um eine Präzisierung von Satz 5.10: Dieser Satz besagte, dass man jede natürliche Zahl als Produkt von Primzahlen darstellen kann. Wir betrachten zunächst ein Beispiel: Die Zahl 60 kann man auf verschiedene Arten als Produkt schreiben:

$$60 = 2 \cdot 30 = 6 \cdot 10 = 4 \cdot 15.$$

Falls man also allgemein eine Gleichheit

$$ab = m = cd$$

hat, wobei a, b, c, d beliebige natürliche Zahlen sind, dann kann man daraus nicht schlussfolgern, dass $a = c$, $b = d$ oder $a = d$, $b = c$ gilt. Der nächste Satz sagt, dass dies aber doch gilt, falls wir Zerlegungen in Produkte von Primzahlen betrachten.

Satz 6.10 (Fundamentalsatz der elementaren Zahlentheorie)**.** *Jede natürliche Zahl $n \in \mathbb{N}$ ist eindeutig (bis auf Reihenfolge) als Produkt von Primzahlen darstellbar.*

Beweis. Induktion nach n:

Induktionsanfang: Für $n = 1$ ist die Aussage offensichtlich richtig.

Induktionsvoraussetzung: Angenommen, die Aussage sei für alle Zahlen kleiner als n richtig.

Induktionsschritt: Seien Produktzerlegungen

$$n = p_1 \cdot \ldots \cdot p_k \qquad \text{und} \qquad n = q_1 \cdot \ldots \cdot q_l$$

gegeben, wobei $p_1, \ldots, p_k, q_1, \ldots, q_l$ Primzahlen sind und so, dass $1 < p_1 \leq p_2 \leq \ldots \leq p_k$ sowie $1 < q_1 \leq q_2 \leq \ldots \leq q_l$ gelte. Dann wollen wir beweisen, dass $k = l$ ist und, dass für alle $i \in \{1, \ldots, k\}$ die

Gleichheit $p_i = q_i$ gilt.

Aus $p_1 | p_1 \cdot \ldots \cdot p_k$ folgt $p_1 | n$, also $p_1 | q_1 \cdot \ldots \cdot q_l$. Wegen Korollar 6.9 folgt: $\exists i \in \{1, \ldots, l\}$ mit $p_1 | q_i$, aber da auch q_i eine Primzahl und $1 < p_1$ ist, gilt $p_1 = q_i$. Ganz analog kann man zeigen: $\exists j \in \{1, \ldots, k\} : p_j = q_1$. Wegen $p_1 \leq p_j = q_1 \leq q_i = p_1$ folgt dann, $p_1 = p_j = q_1 = q_i$ und damit können wir die Gleichung

$$p_1 \cdot \ldots \cdot p_k = q_1 \cdot \ldots \cdot q_l$$

durch $p_1 = q_1$ teilen und erhalten

$$\frac{n}{p_1} = p_2 \cdot \ldots \cdot p_k = q_2 \cdot \ldots \cdot q_l = \frac{n}{q_1}.$$

Wegen $1 < p_1 = q_1$ ist aber $\frac{n}{p_1} = \frac{n}{q_1} < n$ und damit lässt sich die Induktionsvoraussetzung auf $\frac{n}{p_1}$ anwenden: Die Zerlegung

$$\frac{n}{p_1} = p_2 \cdot \ldots \cdot p_k = q_2 \cdot \ldots \cdot q_l = \frac{n}{q_1}.$$

ist also eindeutig (da die Zahlen $p_2, \ldots, p_k$ und $q_2, \ldots, q_l$ der Größe nach angeordnet sind), also folgt $k = l$ und $p_i = q_i \, \forall i \in \{2, \ldots, k\}$. Da wir $p_1 = q_1$ schon gezeigt haben, ist der Beweis damit zu Ende. □

Definition 6.11. *Seien $a, b \in \mathbb{N}$, dann heißt die Zahl*

$$\mathrm{kgV}(a, b) \coloneqq \min \{c \in \mathbb{N} \mid a|c \text{ und } b|c\}$$

das kleinste gemeinsame Vielfache von a und b.

Korollar 6.12. *$\forall a, b \in \mathbb{N}$ gilt:*

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

Beweis. Wir benutzen Satz 6.10. Seien

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k} \qquad \text{und} \qquad b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k} \tag{6.2}$$

die eindeutigen Zerlegungen in Primfaktoren. Hierbei sind zwei Dinge zu beachten: In den Gleichungen (6.2) sollen die Zahlen $p_1, \ldots, p_k$ alle verschieden sein, möglicherweise mehrfach vorkommende Primzahlen werden mit Hilfe der Exponenten $\alpha_1, \ldots, \alpha_k$ bzw. $\beta_1, \ldots, \beta_k$ zusammengefasst. Andererseits können diese Exponenten auch gleich Null sein, da in den Zerlegungen von a und b natürlich nicht die gleichen Primfaktoren auftreten müssen. Wie man nun leicht sieht, muss gelten:

$$\mathrm{ggT}(a, b) = p_1^{\gamma_1} \cdot \ldots \cdot p_k^{\gamma_k},$$
$$\mathrm{kgV}(a, b) = p_1^{\delta_1} \cdot \ldots \cdot p_k^{\delta_k},$$

wobei $\gamma_i = \min(\alpha_i, \beta_i)$ und $\delta_i = \max(\alpha_i, \beta_i)$ ist. Also gilt

$$\mathrm{ggT}(a, b) \cdot \mathrm{kgV}(a, b) = p_1^{\gamma_1 + \delta_1} \cdot p_2^{\gamma_2 + \delta_2} \cdot \ldots \cdot p_k^{\gamma_k + \delta_k},$$

und wegen $\alpha_i + \beta_i = \min(\alpha_i, \beta_i) + \max(\alpha_i + \beta_i)$ folgt

$$\mathrm{ggT}(a, b) \cdot \mathrm{kgV}(a, b) = p_1^{\alpha_1 + \beta_1} \cdot p_2^{\alpha_2 + \beta_2} \cdot \ldots \cdot p_k^{\alpha_k + \beta_k} = a \cdot b.$$

□

Beispiel: $a = 45$, $b = 35$

$$\begin{array}{lllll} & 45 & = 5 \cdot 3 \cdot 3 & = 5^1 \cdot 3^2 \cdot 7^0 \\ & 35 & = 5 \cdot 7 & = 5^1 \cdot 3^0 \cdot 7^1 \\ \Rightarrow & \mathrm{ggT}(45, 35) & = 5^1 \cdot 3^0 \cdot 7^0 & = 5 \\ & \mathrm{kgV}(45, 35) & = 5^1 \cdot 3^2 \cdot 7^1 & = 315 \\ \Rightarrow & 45 \cdot 35 & = 5 \cdot 315 & = 1575 \end{array}$$

Kapitel 7

Kongruenzrechnung

Wir haben im letzten Kapitel schon den Begriff der Kongruenz zweier Zahlen eingeführt (Definition 6.2). Dies wollen wir etwas verallgemeinern:

Definition 7.1. *Seien $a, b \in \mathbb{Z}$ und $n \in \mathbb{N}$, dann heißt*

$$a \equiv b \mod n,$$

falls n ein Teiler von $a - b$ ist. Falls n kein Teiler von $a - b$ ist, schreibt man manchmal auch

$$a \not\equiv b \mod n.$$

Wir schreiben auch „(n)“ statt „ mod n“.

Beispiele:

$$\begin{aligned} 15 &\equiv 3 && \mod 12 \\ 365 &\equiv 1 && \mod 7 \quad (\text{denn } 52 \cdot 7 = 364) \\ -4 \equiv 3 \equiv 10 \equiv 17 &\equiv -11 && \mod 7 \\ 14328529 &\equiv 9 && \mod 10 \\ n \text{ gerade } &\Leftrightarrow n \equiv 0 && \mod 2 \\ n \text{ ungerade } &\Leftrightarrow n \equiv 1 && \mod 2 \end{aligned}$$

Lemma 7.2. *Für das Rechnen mit Kongruenzen gelten die folgenden Regeln:*

1.) $a \equiv a \quad (n)$

2.) $a \equiv b \quad (n) \Rightarrow b \equiv a \quad (n)$

3.) $a \equiv b \quad (n),\ b \equiv c \quad (n) \Rightarrow a \equiv c \quad (n)$

Diese 3 Eigenschaften fasst man zusammen, indem man sagt, dass „Kongruenz modulo n “ eine Äquivalenzrelation ist.

4.) Seien $a \equiv b \quad (n),\ c \equiv d \quad (n)$, *dann gilt:*

$$a + c \equiv b + d \quad (n) \text{ und } a \cdot c \equiv b \cdot d \quad (n)$$

Beweis. Die ersten 3 Eigenschaften sind sofort aus Definition 7.1 klar. Wir beweisen 4.):

$$a \equiv b \quad (n) \Rightarrow \exists k \in \mathbb{Z} : a = b + k \cdot n, \quad c \equiv d \quad (n) \Rightarrow \exists l \in \mathbb{Z} : c = d + l \cdot n.$$

Dann gilt:

$$a + c = b + d + (l + k) \cdot n \Rightarrow a + c \equiv b + d \quad (n).$$

Analog haben wir:

$$\begin{aligned} a \cdot c &= (b + k \cdot n) \cdot (d + l \cdot n) \\ &= bd + bl \cdot n + dk \cdot n + kl \cdot n^2 \\ &= bd + n(bl + dk + kln) \\ \Rightarrow ac &\equiv bd \qquad \mod n \end{aligned}$$

□

Bemerkung: Aus der Regel „$a \equiv b\ (n), c \equiv d\ (n) \Rightarrow ac \equiv bd\ (n)$“ kann man per vollständiger Induktion schlussfolgern:

$$a \equiv b \quad (n) \Rightarrow \forall m \in \mathbb{N} : a^m \equiv b^m \quad (n)$$

Beispiele:

1.)
$$11^2 = 121 = 12 \cdot 10 + 1 \Rightarrow 11^2 \equiv 1 \qquad \mod 12$$
Dies kann man schneller ausrechnen:
$$11 \equiv -1 \qquad \mod 12 \Rightarrow 11^2 \equiv (-1)^2 = 1 \qquad \mod 12$$
Genauso folgt auch $11^{36} \equiv (-1)^{36} = 1 \mod 12$.

2.)
$$13 \cdot 15 \equiv 1 \cdot 3 = 3 \quad (12)$$

3.) $135^4 \equiv ?\ (12)$:
$$135 = 120 + 12 + 3 \Rightarrow 135 \equiv 3 \quad (12)$$
$3^4 \equiv ?\ (12)$:
$$3^2 = 9 \equiv -3 \quad (12) \Rightarrow 3^4 = (3^2)^2 = 9^2 \equiv (-3)^2 = 9 \quad (12)$$
$\Rightarrow 135^4 \equiv 9 \quad (12)$.

4.) $10 \equiv 1 \quad (9) \Rightarrow \forall k \in \mathbb{N} : 10^k \equiv 1 \quad (9)$. Damit gilt für eine Zahl
$$\ldots + a_4 \cdot 10^4 + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \equiv \ldots + a_4 + a_3 + a_2 + a_1 + a_0 \qquad \mod 9,$$
also ist eine Zahl genau dann durch 9 teilbar, wenn ihre Quersumme (die Summe ihrer Ziffern) durch 9 teilbar ist. Bsp.:

18: Quersumme $1 + 8 = 9 \rightsquigarrow$ teilbar
28: Quersumme $2 + 8 = 10 \rightsquigarrow$ nicht teilbar
117: Quersumme $1 + 7 + 1 = 9 \rightsquigarrow$ teilbar $(171 = 9 \cdot 19)$

5.) Die Zahlen $2^{2^k} + 1$ scheinen für kleine alle k Primzahlen zu sein:

$k = 0$: $2^{2^0} + 1 = 2^1 + 1 = 2 + 1 = 3$
$k = 1$: $2^{2^1} + 1 = 2^2 + 1 = 4 + 1 = 5$
$k = 2$: $2^{2^2} + 1 = 2^4 + 1 = 16 + 1 = 17$
$k = 3$: $2^{2^3} + 1 = 2^8 + 1 = 256 + 1 = 257$ (ist Primzahl)

$k = 4$: $2^{2^4} + 1 = 2^{16} + 1 = 65536 + 1 = 65537$ (ist Primzahl)

aber: $k = 5$: $2^{2^5} + 1 = 2^{32} + 1 = 4294967297$

Euler:

$$64 = 2^6 \Rightarrow 641 = 10 \cdot 2^6 + 1$$

aber es gilt auch:

$$641 = 16 + 625 = 2^4 + 25 \cdot 25 = 2^4 + 5^4$$

Wir erhalten also:

$$10 \cdot 2^6 = 5 \cdot 2^7 \equiv -1 \qquad \text{mod } 641$$

$$\Rightarrow \quad 5^4 \cdot 2^{7 \cdot 4} = 5^4 \cdot 2^{28} \overset{(i)}{\equiv} 1 \qquad \text{mod } 641$$

$$\text{sowie} \quad 5^4 \overset{(ii)}{\equiv} -2^4 \qquad \text{mod } 641$$

Einsetzen der Kongruenzgleichung (ii) in die Gleichung (i):

$$-2^4 \cdot 2^{28} \equiv 1 \qquad \text{mod } 641$$

$$\Rightarrow \quad 2^{32} + 1 \equiv 0 \qquad \text{mod } 641$$

Damit ist also $2^{32} + 1 = 2^{2^5} + 1$ durch 641 teilbar, also keine Primzahl.

Wir wissen schon, dass die Zahl a^2 gerade bzw. ungerade ist, genau dann, wenn a gerade bzw. ungerade ist. Das kann man mit Kongruenzen so schreiben:

$$a^2 \equiv a \quad (2)$$

Der folgende berühmte Satz ist eine Verallgemeinerung davon:

Satz 7.3 (kleiner Satz von Fermat)**.** *Sei $p \in \mathbb{P}$ eine Primzahl, $a \in \mathbb{Z}$. Dann gilt stets:*

$$a^p \equiv a \qquad \text{mod } p$$

Beweis. Zuerst betrachten wir den Fall $a \in \mathbb{N}_0$. Hierfür führen wir einen Beweis mit vollständiger Induktion:

Induktionsanfang: $a = 0 \rightsquigarrow 0^p \equiv 0 \quad (p) \qquad \checkmark$

Induktionsvoraussetzung: Angenommen, es gelte $a^p \equiv a\ (p)$ für ein fest gewähltes $a \in \mathbb{N}_0$.

Induktionsschritt: Es ist nach der binomischen Formel (Korollar 5.8)

$$(a+1)^p = \sum_{k=0}^{p} \binom{p}{k} a^k.$$

Jetzt ist der Binomialkoeffizient $\binom{p}{k} = \frac{p!}{k! \cdot (p-k)!}$ für alle $k \in \{1, 2, \ldots, p-1\}$ durch p teilbar, also ist

$$(a+1)^p = \sum_{k=0}^{p} \binom{p}{k} a^k \equiv a^p + 1 \quad (p).$$

Nach Induktionsvoraussetzung ist $a^p \equiv a\ (p)$, also

$$(a+1)^p = \sum_{k=0}^{p} \binom{p}{k} a^k \equiv a^p + 1 \equiv a + 1 \quad (p).$$

Damit ist der Satz für $a \in \mathbb{N}_0$ bewiesen. Wegen $(-a)^p = (-1)^p a^p \equiv (-1)^p a \mod p$ gilt der Satz für alle $a \in \mathbb{Z}$. □

Beispiel: Wir wollen den Rest von 8^{308} bei Division durch 17 bestimmen (das ist direkt natürlich unmöglich). Wir haben

$$308 = 18 \cdot 17 + 2 = (17+1) \cdot 17 + 2 = 17^2 + 17 + 2.$$

Also ist

$$8^{308} = 8^{17^2} \cdot 8^{17} \cdot 8^2 \equiv ? \quad (17)$$

Der kleine Satz von Fermat (Satz 7.3) sagt:

$$\begin{aligned} & 8^{17} \equiv 8 && (17) \\ \Rightarrow \quad & 8^{17^2} = 8^{17 \cdot 17} = \left(8^{17}\right)^{17} \equiv 8^{17} \equiv 8 && (17) \\ \Rightarrow \quad & 8^{308} \equiv 8 \cdot 8 \cdot 8^2 = 8^2 \cdot 8^2 && (17) \end{aligned}$$

Jetzt ist $8^2 = 64 \equiv 13 \equiv -4\,(17)$, also:

$$8^{308} \equiv 8^2 \cdot 8^2 \equiv (-4) \cdot (-4) = 16 \quad (17)$$

Wir befassen uns jetzt mit der Frage der Lösbarkeit von Kongruenzsystemen (im Gegensatz zu Gleichungssystemen). Zunächst diskutieren wir eine Kongruenzversion des Dreisatzes.

Proposition 7.4. *Seien $a, b, n \in \mathbb{N}$, dann hat die Kongruenzgleichung*

$$a \cdot x \equiv b \quad (n) \tag{7.1}$$

genau dann eine Lösung, wenn gilt

$$\mathrm{ggT}(a,n) | b.$$

Falls x_1, x_2 Lösungen von (7.1) sind, dann gilt

$$x_1 \equiv x_2 \qquad \mathrm{mod}\ \overline{n},$$

wobei $\overline{n} := \frac{n}{\mathrm{ggT}(a,n)}$ ist. Man sagt, dass die Lösung der Gleichung (7.1) eindeutig modulo $\overline{n}$ ist.

Beweis. Angenommen, x sei eine Lösung von $ax \equiv b(n)$. Dann gilt also $ax = b + k \cdot n$ für ein $k \in \mathbb{Z}$. Natürlich gilt: $\mathrm{ggT}(a,n) | a \cdot x$ und $\mathrm{ggT}(a,n) | k \cdot n$, also bekommen wir: $\mathrm{ggT}(a,n) | b$.

Umgekehrt nehmen wir jetzt an, dass $\mathrm{ggT}(a,n) | b$ gilt, dann haben wir $d \cdot \mathrm{ggT}(a,n) = b$ für ein $d \in \mathbb{Z}$. Wegen Satz 6.7 (Darstellung des ggT) gibt es $A, B \in \mathbb{Z}$ mit $(Aa + Bn)d = b$, also $a \cdot A \cdot d = b - B \cdot d \cdot n$, dies bedeutet aber

$$a \cdot A \cdot d \equiv b \quad (n).$$

Damit ist die Zahl $x := A \cdot d$ eine Lösung der Kongruenzgleichung $ax \equiv b\,(n)$ und wir haben den ersten Teil der Proposition bewiesen.

Seien jetzt x_1 und x_2 Lösungen von (7.1), d. h.:

$$\exists k \in \mathbb{Z} : a \cdot (x_1 - x_2) = k \cdot n. \tag{7.2}$$

Sei wie in der Formulierung der Proposition jetzt $\overline{n} := \mathrm{ggT}(a,n)$, dann dividieren wir die Gleichung (7.2) durch $\mathrm{ggT}(a,n)$ und erhalten:

$$\overline{a} \cdot (x_1 - x_2) = k \cdot \overline{n}, \tag{7.3}$$

wobei $\overline{a} := \frac{a}{\mathrm{ggT}(a,n)}$. Es ist jetzt $\mathrm{ggT}(\overline{a}, \overline{n}) = 1$ und dann folgt aus Gleichung (7.3), dass $\overline{n} | x_1 - x_2$, d. h. $x_1 \equiv x_2\,(\overline{n})$. □

Wir erhalten die folgende Konsequenz, welche wir später noch benötigen:

Korollar 7.5.

1.) *Die Kongruenzgleichung*

$$ax \equiv 1 \quad (n)$$

hat genau dann eine Lösung, wenn $\mathrm{ggT}(a,n) = 1$ *gilt. Solch eine Zahl* x *heißt Inverses zu* a *modulo* n *und ist eindeutig modulo* n*.*

2.) *Sei* p *eine Primzahl (dann ist also* $\mathrm{ggT}(a,p) = 1$ *für alle ganzen Zahlen* a *mit* $a \not\equiv 0\,(p)$*). Dann existiert immer ein Inverses modulo* p*.*

3.) *Wenn wir das eindeutig bestimmte inverse Element zu* a *aus 1.) mit* a^{-1} *bezeichnen, dann können wir die Kongruenzgleichung* $ax \equiv b\,(n)$ *durch Multiplizieren mit* a^{-1} *lösen:*

$$a^{-1} \cdot a \cdot x \equiv a^{-1} \cdot b \quad (n) \quad \Rightarrow \quad x \equiv a^{-1} \cdot b \quad (n)$$

Wir betrachten einige Beispiele:

1.) Wir bestimmen die inversen Elemente modulo 7:

$$1 \cdot 1 \equiv 1\,(7),\ 2 \cdot 4 \equiv 1\,(7),\ 3 \cdot 5 \equiv 1\,(7),\ 4 \cdot 2 \equiv 1\,(7),\ 5 \cdot 3 \equiv 1\,(7),\ 6 \cdot 6 \equiv 1\,(7).$$

Dies könne wir in der folgenden Tabelle zusammenfassen:

a	1	2	3	4	5	6
a^{-1}	1	4	5	2	3	6

2.) Die Lösung der Kongruenzgleichung $3x \equiv 5\,(7)$ ist:

$$3^{-1} \cdot 3x \equiv x \equiv 3^{-1} \cdot 5 \equiv 5 \cdot 5 = 25 \equiv 4 \quad (7)$$

3.) Wir wollen die Gleichung $5x \equiv 16\,(101)$ lösen: Zuerst bestimmen wir 5^{-1} modulo 101: Da $101 = 5 \cdot 20 + 1$ ist, gilt

$$\begin{aligned} & 20 \cdot 5 \equiv -1 && (101) \\ \Rightarrow \quad & 20 \cdot 5 \cdot 5^{-1} \equiv -5^{-1} && (101) \\ \Rightarrow \quad & 5^{-1} \equiv -20 && (101) \end{aligned}$$

Dann folgt: $x \equiv -16 \cdot 20\,(101)$. Also ist

$$x \equiv -320 = -303 - 17 \equiv -17 \equiv 84 \quad (101)$$

4.) Wir wollen das Inverse von 30 modulo 101 bestimmen. Dies existiert nach Korollar 7.5 genau dann, wenn $\mathrm{ggT}(30, 101) = 1$ gilt. Dies überprüfen wir mit dem Euklidischen Algorithmus:

$$\begin{aligned} 101 &= 3 \cdot 30 + 11 \\ 30 &= 2 \cdot 11 + 8 \\ 11 &= 1 \cdot 8 + 3 \\ 8 &= 2 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 \end{aligned}$$

Also existiert 30^{-1} modulo 101. Um dieses Inverse wirklich zu bestimmen, benutzen wir Satz 6.7, d. h.die Darstellung von $1 = \mathrm{ggT}(101, 30)$ als Linearkombination $1 = A \cdot 101 + B \cdot 30$. Wir führen wieder „Rückeinsetzen“ im Gleichungssystem oben durch:

$$\begin{aligned}
1 &= 3 - 1 \cdot 2 \\
&= (11 - 1 \cdot 8) - (8 - 2 \cdot 3) && = 11 - 2 \cdot 8 + 2 \cdot 3 \\
&= 11 - 2 \cdot 8 + 2 \cdot (11 - 1 \cdot 8) \\
&= 3 \cdot 11 - 4 \cdot 8 \\
&= 3 \cdot 11 - 4 \cdot (30 - 2 \cdot 11) \\
&= 11 \cdot 11 - 4 \cdot 30 \\
&= 11 \cdot (101 - 3 \cdot 30) - 4 \cdot 30 \\
&= \underbrace{11}_{=A} \cdot 101 \underbrace{-37}_{=B} \cdot 30
\end{aligned}$$

Tatsächlich ist $11 \cdot 101 = 1111$ und $37 \cdot 30 = 1110$, also $11 \cdot 101 - 37 \cdot 30 = 1$. Damit erhalten wir

$$\begin{aligned}
(11 \cdot 101 - 37 \cdot 30) \cdot 30^{-1} &\equiv 30^{-1} \quad (101) \\
11 \cdot 101 \cdot 30^{-1} - 37 \cdot 30 \cdot 30^{-1} &\equiv 30^{-1} \quad (101) \\
-37 &\equiv 30^{-1} \quad (101)
\end{aligned}$$

Also ist -37 ($\equiv 64 \ \ (101)$) das Inverse von 30 modulo 101.

Wir wollen als nächstes einen wichtigen Satz der Zahlentheorie, den sogenannten Chinesischen Restsatz, behandeln. Dieser hat eine große Bedeutung zum Verständnis von periodisch wiederkehrenden Phänomenen. Wir betrachten zunächst ein Beispiel: Eine Mondphase dauert 29 Tage. Wir nehmen an, dass an einem bestimmten Sonntag Neumond ist. In wievielen Tagen fällt dann der Vollmond auf einen Dienstag? Wenn wir die gesuchte Anzahl von Tagen mit x bezeichnen, dann können wir dieses Problem als ein System von Kongruenzgleichungen formulieren:

Zuerst nummerieren wir die Wochentage (1 = Montag, ..., 7 = Sonntag), dann muss $x \equiv 2\ (7)$ gelten, da der gesuchte Tag auf einen Dienstag fallen soll. Wenn wir andererseits die Tage einer Mondphase von 0 bis 28 nummerieren (0 = Neumond,...), dann fällt der Vollmond auf den 15. Tag, also muss auch gelten: $x \equiv 15\ (29)$. Wir haben also das System

$$\begin{aligned}
x &\equiv 2 \quad (7) \\
x &\equiv 15 \quad (29)
\end{aligned}$$

Durch Probieren findet man, dass z. B. $x = 44$ eine Lösung ist. Solche Situationen wollen wir jetzt im Allgemeinen studieren.

Satz 7.6 (Chinesischer Restsatz)**.** *Seien $m_1, \ldots, m_n \in \mathbb{N}$, so dass $\mathrm{ggT}(m_i, m_j) = 1$ gilt $\forall i, j \in \{1, \ldots, n\}$ mit $i \neq j$. Seien weiterhin $a_1, \ldots, a_n \in \mathbb{Z}$. Dann hat das Kongruenzsystem*

$$\begin{aligned}
x &\equiv a_1 \quad \mod m_1 \\
x &\equiv a_2 \quad \mod m_2 \\
&\vdots \\
x &\equiv a_n \quad \mod m_n
\end{aligned} \tag{7.4}$$

eine eindeutige Lösung x aus der Menge

$$\{0, 1, \ldots, m_1 \cdot m_2 \cdot \ldots \cdot m_n - 1\}$$

Jede weitere Lösung $x' \in \mathbb{Z}$ des Systems (7.4) erfüllt dann:

$$x' \equiv x \qquad \mod m_1 \cdot \ldots \cdot m_n$$

Der Beweis zeigt uns auch, wie wir x bestimmen können.

Beweis. Wir setzen $M \coloneqq m_1 \cdot \ldots \cdot m_n$, sowie $M_i \coloneqq \frac{M}{m_i}$. Dann ist $M_i \in \mathbb{N}$ und es gilt $\mathrm{ggT}(M_i, m_i) = 1$ (wegen $\mathrm{ggT}(m_i, m_j) = 1 \, \forall i \neq j$). Aus Korollar 7.5 folgt dann, dass die Kongruenzen

$$M_i \cdot b_i \equiv 1 \qquad \mod m_i$$

Lösungen $b_i \in \mathbb{N}$ haben, für alle $i \in \{1, \ldots, n\}$. Dann definieren wir $E_i \coloneqq M_i \cdot b_i \, \forall i \in \{1, \ldots, n\}$, es folgt:

$$E_i \equiv \begin{cases} 1 & \mod m_i \\ 0 & \mod m_j \, \forall j \neq i \end{cases}$$

Wenn wir dann noch $x \coloneqq a_1 \cdot E_1 + \ldots + a_n \cdot E_n$ setzen, dann folgt

$$x \equiv a_i \qquad \mod m_i,$$

also ist x eine Lösung des Systems (7.4). A priori ist $x \in \mathbb{N}$ und wir müssen noch beweisen, dass es eine (eindeutige) Lösung $x \in \{0, \ldots, M-1\}$ gibt. Nehmen wir zunächst an, es gäbe noch eine Lösung x' des Systems (7.4). Dann gilt also $\forall i \in \{1, \ldots, n\}$: $x \equiv a_i \, (m_i)$ und $x' \equiv a_i \, (m_i)$. Hieraus folgt $x - x' \equiv 0 \, (m_i)$, d. h. $m_i | x - x'$. Da dies für alle $i \in \{1, \ldots, n\}$ gilt, folgt auch $M | x - x'$, d. h. $x \equiv x' \, (M)$. Andersherum ist für jedes $k \in \mathbb{Z}$ die Zahl $x + k \cdot M$ eine lösung von (7.4), wenn x eine Lösung ist. Also gibt es genau eine Lösung x des Systems (7.4) aus dem Bereich $\{0, 1, \ldots, M-1\}$. □

Beispiel: Wir suchen eine Lösung x des Systems

$$\begin{aligned} x &\equiv 1 \quad (5) \\ x &\equiv 2 \quad (7) \\ x &\equiv 3 \quad (11) \end{aligned} \tag{7.5}$$

Es ist also $M = 5 \cdot 7 \cdot 11 = 35 \cdot 11 = 385$, $M_1 = \frac{285}{5} = 7 \cdot 11 = 77$, $M_2 = \frac{385}{7} = 5 \cdot 11 = 55$ sowie $M_3 = \frac{385}{11} = 5 \cdot 7 = 35$. Wir haben also die Gleichungen

$$\begin{aligned} 77 b_1 \equiv 2 b_1 &\overset{!}{\equiv} 1 \quad (5) \qquad \Rightarrow b_1 \equiv 3 \quad (5) \\ 55 b_2 \equiv 6 b_1 &\overset{!}{\equiv} 1 \quad (7) \qquad \Rightarrow b_2 \equiv 6 \quad (7) \\ 35 b_3 \equiv 2 b_3 &\overset{!}{\equiv} 1 \quad (11) \qquad \Rightarrow b_3 \equiv 6 \quad (11) \end{aligned}$$

Wir setzen also $E_1 \coloneqq 77 \cdot 3 = 231$, $E_2 \coloneqq 55 \cdot 6 = 330$, $E_3 \coloneqq 35 \cdot 6 = 210$. Dann ist

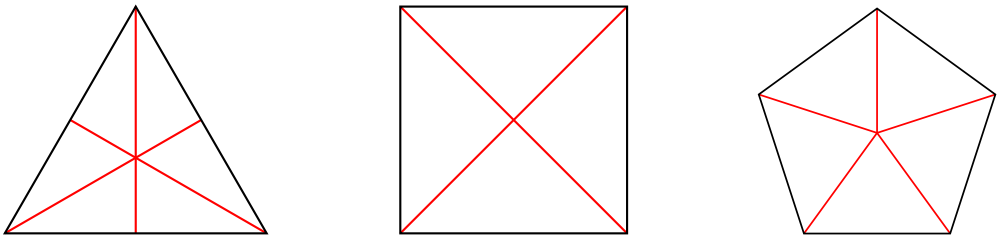
$$\begin{aligned} x &= E_1 \cdot a_1 + E_2 \cdot a_2 + E_3 \cdot a_3 \\ &= 231 \cdot 1 + 330 \cdot 2 + 210 \cdot 3 \equiv 231 + 275 + 245 = 231 + 520 \equiv 231 + 135 = 366 \quad (385) \end{aligned}$$

Also ist 366 die eindeutige Lösung von (7.5) in $\{0, 1, \ldots, 384\}$.

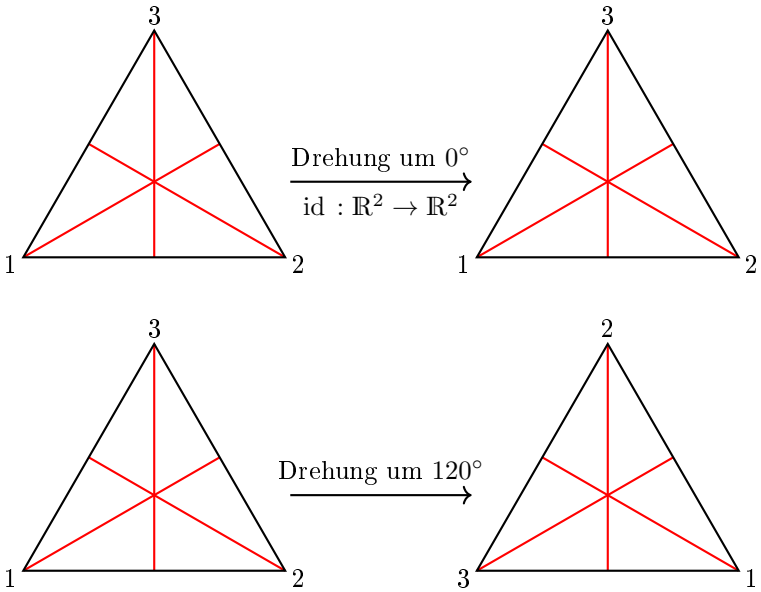
Kapitel 8

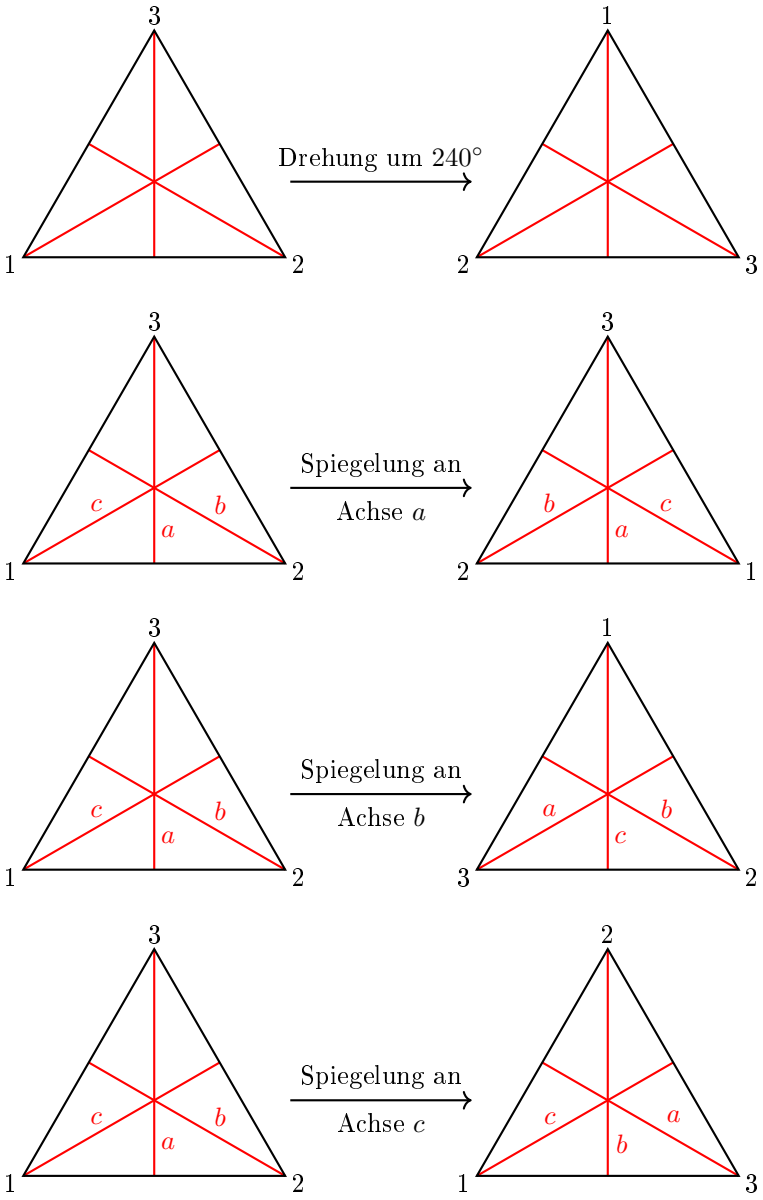
Gruppentheorie

In diesem Kapitel wollen wir ein ganz grundlegendes Konzept der Mathematik kennenlernen, nämlich den Begriff einer Gruppe. Wir beginnen mit einem Beispiel:
Sei eine geometrische Figur in der Ebene ($\widehat{=}\mathbb{R}^2$) vorgegeben, z. B. ein regelmäßiges 3-Eck, 4-Eck, 5-Eck, ..., n-Eck,



oder aber eine kompliziertere Figur wie ein Schneekristall. Man möchte jetzt verstehen, welche Transformationen der Ebene (d. h., welche Bijektionen $\mathbb{R}^2 \to \mathbb{R}^2$) solch eine Figur fest lassen, also in sich selbst überführen. Für das Dreieck gibt es 6 solcher Transformationen, nämlich Drehungen um 0° (das ist die Abbildung $\mathrm{id} : \mathbb{R}^2 \to \mathbb{R}^2$), um 120° und um 240°, sowie die Spiegelungen an den Mittelsenkrechten. Konkreter:





Transformationen, welches ein geometrisches Gebilde in sich selbst überführen, nennen wir Symmetrien. Das regelmäßige ($\widehat{=}$ gleichseitige) Dreieck hat also 6 Symmetrien. Analog hat das Quadrat 8 Symmetrien. Allgemeiner hat das regelmäßige n-Eck $2 \cdot n$ Symmetrien. Man sieht auch, dass die Symmetrien des 6-Ecks genau die des Schneekristalls sind: Drehungen um Vielfache von 60° sowie 6 Spiegelungen. Anschaulich gelten folgende Regeln für diese Symmetrien:

1.) Die Identitätsabbildung ist eine Symmetrie.

2.) Das Hintereinanderausführen von zwei Symmetrien ist wieder eine Symmetrie.

3.) Zu jeder Symmetrie gibt es eine Inverse: Dies ist eine weitere Symmetrie mit der Eigenschaft, dass das Hintereinanderausführen der beiden die Identität ist.

Mathematisch kann man diese Regeln so formulieren, dass die Menge der Symmetrien eines geometrischen Objekts eine Gruppe bildet. Den Gruppenbegriff behandeln wir jetzt.

Definition 8.1. *Sei M eine beliebige, aber nichtleere Menge. Eine Verknüpfung auf M ist eine Abbildung*

$$M \times M \to M.$$

Bezeichnet man diese Abbildung z. B. mit $*$, dann würde man also $c := *(a,b)$ schreiben, wenn die Abbildung das Paar $(a,b) \in M \times M$ auf das Element $c \in M$ abbildet. Man benutzt aber fast immer die viel natürlichere Schreibweise $c := a * b$, weil diese an die üblichen Verknüpfungen (Addition, Multiplikation) erinnert. Eine Menge M mit Verknüpfung $*$ heißt Gruppe, falls folgende Axiome gelten:

G1) $\forall x,y,z \in M : x*(y*z) = (x*y)*z$ *(Assoziativgesetz)*

G2) $\exists e \in M : \forall x \in M : e*x = x*e = x$ *(neutrales Element)*

G3) $\forall x \in M : \exists y \in M : x*y = y*x = e$ *(inverses Element)*

Falls zusätzlich noch gilt:

G4) $\forall x,y \in M : x*y = y*x$ *(Kommutativgesetz)*

dann sagt man, dass M mit der Verknüpfung $*$ eine abelsche Gruppe ist (nach dem Mathematiker Niels Henrik Abel).

Wir schreiben häufig $(M,*)$ für die Gruppe M mit der Verknüpfung $*$. Beispiele für Verknüpfungen und Gruppen:

1.) Sei $M = \mathbb{N}_0$ und $* = +$: Dies ist eine Verknüpfung, aber keine Gruppe: es gelten G1, G2 (mit $e = 0$) und sogar G4, aber nicht G3.

2.) $M = \mathbb{Z}, * = +$: Dies ist eine (sogar abelsche) Gruppe.

3.) $M = \mathbb{Z} \setminus \{0\}, * = \cdot$: Dies ist wieder eine Verknüpfung, aber keine Gruppe: Es gilt G1, G2 ($e = 1$), G4, aber nicht G3 (außer 1 und -1 hat kein Element ein Inverses).

4.) $(\mathbb{Q},+)$ sowie $(\mathbb{Q} \setminus \{0\}, \cdot)$: Dies sind beides abelsche Gruppen, es gelten G1 bis G4.

Das letzte Beispiel kann man verallgemeinern. Zur Erinnerung: Wir hatten in Kapitel 3 den Begriff des Körpers definiert als eine Menge K mit zwei Verknüpfungen $+$ und $\cdot$ (welche wir dort „Rechenoperationen“ genannt hatten), welche die Axiome A1 bis A4, M1 bis M4 sowie D erfüllen. Man sieht durch Vergleich dieser Axiome mit Definition 8.1, dass folgendes gilt.

Lemma 8.2. *Sei $(K,+,\cdot)$ ein Körper (entsprechend Definition 3.1). Dann sind K mit der Verknüpfung $+$ sowie $K \setminus \{0\}$ mit der Verknüpfung $\cdot$ abelsche Gruppen (hierbei ist 0 das neutrale Element bezüglich der Verknüpfung $+$ und 1 das neutrale Element bezüglich der Verknüpfung $\cdot$).*

Die endlichen Körper $\mathbb{F}_p$ (p Primzahl) liefern also Beispiele für Gruppen, z. B. $(\{0,1\},+)$, $(\{0,1,2\},+)$. Allgemein kann man endliche Gruppen durch eine Verknüpfungstabelle beschreiben:

für $(\{0,1\},+)$:

$+$	0	1
0	0	1
1	1	0

für $(\{0,1,2\},+)$:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Ein weiteres Beispiel für Gruppen haben wir (implizit) in Kapitel 4 kennengelernt:

Wir hatten mit $S^1 := \{z \in \mathbb{C} : |z| = 1\}$ die komplexen Zahlen der Länge 1 bezeichnet. Betrachtet man die Multiplikation komplexer Zahlen als Verknüpfung auf S^1, dann gelten G1, G2 und G3. Analog ist die Menge $\mu_n := \{z \in S^1 : z^n = 1\}$ der n-ten Einheitswurzeln eine endliche Gruppe, wobei wieder $\cdot$ die Verknüpfung ist. Offensichtlich ist $\mu_n \subset S^1$ und $S^1 \subset \mathbb{C} \setminus \{0\}$ (Erinnerung: $(\mathbb{C} \setminus \{0\})$ ist eine Gruppe), wobei jedes Mal die Teilmenge eine Gruppe mit der gleichen Verknüpfung wie die größere Gruppe ist. Dies führt uns zu folgendem Begriff:

Definition 8.3. *Sei $(G, *)$ eine Gruppe und sei $U \subset G$ eine Teilmenge, $U \neq \varnothing$. Dann heißt U (zusammen mit der Verknüpfung $*$) eine Untergruppe von $(G, *)$, falls gilt:*

U1) $e \in U$ *(Erinnerung: e ist das neutrale Element von G)*

U2) $\forall x, y \in U : x * y \in U$

U3) $\forall x \in U : x^{-1} \in U$ *(x^{-1} bezeichnet das Inverse Element zu x in G, welches nach G3 existiert, Übung: es ist sogar eindeutig)*

Aus dieser Definition folgt sofort:

Lemma 8.4. *Sei $(G, *)$ eine Gruppe und $U \subset G$ eine Untergruppe. Dann ist $(U, *)$ auch eine Gruppe.*

Beweis. Wegen dem Axiom U2 definiert $*$ eine Verknüpfung $U \times U \to U$ (anders gesagt: Wenn man in die Verknüpfung $*$ zwei Elemente aus U hineingibt, kommt auch ein Element aus U heraus). Wir müssen G1, G2 und G3 nachprüfen: G1 gilt, weil es schon in der Gruppe G gilt. G2 folgt aus dem Axiom U1 und G3 aus dem Axiom U3. □

Beispiele für Untergruppen:
$(\mathbb{Z}, +) \subset (\mathbb{Q}, +)$, $(\mathbb{Q}, +) \subset (\mathbb{R}, +)$, $(\mathbb{R}, +) \subset (\mathbb{C}, +)$,
$(\mathbb{Q} \setminus \{0\}, \cdot) \subset (\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot) \subset (\mathbb{C} \setminus \{0\}, \cdot)$,
$(\mu_n, \cdot) \subset (S^1, \cdot) \subset (\mathbb{C} \setminus \{0\}, \cdot)$

Wir wollen nun ein Beispiel für nicht-abelsche Gruppen kennenlernen, nämlich die Permutationsgruppen. Permutation bedeutet „Umordnung“, falls z. B. eine Menge $\{a, b, c, d\}$ anders angeordnet wird (z. B. c,b,d,a), dann liefert dies eine Abbildung $a \mapsto c$, $b \mapsto b, c \mapsto d$, $d \mapsto a$. So eine Abbildung ist genau ein Element der Permutationsgruppe. Wir geben nun eine formale Definition von Permutationen.

Definition 8.5.

- *Sei M eine beliebige Menge, dann nennen wir jede bijektive Abbildung $\sigma : M \to M$ (d. h. σ ist injektiv und surjektiv, insbesondere existiert eine Umkehrabbildung $\sigma^{-1} : M \to M$) eine Permutation.*
- *Die Menge der Permutationen von M wird mit $S(M)$ bezeichnet.*
- *Sind $\sigma, \tau \in S(M)$ (also σ und τ sind bijektive Abbildungen $M \to M$), dann kann man die Hintereinanderausführung oder Komposition (siehe Definition 2.9) $\sigma \circ \tau$ (oder auch $\tau \circ \sigma$) betrachten, dies ist wieder eine Permutation (d. h. bijektiv). Man beachte: $\sigma \circ \tau$ ist im Allgemeinen nicht gleich zu $\tau \circ \sigma$.*

Wir können nun die Permutationsgruppe konstruieren.

Satz 8.6. *Sei M eine Menge und $S(M)$ die Menge der Permutationen von M. Dann ist $S(M)$ mit der Verknüpfung $\circ$ (Komposition von Abbildungen) eine Gruppe, welche im Allgemeinen nicht abelsch ist.*

Beweis. Wir haben schon erklärt, dass $\circ$ eine Verknüpfung auf $S(M)$ ist. Wir müssen die Axiome G1, G2 und G3 überprüfen:

G1: Seien $\sigma, \tau, \varepsilon \in S(M), x \in M$, dann gilt:

$$((\sigma \circ \tau) \circ \varepsilon)(x) = (\sigma \circ \tau)(\varepsilon(x)) = \sigma(\tau(\varepsilon(x))) = \sigma((\tau \circ \varepsilon)(x)) = \sigma \circ (\tau \circ \varepsilon)(x)$$

Da dies für alle $x \in M$ gilt, folgt $(\sigma \circ \tau) \circ \varepsilon = \sigma \circ (\tau \circ \varepsilon)$.

G2: Sei $e \coloneqq \mathrm{id}_M \in S(M)$, dann gilt:

$$\sigma \circ e = e \circ \sigma = \sigma$$

Also ist e das neutrale Element.

G3: Sei $\sigma \in S(M)$, da σ eine Bijektion ist, existiert eine Umkehrabbildung $\sigma^{-1} : M \to M$ und $\sigma^{-1} \in S(M)$. Es folgt:

$$\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = id_M$$

□

Besonders wichtig ist der Fall $M = \{1, 2, \ldots, n\}$, dann setzen wir $S_n := S(M)$ und nennen S_n die symmetrische Gruppe. Ein Element $\sigma \in S_n$ kann man wie folgt schreiben:

$$\begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ a_1 & a_2 & a_3 & \ldots & a_n \end{pmatrix},$$

wobei $a_i \in \{1, \ldots, n\}$ und zwar so, dass jede Zahl genau einmal vorkommt. Es ist dann $a_i = \sigma(i)$ und dadurch ist die Abbildung $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$ eindeutig festgelegt und bijektiv.

Beispiele für symmetrische Gruppen:

- $S_1 = \{\mathrm{id}_{\{1\}}\}$
- $S_2 = \{\mathrm{id}_{\{1,2\}}, \tau\}$ mit

$$\mathrm{id}_{\{1,2\}} = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \text{ und } \tau = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}.$$

- $S_3 = \{\mathrm{id}_{\{1,2,3\}}, \tau_{12}, \tau_{23}, \tau_{13}, \alpha, \beta\}$ mit

$$\tau_{12} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \tau_{23} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \tau_{13} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

- Die Verknüpfungstabelle für S_2:

$\circ$	id	τ
id	id	τ
τ	τ	id

denn $\tau \circ \tau = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = \mathrm{id}$.

Übung: Berechne Verknüpfungstabelle für S_3. Achtung: nicht-abelsch, z. B. $\tau_{12} \circ \tau_{23} \neq \tau_{23} \circ \tau_{12}$.

Lemma 8.7. *Die Gruppe S_n hat $n!$ Elemente.*

Beweis. Wir haben schon in Kapitel 5 gesehen, dass es genau $n!$ Möglichkeiten gibt, n verschiedene Zahlen anzuordnen. Jede solche Anordnung definiert eine Bijektion $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$, also ein Element $\sigma \in S_n$. □

Besonders wichtig sind spezielle Permutationen, die sogenannten Zykeln. Hierbei werden einige Zahlen aus $\{1, \ldots, n\}$ einfach „zyklisch gedreht“, alle anderen fest gelassen. Beispiele sind die Permutationen $\alpha \in S_3$ (hier werden alle drei Elemente zyklisch permutiert), oder auch $\tau_{12} \in S_3$ (3 wird fest gelassen, 1 und 2 werden zyklisch permutiert) und analog $\tau_{13}, \tau_{23} \in S_3$. Formal definiert man Zykeln folgendermaßen:

Definition 8.8. *Seien $n_1, \ldots, n_k \in \{1, \ldots, n\}$ k verschiedene Zahlen, wobei $k \geq 2$ ist. Betrachte die folgende Permutation aus S_n:*

$$\{1, \ldots, n\} \to \{1, \ldots, n\}$$
$$a \mapsto \begin{cases} n_{i+1}, & \text{falls } a = n_i \text{ für ein } i \in \{1, \ldots, k-1\} \text{ ist} \\ n_1, & \text{falls } a = n_k \text{ ist} \\ a, & \text{falls } a \notin \{n_1, \ldots, n_k\} \text{ ist} \end{cases}$$

Wir bezeichnen diese Permutation mit $(n_1\ n_2\ \ldots\ n_k)$ (Schreibweise ohne Komma). Sie heißt Zykel oder zyklische Permutation der Länge k.

Zwei Zykel $(n_1\ n_2\ \ldots\ n_k)$ und $(m_1\ m_2\ \ldots\ m_l)$ heißen disjunkt, falls gilt $\{n_1, \ldots, n_k\} \cap \{m_1, \ldots, m_l\} = \varnothing$. Beachte: Falls $\{n_1, \ldots, n_k\} \cap \{m_1, \ldots, m_l\} = \varnothing \Rightarrow (n_1\ \ldots\ n_k) \circ (m_1\ \ldots\ m_l) = (m_1\ \ldots\ m_l) \circ (n_1\ \ldots\ n_k)$.

Beispiele für Zykeln:

- $\forall n:$ $\mathrm{id}_{\{1,\ldots,n\}}$ ist Zykel, geschrieben (1) (oder auch (a) für beliebiges $a \in \{1, \ldots, n\}$).
- $S_2 : \tau = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ ist Zykel, nämlich $\tau = (1\,2) = (2\,1)$.
- S_3 :

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\,2\,3) = (2\,3\,1) = (3\,1\,2)$$
$$\beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\,3\,2) = (3\,2\,1) = (2\,1\,3)$$
$$\tau_{12} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1\,2) = (2\,1)$$
$$\tau_{13} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1\,3) = (3\,1)$$
$$\tau_{23} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2\,3) = (3\,2)$$

Ist jede Permutation ein Zykel? Nein, z. B. ist $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (1\,2) \circ (3\,4)$ ein Produkt zweier Zykeln, aber selbst kein Zykel. Eine solche Zerlegung in Produkte kann man immer durch führen, es gilt der folgende wichtige Satz (hier ohne Beweis):

Satz 8.9. *Jede Permutation $\sigma \in S_n$ lässt sich als Produkt $\sigma = \sigma_1 \circ \ldots \circ \sigma_k$ schreiben, wobei $\sigma_1, \ldots, \sigma_k$ Zykeln sind, welche paarweise disjunkt sind (also σ_i und σ_j sind disjunkt, falls $i \neq j$).*

Statt des Beweises geben wir hier einen Algorithmus an, mit welchem man die Zerlegung in ein Produkt von Zykeln bestimmen kann. Gegeben sei eine Permutation $\sigma = \begin{pmatrix} 1 & \ldots & n \\ a_1 & \ldots & a_n \end{pmatrix} \in S_n$. Die Zahl 1 wird auf a_1 abgebildet, und wir nehmen hier an, dass $a_1 \neq 1$ ist. Ist dies nicht der Fall, startet man statt mit 1 mit 2 etc. Gilt für alle i, dass $\sigma(i) = i$ ist, dann ist $\sigma = \mathrm{id}_{S_n}$ und dies ist natürlich ein Zykel. Wir können also $a_1 \neq 1$ annehmen. Man sucht dann (in der ersten Zeile) die Zahl a_1, diese wird auf eine Zahl a_m abgebildet, man sucht wieder in der ersten Zeile die Zahl a_m, diese wird auf a_l abgebildet etc. Irgendwann findet man eine Zahl a_r in der ersten Zeile, welche auf 1 abgebildet wird. Es gilt dann

$$\sigma = \begin{pmatrix} 1 & \ldots & n \\ a_1 & \ldots & a_n \end{pmatrix} \overset{!}{=} \tau \circ (1\ a_1\ a_m\ a_l\ \ldots\ a_r),$$

wobei τ ein gewisses anderes Element aus S_n ist. Genauer gilt: Falls alle Zahlen von 1 bis n unter den Zahlen $1, a_1, a_m, a_l, \ldots, a_r$ vorkommen, dann ist $\tau = \mathrm{id}$ und die gegebene Permutation σ ist schon selbst ein Zykel. Falls nicht, dann gilt also $\{1, \ldots, n\} = \underbrace{\{1, a_1, a_m, a_l, \ldots, a_r\}}_{t \text{ Zahlen}} \cup \{b_1, \ldots, b_s\}$ (mit $t + s = n$) und danach führt man den gleichen Prozess, startend mit b_1, fort, d. h., man zerlegt die Permutation τ in ein Produkt aus Zykeln. Dies liefert dann die gewünschte Zerlegung von σ.

Beispiele zur Zyklenzerlegung:

1.) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 1 & 4 & 2 & 6 \end{pmatrix} \in S_6$

Es gilt: $1 \mapsto 3 \mapsto 1 \quad \Rightarrow \quad \sigma = \tau \circ (1\,3)$ mit $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 3 & 4 & 2 & 6 \end{pmatrix}$.

Es gilt: $2 \mapsto 5 \mapsto 2 \quad \Rightarrow \quad \sigma = \tau' \circ (2\,5) \circ (1\,3)$ mit $\tau' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \mathrm{id}$.

Also $\sigma = (2\,5)(1\,3)$.

2.) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 4 & 1 \end{pmatrix} \in S_5$

$1 \mapsto 2 \mapsto 3 \mapsto 5 \mapsto 1 \quad \Rightarrow \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} \circ (1\,2\,3\,5)$

$\Rightarrow \quad \sigma = (1\,2\,3\,5)$

3.) Sei $\sigma = (8\,7\,6\,5\,4) \circ (3\,2\,1) \circ (7\,5\,3\,1) \in S_8$. σ ist also ein Produkt von Zykeln, aber diese sind nicht disjunkt. Wir berechnen zunächst die Standarddarstellung von $\sigma = \begin{pmatrix} 1 & 2 & \ldots & 8 \\ a_1 & a_2 & \ldots & a_8 \end{pmatrix}$. Sei $\sigma = \sigma_1 \circ \sigma_2 \circ \sigma_3$ mit $\sigma_1 = (8\,7\,6\,5\,4)$, $\sigma_2 = (3\,2\,1)$, $\sigma_3 = (7\,5\,3\,1)$, dann gilt

$\sigma(1) = \sigma_1(\sigma_2(\sigma_3(1))) = \sigma_1(\sigma_2(7)) = \sigma_1(7) = 6.$
$\sigma(2) = \sigma_1(\sigma_2(\sigma_3(2))) = \sigma_1(\sigma_2(2)) = \sigma_1(1) = 1.$
$\sigma(3) = \sigma_1(\sigma_2(\sigma_3(3))) = \sigma_1(\sigma_2(1)) = \sigma_1(3) = 3.$
$\sigma(4) = \ldots = 8.$ $\sigma(5) = \ldots = 2.$
$\sigma(6) = \ldots = 5.$ $\sigma(7) = \ldots = 4.$
$\sigma(8) = \ldots = 7.$

Damit gilt also: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 1 & 3 & 8 & 2 & 5 & 4 & 7 \end{pmatrix}$. Jetzt zerlegen wir σ wie vorher:

$1 \mapsto 6 \mapsto 5 \mapsto 2 \mapsto 1, \quad 3 \mapsto 3, \quad 4 \mapsto 8 \mapsto 7 \mapsto 4$, also gilt $\sigma = (1\,6\,5\,2) \circ (4\,8\,7)$.

Möchte man Gruppen vergleichen, so betrachtet man spezielle Abbildungen zwischen ihnen, die sogenannten Homomorphismen.

Definition 8.10. *Seien $(G, *)$ und $(H, \circ)$ zwei Gruppen und $f : G \to H$ eine beliebige Abbildung. Dann heißt f ein Gruppenhomomorphismus, falls für alle Elemente $x, y \in G$ gilt, dass*

$$f(x * x) = f(x) \circ f(y)$$

ist. Wir schreiben dann

$$f : (G, *) \longrightarrow (H, \circ).$$

Beispiele:

- Sei $G = \mathbb{Z}, * = +, H = \mathbb{Q}, \circ = +$ und die Abbildung $f : \mathbb{Z} \to \mathbb{Q}$ einfach definiert durch $f(n) = n$, d. h.man benutzt einfach, dass eine ganze Zahl auch eine rationale Zahl ist. Dann ist $f : (\mathbb{Z}, +) \to (\mathbb{Q}, +)$ ein Gruppenhomomorphismus.
- Analog erhält man Gruppenhomomorphismen $(\mathbb{Q}, +) \to (\mathbb{R}, +)$, $(\mathbb{R}, +) \to (\mathbb{C}, +)$, $(\mathbb{Z}, +) \to (\mathbb{R}, +)$ etc.
- Ein interessanteres Beispiel: Sei $a \in \mathbb{R}_{>0}$ und die Potenzfunktion $\mathbb{R} \to \mathbb{R}, x \mapsto a^x$ gegeben. Klar ist, dass $a^x > 0$ ist $\forall x \in \mathbb{R}$, d. h., wir können diese Funktion als Abbildung

$$\begin{aligned} f : \mathbb{R} &\to \mathbb{R}_{>0} \\ x &\mapsto a^x \end{aligned}$$

schreiben. Es gilt das Exponentialgesetz: $a^{x+y} = a^x \cdot a^y \; \forall x, y \in \mathbb{R}$. Dies heißt nichts anderes, als dass f ein Gruppenhomomorphismus $f : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot)$ ist.

Definition-Lemma 8.11. *Sei $f : (G, *) \to (H, \circ)$ ein Gruppenhomomorphismus und e_H das neutrale Element von $(H, \circ)$. Dann definieren wir*

$$\begin{aligned} \ker(f) &:= \{x \in G \mid f(x) = e_H\} && \textit{(Kern von } f\textit{)} \\ \operatorname{im}(f) &:= \{z \in H \mid \exists x \in G, f(x) = z\} && \textit{(Bild von } f\textit{)} \end{aligned}$$

Man beachte, dass $\operatorname{im}(f)$ nichts anderes als das schon in Kapitel 2 (Definition 2.8) definierte Bild der Abbildung $f : G \to H$ ist. Es gilt dann: $\ker(f)$ ist eine Untergruppe von G und $\operatorname{im}(f)$ ist eine Untergruppe von H.

Beweis. Wir müssen die Axiome U1, U2 und U3 aus Definition 8.3 nachrechnen. Zuerst wollen wir zeigen, dass immer $f(e_G) = e_H$ gilt: Wir haben $f(e_G) = f(e_g * e_G)$. Jetzt ist f ein Gruppenhomomorphismus, d. h.$f(e_G) = f(e_G) \circ f(e_G)$. Wenn wir definieren $a := f(e_G) \in H$, dann gilt also:

$$a \circ a = a \quad \Rightarrow \quad a^{-1} \circ a \circ a = a^{-1} \circ a \quad \Rightarrow \quad a = e_H.$$

Also gilt $f(e_G) = e_H$. Damit ist $e_G \in \ker(f)$ und $e_H \in \operatorname{im}(f)$, es gilt U1 sowohl für $\ker(f)$ als auch für $\operatorname{im}(f)$. Nun zeigen wir U2: Seien $x, y \in \ker(f)$.

$$\Rightarrow \quad f(x) = f(y) = e_H \quad \Rightarrow \quad f(x) \circ f(y) = e_H \circ e_H = e_H,$$

aber $f(x) \circ f(y) = f(x * y)$, also $f(x * y) \in e_H$, also $x * y \in \ker(f)$. Seien andererseits $a, b \in \operatorname{im}(f)$, d. h.

$$\exists x, y \in G : \; f(x) = a, f(y) = b \quad \Rightarrow \quad f(x * y) = f(x) \circ f(y) = a \circ b \quad \Rightarrow \quad a \circ b \in \operatorname{im}(f).$$

Schließlich verifizieren wir noch U3: Sei $x \in \ker(f)$, also $f(x) = e_H$, dann gilt:

$$e_H = f(e_G) = f(x * x^{-1}) = f(x) \circ f(x^{-1}) = e_H \circ f(x^{-1}) = f(x^{-1}) \quad \Rightarrow \quad x^{-1} \in \ker(f).$$

Sei $a \in \operatorname{im}(f)$, d. h.$\exists x \in G : \; f(x) = a$.

$$\Rightarrow \quad e_H = f(e_G) = f(x * x^{-1}) = f(x) \circ f(x^{-1}) = a \circ f(x^{-1}) \quad \Rightarrow \quad a^{-1} = f(x^{-1}) \quad \Rightarrow \quad a^{-1} \in \operatorname{im}(f).$$

□

Wir studieren nun einen besonders wichtigen Gruppenhomomorphismus, welcher auf den symmetrischen Gruppen definiert ist.

Definition 8.12. *Sei $\sigma \in S_n$ eine Permutation. Seien $i, j \in \{1, \ldots, n\}$ mit $i \neq j$. Dann heißt das Paar (i, j) ein Fehlstand, falls gilt: $i < j$ und $\sigma(i) > \sigma(j)$. Wir definieren*

$$\text{Fehlstände}(\sigma) := \left\{(i, j) \in \{1, \ldots, n\}^2 \;\middle|\; i < j \text{ und } \sigma(i) > \sigma(j)\right\},$$

sowie

$$\operatorname{sign}(\sigma) := (-1)^{|\,\text{Fehlstände}(\sigma)|}$$

Es gibt also $\operatorname{sign}(\sigma) \ni \{1, -1\}$. Die Zahl $\operatorname{sign}(\sigma)$ heißt Signum oder Vorzeichen der Permutation σ.

Berechnung des Vorzeichens:

1. Methode: Schreibe die Permutation σ in der Form $\sigma = \begin{pmatrix} 1 & \dots & n \\ a_1 & \dots & a_n \end{pmatrix}$ und verbinde jeweils gleiche Zahlen in der oberen und unteren Zeile, Beispiel:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix} \in S_5$$

Dann liefert jeder Überschneidungspunkt genau einen Fehlstand, in obigem Beispiel also:

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

2. Methode: Zerlege σ gemäß Satz 8.9 in ein Produkt von Zykeln, im Beispiel: $\sigma = (1\,3) \circ (2\,5\,4)$. Danach verwende das folgende Lemma (hier ohne Beweis):

Lemma 8.13.

1.) Sei $(a_1 \dots a_k) \in S_n$ ein Zykel, dann ist

$$\operatorname{sign}((a_1 \dots a_k)) = (-1)^{k-1}.$$

2.) Seien $\sigma, \tau \in S_n$, dann gilt:

$$\operatorname{sign}(\sigma \circ \tau) = \operatorname{sign}(\sigma) \cdot \operatorname{sign}(\tau).$$

Wir erhalten also im obigen Beispiel $\sigma = (1\,3) \circ (2\,5\,4)$:

$$\operatorname{sign}(\sigma) = \operatorname{sign}((1\,3)) \cdot \operatorname{sign}((2\,5\,4)) = (-1)^{2-1} \cdot (-1)^{3-1} = (-1) \cdot 1 = -1.$$

Wir können eine wichtige Konsequenz aus dem letzten lemma ziehen.

Korollar 8.14. *Betrachte die Gruppe $G = \{1, -1\}$ mit Verknüpfung $\cdot$, d. h., mit folgender Verknüpfungstabelle:*

$\cdot$	*1*	*-1*
1	*1*	*-1*
-1	*-1*	*1*

Dann definiert die Abbildung

$$\operatorname{sign} : S_n \to G$$

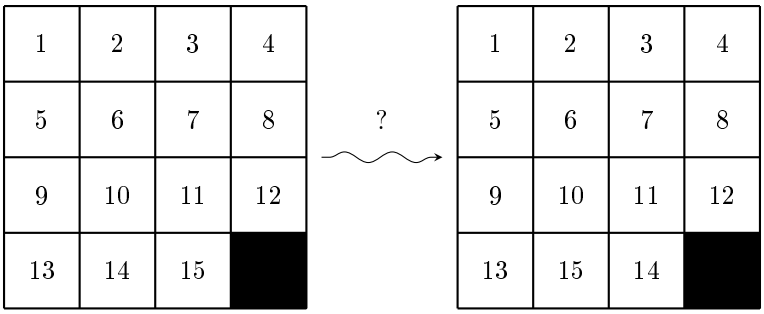
einen Gruppenhomomorphismus.

Beweis. Dies folgt direkt aus dem Lemma 8.13, 2., d. h., es gilt:

$$\forall \sigma, \tau \in S_n : \ \operatorname{sign}(\sigma \circ \tau) = \operatorname{sign}(\sigma) \cdot \operatorname{sign}(\tau).$$

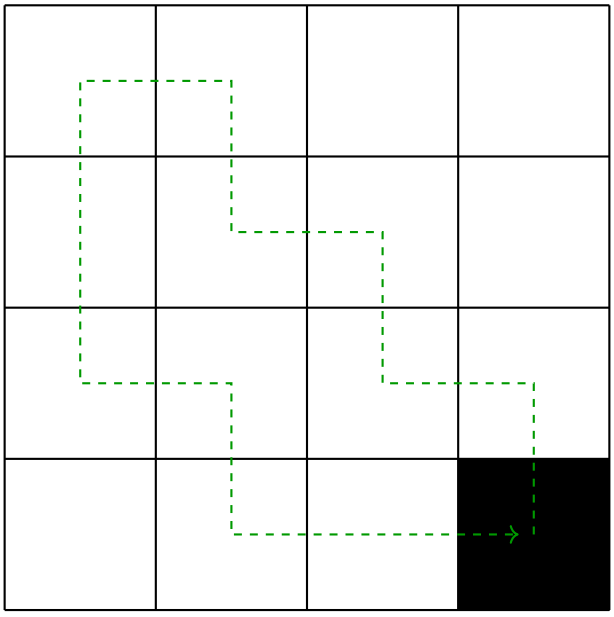
□

Als Anwendung wollen wir noch das bekannte Schiebepuzzle untersuchen. Das Ziel ist es z. B. , das linke Puzzle durch Verschieben in das rechte zu überführen:



Das schwarze Feld ist leer und man kann durch Verschieben die anderen 15 Felder umordnen. Frage: Lässt sich das Puzzle von der linken in die rechte Position bringen? Einige Versuche suggerieren, dass dies nicht geht. Man kann natürlich versuchen, alle Varianten durchzuprobieren, aber bei größeren Puzzlespielen (z. B. 5×5 oder 6×6 Felder) wird das sehr schwierig. Wir brauchen also einen Beweis, dass es nicht geht. Wir argumentieren so:

Das schwarze Feld habe die Nummer 16. In jedem Schritt wird es mit einem anderen Feld vertauscht, dies entspricht einem Zyklus $(i\ 16)$, wobei i eine Zahl zwischen 1 und 15 ist (in jedem Schritt kommen dafür nur manche Zahlen in Frage, nämlich die Felder, die an das schwarze Feld angrenzen). Das schwarze Feld wandert über das Feld, z. B. so:



Wenn es am Anfang und am Ende unten rechts ist, dann haben wir eine gerade Anzahl von Vertauschungen durchgeführt, da jede Verschiebung des schwarzen Feldes nach oben, bzw. nach links durch ein Verschiebung nach unten bzw. nach rechts kompensiert werden muss. Die Gesamtverschiebung entspricht also einer Permutation $\sigma = \sigma_1 \circ \ldots \circ \sigma_{2l}$ mit $\sigma_k = (i_k\ 16)$, $i_k \in \{1, \ldots, 15\}\ \forall k \in \{1, \ldots, 2l\}$. Wegen Lemma 8.13 gilt jetzt

$$\operatorname{sign}(\sigma) = \operatorname{sign}(\sigma_1) \cdot \ldots \cdot \operatorname{sign}(\sigma_{2l}) = (-1)^{2l} = 1,$$

denn das Vorzeichen eines Zykels mit der Länge 2 ist gleich -1. Aber die rechte Puzzleposition entsteht durch Vertauschen von 14 und 15, also müsste $\sigma = (14\ 15)$ gelten, aber $\operatorname{sign}((14\ 15)) = -1$. Daher kann man durch Verschieben das Puzzle nicht von der linken in die rechte Position bringen.

Kapitel 9

Elemente der linearen Algebra

Das Grundproblem der linearen Algebra ist das Lösen von linearen Gleichungssystemen. Hierzu wollen wir zunächst einige Beispiele betrachten. Wir beginnen mit einem ganz praktischen Problem: Eine Bank habe n Kunden, diese haben zu einem bestimmten Zeitpunkte n Kontostände. Jeder dieser Kontostände ist eine reelle Zahle x_i, alle zusammen können wir als einen Vektor $(x_1, \ldots, x_n) \in \mathbb{R}^n$ auffassen. Will man nun das Gesamtguthaben x ermitteln, hat man die Summe der Einträge dieser Vektoren zu berechnen, also $x = x_1 + \ldots + x_n$. Sei nun die Zahl x_i nicht ein Kontostand, sondern der Stand eines Aktiendepots, mit Aktienwert b_i, dann ergibt sich der Gesamtwert als

$$x = b_1 x_1 + \ldots + b_n x_n.$$

Dies ist ein typisches Beispiel einer linearen Gleichung. Hat man noch weitere Bedingungen gegeben (z. B. ein jährliche Dividendenzahlung d_i für die Aktie x_i), so erhält man ein lineares Gleichungssystem:

$$\begin{aligned} x &= b_1 x_1 + \ldots + b_n x_n \\ d &= d_1 x_1 + \ldots + d_n x_n \end{aligned}$$

und man kann z. B. fragen, ob es für vorgegebene Zahlen x und d (also für einen vorgegebenen Wert des Depots x und eine vorgegebene Dividendenzahlung d) eine Lösung $(x_1, \ldots, x_n) \in \mathbb{R}^n$ gibt, so dass das Depot genau diesen Wert und diese Dividende liefert. In der Praxis wird man es häufiger mit Ungleichungen zu tun haben (bei der gewisse Parameter nicht genau erreicht, sondern optimiert werden sollen), aber auch dafür ist das Verständnis von linearen Gleichungssystemen fundamental. Zum Aufstellen und Lösen linearer Gleichungssysteme benötigt man Vektoren. Wir behandeln gleich einen etwas allgemeineren Fall.

Definition 9.1. *Sei K ein beliebiger Körper und $n \in \mathbb{N}$. Ein Vektor der Länge n mit Einträgen aus K ist ein Element*

$$(x_1, \ldots, x_n) \in K^n := \underbrace{K \times \ldots \times K}_{n\text{-}mal},$$

d. h., $x_i \in K \; \forall i = 1, \ldots, n$.

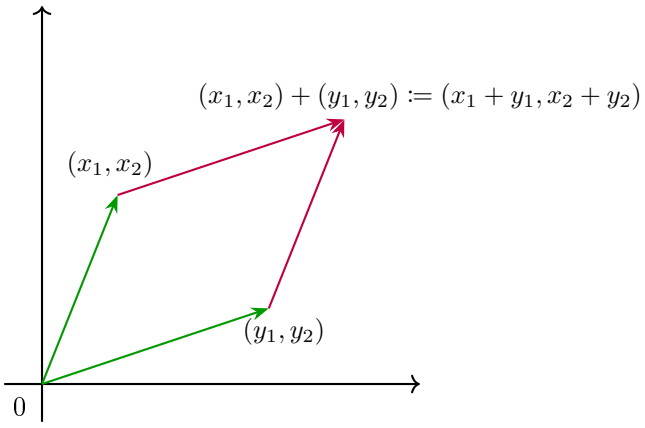
Vektoren kann man addieren, d. h., es gibt eine Abbildung

$$\begin{aligned} K^n \times K^n &\to K^n \\ (x_1, \ldots, x_n), (y_1, \ldots, y_n) &\mapsto (x_1 + y_1, \ldots, x_n + y_n) \end{aligned}$$

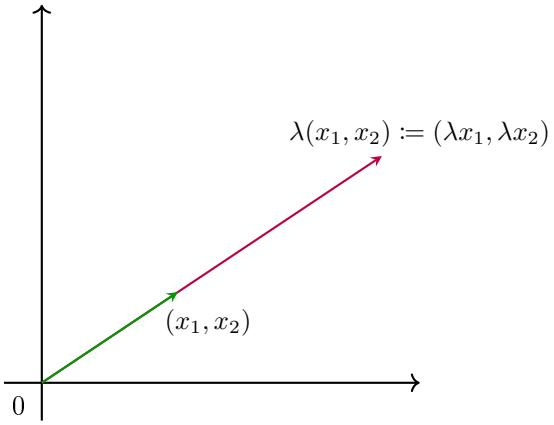
sowie mit Elementen aus K multiplizieren, d. h., es gibt eine Abbildung

$$\begin{aligned} K \times K^n &\to K^n \\ \lambda, (x_1, \ldots, x_n) &\mapsto (\lambda x_1, \lambda x_2 \ldots, \lambda x_n) \end{aligned}$$

Man kann diese Rechenoperationen geometrisch deuten, wenn man sich z. B. den Fall $K = \mathbb{R}$ und $n = 2$ anschaut. Ein Vektor (x_1, x_2) ist dann ein Pfeil in der Ebene vom Nullpunkt zum Punkt $(x_1, x_2) \in \mathbb{R}^2$:



Die Summe der Vektoren erhält man durch Bilden des Parallelogramms über den beiden Vektoren. Analog erhält man Multiplikation mit $\lambda \in \mathbb{R}$ durch Streckung:



Wir studieren jetzt lineare Gleichungssysteme genauer. Zunächst ein Beispiel: Gegeben sei das folgende System von zwei Gleichungen in drei Variablen (wir suchen Lösungen $(x_1, x_2, x_3) \in \mathbb{R}^3$):

$$\begin{aligned} x_1 + x_2 + x_3 &= -6 && \text{(I)} \\ x_1 + 2x_2 + 3x_3 &= -10 && \text{(II)} \end{aligned}$$

Umformen führt zu:

$$\begin{aligned} x_1 + x_2 + x_3 &= -6 && \text{(I)} \\ x_2 + 2x_3 &= -4 && (\widetilde{\text{II}} \coloneqq \text{II}-\text{I}) \end{aligned}$$

Gleichung $(\widetilde{\text{II}})$ lässt sich auch schreiben als:

$$x_2 = -4 - 2x_3 \qquad (*)$$

Durch Einsetzen in Gleichung (I) erhalten wir:

$$\begin{aligned} & x_1 - 4 - 2x_3 + x_3 && = -6 \\ \Leftrightarrow \quad & x_1 - x_3 && = -2 \\ \Leftrightarrow \quad & x_1 && = x_3 - 2 \qquad (**) \end{aligned}$$

Wir erhalten also als umgeformtes System:

$$\begin{aligned} x_2 &= -4 - 2x_3 \\ x_1 &= x_3 - 2 \end{aligned}$$

Für jede Zahl $x_3 \in \mathbb{R}$ erhalten wir also Zahlen $x_1, x_2 \in \mathbb{R}$, so dass der Vektor $(x_1, x_2, x_3) \in \mathbb{R}^3$ eine Lösung des ursprünglichen Systems darstellt. Dieses Gleichungssystem hat unendlich viele Lösungen. Ein weiteres Beispiel:

$$\begin{aligned} x_1 + 3x_2 &= 7 && \text{(I)} \\ 2x_1 + 4x_2 &= 10 && \text{(II)} \end{aligned}$$

Einsetzen von (I) in (II) ergibt:

$$\begin{aligned} & 2 \cdot (7 - 3x_2) + 4x_2 && = 10 \\ \Leftrightarrow \quad & -2x_2 && = 10 - 14 = -4 \\ \Leftrightarrow \quad & x_2 && = 2 \end{aligned}$$

Einsetzen in (I) liefert:

$$\begin{aligned} x_1 + 6 &= 7 \\ \Leftrightarrow \quad x_1 &= 1 \end{aligned}$$

Dieses System hat also genau eine Lösung, nämlich den Vektor $(x_1, x_2) = (1, 2) \in \mathbb{R}^2$. Ändert man das obige System in

$$\begin{aligned} x_1 + 3x_2 &= 7 && \text{(I)} \\ 2x_1 + 6x_2 &= 10 && \text{(II)} \end{aligned}$$

dann ergibt sich durch Einsetzen von (I) in (II):

$$2(7 - 3x_2) + 6x_2 = 14 + 0x_2 \stackrel{!}{=} 10$$

und dies führt auf die offensichtlich falsche Gleichung $14 = 10$. Hier gibt es also keinen einzigen Vektor $(x_1, x_2) \in \mathbb{R}^2$, welcher das Gleichungssystem löst.

Wir wollen jetzt eine systematische Methode zum Lösen von Gleichungssystemen behandeln, nämlich das Eliminationsverfahren von Gauß. Dafür benötigen wir Matrizen.

Definition 9.2. *Eine Matrix A ist ein Schema*

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

bestehend aus m Zeilen und n Spalten mit Einträgen aus einem Körper K. Die Menge der Matrizen mit m Zeilen und n Spalten wird mit $\mathrm{M}(m \times n, K)$ bezeichnet. Falls $m = 1$ ist, dann nennen wir ein Element $v \in \mathrm{M}(1 \times n, K)$ einen Zeilenvektor und schreiben

$$v = (v_1, v_2, \dots, v_n),$$

es ist also $\mathrm{M}(1 \times n, K) = K^n$. Solche Zeilenvektoren sind genau die Vektoren aus Definition 9.1. Falls $n = 1$ ist, nennen wir $w \in \mathrm{M}(m \times 1, K)$ einen Spaltenvektor und schreiben

$$w = \begin{pmatrix} w_1 \\ \vdots \\ w_m \end{pmatrix}.$$

Um mit Matrizen rechnen zu können, benötigen wir Verknüpfungen. Diese werden jetzt definiert.

Definition 9.3.

a) Seien $A, B \in \mathrm{M}(m \times n, K)$ *gegeben durch*

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \text{ und } B = \begin{pmatrix} b_{11} & \dots & b_{1n} \\ \vdots & & \vdots \\ b_{m1} & \dots & b_{mn} \end{pmatrix}$$

und sei $c \in K$. *Dann definieren wir*

$$A + B := \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} & \dots & a_{1n} + b_{1n} \\ a_{21} + b_{21} & a_{22} + b_{22} & \dots & a_{2n} + b_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} + b_{m1} & a_{m2} + b_{m2} & \dots & a_{mn} + b_{mn} \end{pmatrix} \in \mathrm{M}(m \times n, K)$$

sowie

$$c \cdot A := \begin{pmatrix} c \cdot a_{11} & \dots & c \cdot a_{1n} \\ \vdots & & \vdots \\ c \cdot a_{m1} & \dots & c \cdot a_{mn} \end{pmatrix} \in \mathrm{M}(m \times n, K)$$

b) Seien jetzt $A \in \mathrm{M}(m \times n, K)$ *und* $B \in \mathrm{M}(n \times r, K)$. *Dann definieren wir* $A \cdot B \in \mathrm{M}(m \times r, K)$ *durch*

$$A \cdot B := \begin{pmatrix} c_{11} & \dots & c_{1r} \\ \vdots & & \vdots \\ c_{m1} & \dots & c_{mr} \end{pmatrix},$$

wobei $c_{ij} := \sum_{k=1}^{n} a_{ik} \cdot b_{kj}$ *sei. Insbesondere können wir für* $A \in \mathrm{M}(p \times q, K), v \in \mathrm{M}(1 \times p, K) \simeq K^p$ *sowie* $w \in \mathrm{M}(q \times 1, K)$ *die Produkte* $v \cdot A \in \mathrm{M}(1 \times q, K), A \cdot w \in \mathrm{M}(p \times 1, K)$ *bilden.*

Beispiele zur Matrizenmultiplikation:

1.) Seien

$$A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \\ 2 & 0 \end{pmatrix} \in \mathrm{M}(3 \times 2, \mathbb{R}), \quad B = \begin{pmatrix} 1 & 3 \\ 2 & 1 \end{pmatrix} \in \mathrm{M}(2 \times 2, \mathbb{R})$$

$\Rightarrow A \cdot B \in \mathrm{M}(3 \times 2, \mathbb{R})$ berechnet man wie folgt:

$$\begin{array}{c|c} & \begin{pmatrix} 1 & 3 \\ 2 & 1 \end{pmatrix} \\ \hline \begin{pmatrix} 1 & 2 \\ 0 & 1 \\ 2 & 0 \end{pmatrix} & \begin{pmatrix} 5 & 5 \\ 2 & 1 \\ 2 & 6 \end{pmatrix} \end{array} \quad \text{mit} \quad \begin{array}{ll} 5 & = 1 \cdot 1 + 2 \cdot 2 \\ 5 & = 3 \cdot 1 + 2 \cdot 1 \\ 5 & = 1 \cdot 0 + 2 \cdot 1 \\ 5 & = 3 \cdot 0 + 1 \cdot 1 \\ 5 & = 1 \cdot 2 + 2 \cdot 0 \\ 5 & = 3 \cdot 2 + 1 \cdot 0 \end{array}$$

2.) Sei $A = \begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix} \in \mathrm{M}(2 \times 2, \mathbb{R})$ und $w = \begin{pmatrix} 1 \\ 2 \end{pmatrix} \in \mathrm{M}(2 \times 1, \mathbb{R})$, dann ist

$$A \cdot w = \begin{pmatrix} 1 & 3 \\ 2 & 4 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 1 \cdot 1 + 2 \cdot 3 \\ 1 \cdot 2 + 2 \cdot 4 \end{pmatrix} = \begin{pmatrix} 7 \\ 10 \end{pmatrix}.$$

3.) Wir können auch Matrizen betrachten, deren Einträge Variablen sind. Sei z. B. $x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$ ein Spaltenvektor mit drei Unbekannten, sei weiterhin $w = \begin{pmatrix} -6 \\ -10 \end{pmatrix} \in \mathrm{M}(2 \times 1, \mathbb{R})$ und sei $A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \end{pmatrix} \in \mathrm{M}(2 \times 3, \mathbb{R})$, dann betrachten wir $A \cdot x = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_1 + x_2 + x_3 \\ x_1 + 2x_2 + 3x_3 \end{pmatrix}$. Wir können also die Matrixgleichung $A \cdot x = w$ aufstellen und diese ist genau äquivalent zu dem System von zwei (gewöhnlichen) Gleichungen

$$\begin{aligned} x_1 + x_2 + x_3 &= -6 \\ x_1 + 2x_2 + 3x_3 &= -10, \end{aligned}$$

welches wir weiter oben behandelt hatten.

Das letzte Beispiel gilt ganz allgemein: Sei ein lineares Gleichungssystem

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

gegeben, mit Koeffizienten $a_{ij} \in K, (i = 1, \ldots, m,\ j = 1, \ldots, n)$, Unbekannten $x_1, \ldots, x_n$ sowie Konstanten $b_1, \ldots, b_m \in K$. Dann nennt man

$$A = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \ldots & a_{mn} \end{pmatrix} \in \mathrm{M}(m \times n, K)$$

die Koeffizientenmatrix des Systems. Betrachtet man $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ als Spaltenvektor der Variablen und $b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \in \mathrm{M}(m \times 1, K)$, so kann man das gesamte Gleichungssystem kompakt als

$$A \cdot x = b$$

schreiben. Man nennt außerdem die Matrix

$$A = \begin{pmatrix} a_{11} & \ldots & a_{1n} & b_1 \\ \vdots & & \vdots & \vdots \\ a_{m1} & \ldots & a_{mn} & b_m \end{pmatrix} \in \mathrm{M}(m \times (n+1), K)$$

die erweiterte Koeffizientenmatrix des gegebenen Systems. Wir behandeln jetzt verschiedene Umformungsoperationen für Matrizen, welche für das Eliminationsverfahren von Gauß benötigt werden.

Definition 9.4. *Sei* $A = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \ldots & a_{mn} \end{pmatrix} \in \mathrm{M}(m \times n, K)$. *Dann nennen wir die folgenden Operationen elementare Zeilenumformungen:*

1.) Vertauschen der i-ten und der j-ten Zeile. Die Matrix $\tilde{A} \in \mathrm{M}(m \times n, K)$, welche auf diese Art aus A entsteht, ist also:

$$\tilde{A} = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{j1} & \dots & a_{jn} \\ \vdots & & \vdots \\ a_{i1} & \dots & a_{in} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \begin{matrix} \\ \\ \leftarrow i\text{-te Zeile} \\ \\ \leftarrow j\text{-te Zeile} \\ \\ \\ \end{matrix}$$

2.) Addition des c-Fachen der i-ten Zeile zur j-ten Zeile, wobei $c \in K \setminus \{0\}$ und $i \neq j$ ist. Hier sieht die umgeformte Matrix $\tilde{A}$ so asu:

$$\tilde{A} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & \vdots & & \vdots \\ a_{i1} & a_{i2} & \dots & a_{in} \\ \vdots & \vdots & & \vdots \\ a_{j1} + c \cdot a_{i1} & a_{j2} + c \cdot a_{i2} & \dots & a_{jn} + c \cdot a_{in} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \begin{matrix} \\ \\ \leftarrow i\text{-te Zeile} \\ \\ \leftarrow j\text{-te Zeile} \\ \\ \\ \end{matrix}$$

Der Grund, diese Operationen zu betrachten, liegt in folgender Aussage:

Proposition 9.5. *Sei $A \in \mathrm{M}(m \times n, K)$ und $b \in \mathrm{M}(m \times 1, K)$, definiere*

$$\mathrm{Lös}(A, b) \coloneqq \{x \in \mathrm{M}(n \times 1, K) \mid A \cdot x = b\}$$

als die Lösungsmenge des Gleichungssystems $A \cdot x = b$. Falls die Matrix $(\tilde{A}, \tilde{b}) \in \mathrm{M}(m \times (n+1), K)$ aus der erweiterten Koeffizientenmatrix (A, b) des Systems durch wiederholte elementare Zeilenumformungen gemäß Definition 9.4 hervorgeht, dann gilt

$$\mathrm{Lös}(A, b) = \mathrm{Lös}(\tilde{A}, \tilde{b}).$$

Beweis. Es reicht aus, den Fall zu beweisen, bei dem $(\tilde{A}, \tilde{b})$ aus (A, b) mittels einer einzigen elementaren Zeilenumformung entsteht. Bei Umformungen vom Typ 1.) ist dies völlig klar, denn jede Zeile der (erweiterten) Koeffizientenmatrix entspricht einer Gleichung des Systems. Diese müssen gleichzeitig erfüllt sein, aber auf ihre Reihenfolge kommt es nicht an. Betrachte nun eine Umformung vom Typ 2.). Wir können annehmen, dass unser Gleichungssystem nur aus den zwei Gleichungen

$$\begin{aligned} a_{j1}x_1 + \ldots + a_{jn}x_n &= b_j \\ a_{i1}x_1 + \ldots + a_{in}x_n &= b_i \end{aligned} \tag{9.1}$$

besteht und in das System

$$\begin{aligned} (a_{j1} + c \cdot a_{i1})x_1 + \ldots + (a_{jn} + c \cdot a_{in})x_n &= b_j \\ a_{i1}x_1 + \ldots + a_{in}x_n &= b_i \end{aligned} \tag{9.2}$$

überführt wird, da alle anderen Gleichungen unverändert bleiben. Falls ein $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ Lösung von (9.1) ist, dann sicher auch von (9.2), denn man erhält (9.2) ja gerade durch Kopieren der zweiten Gleichung und durch

Addieren des c-Fachen der zweiten Gleichung von (9.1) zur ersten Gleichung von (9.1). Falls $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ das System (9.2) erfüllt, dann auch das System (9.1), denn man bekommt die erste Gleichung von (9.1) aus dem Addieren des $(-c)$-Fachen der zweiten Gleichung von (9.2) zur ersten Gleichung von (9.2). □

Für das Gaußsche Eliminierungsverfahren brauchen wir spezielle Matrizen.

Definition 9.6. *Eine Matrix $A \in \mathrm{M}(m \times n, K)$ heißt in Zeilenstufenform, falls sie folgende Gestalt hat:*

$$A = \begin{pmatrix} (*) & & & & \\ & (*) & & & \\ & & (*) & & \\ & & & \ddots & \\ & & & & (*) \\ & & & & \end{pmatrix} \Bigg\} r$$

Hierbei sind die Einträge $(*)$ alle ungleich Null und unterhalb der Stufenlinie stehen nur Nullen. Formal definiert man dies so: Es gibt eine Zahl r $(1 \leq r \leq m)$, so dass in der 1. bis zur r. Zeile nicht nur Nullen stehen und so dass in den Zeilen $r+1, \ldots, m$ nur Nullen stehen. Sei weiterhin für alle $i \in \{1, \ldots, r\}$ die Zahl j_i der kleinste Index, so dass $a_{ij} \neq 0$ ist (d. h. der Eintrag der I-ten Zeile und j_i-ten Spalte ist gerade so einer, der oben mit $(*)$ markiert ist.) Dann gelte: $j_1 < j_2 < \ldots < j_r$. Die Zahl r heißt der Rang von A.

Ein Beispiel für eine Matrix in Zeilenstufenform ist:

$$A = \begin{pmatrix} 0 & 2 & 0 & 4 & 6 & 0 & 5 \\ 0 & 0 & 1 & 3 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \in \mathrm{M}(4 \times 7, \mathbb{R})$$

Hier gilt: $r = 3, j_1 = 2, j_2 = 3, j_3 = 6$.

Wir wollen nun definieren, was es eigentlich heißt, ein Gleichungssystem zu lösen. Wie wir gesehen haben, kann es eine Lösung, unendlich viele oder gar keine Lösung geben.

Definition 9.7. *Sei ein lineares Gleichungssystem gegeben durch eine Matrix $A \in \mathrm{M}(m \times n, K)$ und $b \in \mathrm{M}(m \times 1, K)$. Angenommen, es gilt $\mathrm{Lös}(A, b) \neq \varnothing$. Dann nennen wir eine bijektive Abbildung $\Phi : K^k \to \mathrm{Lös}(A, b)$ eine Lösung des Systems (A, b).*

Im ersten Beispiel war $(A, b) = \begin{pmatrix} 1 & 1 & 1 & -6 \\ 1 & 2 & 3 & -10 \end{pmatrix} \in \mathrm{M}(2 \times 4, \mathbb{R})$, hier ist die Abbildung

$$\begin{aligned} \mathbb{R} &\to \mathrm{Lös}(A, b) \subset \mathrm{M}(3 \times 1, \mathbb{R}) \\ x_3 &\mapsto \begin{pmatrix} -4 - 2x_3 \\ x_3 - 2 \\ x_3 \end{pmatrix} = \begin{pmatrix} -2x_3 \\ x_3 \\ x_3 \end{pmatrix} - \begin{pmatrix} 4 \\ 2 \\ 0 \end{pmatrix} \end{aligned}$$

die Lösung.

Um für ein gegebenes System eine Lösung zu berechnen, haben wir zwei Schritte auszuführen:

1.) Wir bringen die erweiterte Koeffizientenmatrix in Zeilenstufenform, diese heiße $(\tilde{A}, \tilde{b})$.

2.) Wir konstruieren die Abbildung $\Phi : K^k \to \text{Lös}(\tilde{A}, \tilde{b}) = \text{Lös}(A, b)$.

Der erste Schritt wird durch die folgende Aussage beschrieben.

Satz 9.8. *Sei $A \in \mathrm{M}(m \times n, K)$. Dann kann A mit elementaren Zeilenumformungen in endlich vielen Schritten auf Zeilenstufenform gebracht werden.*

Beweis. Wir führen einen Induktionsbeweis über die Anzahl der Spalten von A. Falls A null oder auch eine Spalte hat, ist die Aussage klar. Als Induktionsvoraussetzung nehmen wir an, dass der Satz für alle Matrizen $B \in \mathrm{M}(p \times q, K)$ gelte, falls $q < n$ ist.

Sei nun $A \in \mathrm{M}(m \times n, K)$ gegeben. Wir können $A \neq 0$ annehmen, sonst hat A schon Zeilenstufenform mit $r = 0$. Dann existiert aber eine von Null verschiedene Spalte, sei $j_1 = \min\{j : \exists i : a_{ij} \neq 0\}$ der kleinste Index, so dass die j_1-te Spalte nicht nur aus Nullen besteht. Falls $a_{1j_1} = 0$ ist, suchen wir uns eine Zeile i_1 mit $a_{i_1 j_1} \neq 0$ und vertauschen die erste mit der i_1-ten Zeile. Danach sieht die Matrix so aus:

$$\begin{pmatrix} 0 & \dots & 0 & \tilde{a}_{1j_1} & * & \dots & * \\ \vdots & & \vdots & * & * & \dots & * \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & * & * & \dots & * \end{pmatrix}$$

mit $\tilde{a}_{1j_1} \neq 0$, und alle durch $*$ bezeichneten Einträge sind beliebig (eventuell auch gleich Null). Durch elementare Umformungen vom Typ 2.) kann man alle Einträge $*$ unterhalb von $\tilde{a}_{1j_1}$ zu Null machen: Falls z. B. in der Zeile i_1 unter $\tilde{a}_{1j_1}$ die Zahl a steht, soll gelten

$$a + c\Delta\tilde{a}_{1j_1} = 0 \Leftrightarrow c = \frac{a}{\tilde{a}_{1j_1}}$$

und wenn man dann das c-Fache der ersten Zeile auf die i_1-te Zeile addiert, ändert sich der Eintrag a zu 0. Man erhält damit die Matrix

$$\tilde{A}_1 = \left(\begin{array}{cccc|ccc} 0 & \dots & 0 & \tilde{a}_{1j_1} & * & \dots & * \\ \vdots & & \vdots & 0 & & & \\ \vdots & & \vdots & \vdots & & A_2 & \\ 0 & \dots & 0 & 0 & & & \end{array}\right)$$

mit $A_2 \in \mathrm{M}(p \times q, K)$, $p = m - 1, q < n$. Nach Induktionsvoraussetzung gibt es jetzt Zeilenumformungen, welche A_2 in Zeilenstufenform mit Rang r' bringen. Diese Zeilenumformungen von A_2 kann man auf die Zeilen 2 bis m der Martix $\tilde{A}_1$ ausdehnen, denn in den Spalten 1 bis j_1 stehen in diesen Zeilen nur Nullen, dort ändert sich also nichts. Dies liefert die Zeilenstufenform von A und es ist $r = \mathrm{Rang}(A) = r' + 1$. □

Wir betrachten ein einfaches Beispiel: Sei

$$A = \begin{pmatrix} 0 & 0 & 1 & 2 & 9 \\ 0 & 3 & 4 & 5 & 9 \\ 0 & 6 & 7 & 8 & 9 \\ 0 & 9 & 9 & 9 & 9 \end{pmatrix} \overset{(\mathrm{II})\leftrightarrow(\mathrm{I})}{\rightsquigarrow} \begin{pmatrix} 0 & 3 & 4 & 5 & 9 \\ 0 & 0 & 1 & 2 & 9 \\ 0 & 6 & 7 & 8 & 9 \\ 0 & 9 & 9 & 9 & 9 \end{pmatrix}$$

$$\overset{\substack{-2\cdot(\mathrm{I})+(\mathrm{III})\mapsto(\mathrm{III}) \\ -3\cdot(\mathrm{I})+(\mathrm{IV})\mapsto(\mathrm{IV})}}{\rightsquigarrow} \begin{pmatrix} 0 & 3 & 4 & 5 & 9 \\ 0 & 0 & 1 & 2 & 9 \\ 0 & 0 & -1 & -2 & -9 \\ 0 & 0 & -3 & -6 & -18 \end{pmatrix}$$

$$\overset{\substack{1\cdot(\mathrm{II})+(\mathrm{III})\mapsto(\mathrm{III}) \\ -3\cdot(\mathrm{II})+(\mathrm{IV})\mapsto(\mathrm{IV})}}{\rightsquigarrow} \begin{pmatrix} 0 & 3 & 4 & 5 & 9 \\ 0 & 0 & 1 & 2 & 9 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 9 \end{pmatrix}$$

$$\overset{(\mathrm{IV})\leftrightarrow(\mathrm{III})}{\rightsquigarrow} \begin{pmatrix} 0 & 3 & 4 & 5 & 9 \\ 0 & 0 & 1 & 2 & 9 \\ 0 & 0 & 0 & 0 & 9 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Diese letzte Matrix ist in Zeilenstufenform, der Rang von A ist also 3.

Wir müssen noch beschreiebn, wie man eine Lösung (im Sinne von Definition 9.7) eines Gleichungssystems, dessen erweiterte Koeffizientenmatrix in Zeilenstufenform ist, finden kann. Hierbei nehmen wir folgende Vereinfacheung an: Eine allgemeine Matrix in Zeilenstufenform sieht so aus:

$$A = \begin{pmatrix} (*) & & & & \\ & (*) & & & \\ & & (*) & & \\ & & & \ddots & \\ & & & & (*) \\ & & & & \end{pmatrix}$$

und die (von Null verschiedenen) Einträge $(*)$ stehen in den Spalten $j_1, \ldots, j_r$ mit $j_1 < \ldots < j_r$. Wenn man jetzt die Spalten von A umordnet, kann man stets die folgende Zeilenstufenform erreichen:

$$\tilde{A} = \begin{pmatrix} (*) & & & & \\ & (*) & & & \\ & & (*) & & \\ & & & \ddots & \\ & & & & (*) \\ & & & & \end{pmatrix}$$

bei der die Einträge $(*)$ nur in der Diagonale stehen. Das Umordnen von Spalten entspricht dem Umnummerieren der Variablen des Gleichungssystems, ändert also nichts an der Struktur der Lösungsmenge. Wir

nehmen also an, dass wir eine erweiterte Koeffizientenmatrix in der speziellen Zeilenstufenform gegeben haben, d. h., es sei

$$(A,b) = \left(\begin{array}{ccccc|c} a_{11} & & & & & b_1 \\ & a_{22} & & & & b_2 \\ & & a_{33} & & & b_3 \\ & & & \ddots & & \vdots \\ & & & & a_{rr} & b_r \\ \hline & & & & & b_{r+1} \\ & & & & & \vdots \\ & & & & & b_m \end{array}\right) \in \mathrm{M}(m \times n, K)$$

mit $a_{11} \neq 0, \ldots, a_{rr} \neq 0$. In dieser Situation gilt nun:

Satz 9.9. *Falls für ein $i \in \{r+1, \ldots, m\}$ gilt, dass $b_i \neq 0$ ist, so folgt $\mathrm{Lös}(A,b) = \varnothing$. Falls hingegen $b_{r+1} = \ldots = b_m = 0$ gilt, so erhäjt man eine Lösung $\Phi : K^k \to \mathrm{Lös}(A,b)$ mit $k = n - r$ folgendermaßen: Man wählt $(\lambda_1, \ldots, \lambda_k) \in K^k$ freie Parameter und setzt $x_{r+1} = \lambda_1, \ldots, x_n = \lambda_k$. Dann schreibt sich die r-te Gleichung:*

$$\begin{aligned} & a_{rr}x_r + a_{r,r+1}\lambda_1 + \ldots + a_{rn}\lambda_k = b_r \\ \Leftrightarrow \qquad & x_r = \frac{1}{a_{rr}}(b_r - a_{r,r+1}\lambda_1 - \ldots - a_{rn}\lambda_k) \end{aligned} \tag{9.3}$$

Die $(r-1)$-te Gleichung lautet:

$$a_{r-1,r-1}x_{r-1} + a_{r-1,r}x_r + a_{r-1,r+1}\lambda_1 + \ldots + a_{r-1,n}\lambda_k = b_{r-1}.$$

Setzt man die Formel für x_r aus (9.3) in diese Gleichung ein, kann man (wegen $a_{r-1,r-1} \neq 0$) eine Formel für x_{r-1} herleiten. So berechnet man Formeln für $x_{r-2}, x_{r-3}, \ldots, x_2, x_1$. Dann setzt man:

$$\begin{array}{rccc} \Phi: & K^k & \to & \mathrm{Lös}(A,b) \subset \mathrm{M}(n \times 1, K) \\ & (\lambda_1, \ldots, \lambda_k) & \mapsto & \begin{pmatrix} x_1 \\ \vdots \\ x_r \\ \lambda_1 \\ \vdots \\ \lambda_k \end{pmatrix} \end{array}$$

Dies ist eine Lösung des Systems (A,b).

Beweis. Falls $b_i \neq 0$ für ein $i \in \{r+1, \ldots, m\}$, dann enthält das durch (A,b) gegebene System eine Gleichung

$$0 \cdot x_1 + 0 \cdot x_2 + \ldots + 0 \cdot x_n = b_{i+1}.$$

Diese hat natürlich keine Lösung, also ist $\mathrm{Lös}(A,b) = \varnothing$ in diesem Fall. Für $b_{r+1} = \ldots = b_m = 0$ ist die oben konstruierte Abbildung offensichtlich eine Lösung (d. h., bijektiv). □

Wir illustrieren diesen Satz an dem oben betrachteten Beispiel der Matrix

$$A = \left(\begin{array}{ccccccc} 0 & 2 & 0 & 4 & 6 & 0 & 5 \\ 0 & 0 & 1 & 3 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right) \in \mathrm{M}(4 \times 7, \mathbb{R}).$$

Sei $b = \begin{pmatrix} 3 \\ 1 \\ 2 \\ 0 \end{pmatrix}$, d. h., wir haben die erweiterte Koeffizientenmatrix

$$(A,b) = \left(\begin{array}{ccccccc|c} 0 & 2 & 0 & 4 & 6 & 0 & 5 & 3 \\ 0 & 0 & 1 & 3 & 2 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 3 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right).$$

Es ist $r = 3, n = 7$, d. h., $k = 4$, wir haben 4 freie Parameter $\lambda_1, \ldots, \lambda_4$ und suchen eine Abbildung $\mathbb{R}^4 \to \text{Lös}(A,b)$. Wir setzen $x_1 = \lambda_1, x_4 = \lambda_2, x_5 = \lambda_3$ und $x_7 = \lambda_4$. Dann sagt die 3. Gleichung:

$$3x_6 + \lambda_4 = 2 \quad \Leftrightarrow \quad x_6 = \frac{2}{3} - \frac{1}{3}\lambda_4.$$

Die 2. Gleichung liefert:

$$\begin{aligned} x_3 + 3\lambda_2 + 2\lambda_3 + x_6 = 1 \quad &\Leftrightarrow \quad x_3 = 1 - 3\lambda_2 - 2\lambda_3 - \frac{2}{3} + \frac{1}{3}\lambda_4 \\ &\Leftrightarrow \quad x_3 = \frac{1}{3} - 3\lambda_2 - 2\lambda 3 + \frac{1}{3}\lambda_4. \end{aligned}$$

Schließlich gibt die erste Gleichung:

$$2x_2 + 4\lambda_2 + 6\lambda_3 + 5\lambda_4 = 3 \quad \Leftrightarrow \quad x_2 = \frac{3}{2} - 2\lambda_2 - 3\lambda_3 - \frac{5}{2}\lambda_4.$$

Es ist also:

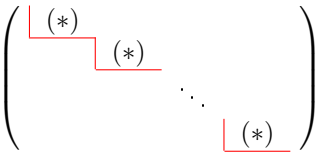
$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix} = \begin{pmatrix} \lambda_1 \\ \frac{3}{2} - 2\lambda_2 - 3\lambda_3 - \frac{5}{2}\lambda_4 \\ x_3 = \frac{1}{3} - 3\lambda_2 - 2\lambda 3 + \frac{1}{3}\lambda_4 \\ \lambda_2 \\ \lambda_3 \\ \frac{2}{3} - \frac{1}{3}\lambda_4 \\ \lambda_4 \end{pmatrix} = \begin{pmatrix} 0 \\ \frac{3}{2} \\ \frac{1}{3} \\ 0 \\ 0 \\ \frac{2}{3} \\ 0 \end{pmatrix} + \lambda_1 \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \lambda_2 \begin{pmatrix} 0 \\ -2 \\ -3 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \lambda_3 \begin{pmatrix} 0 \\ -2 \\ -3 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + \lambda_4 \begin{pmatrix} 0 \\ \frac{5}{2} \\ \frac{1}{3} \\ 0 \\ 0 \\ -\frac{1}{3} \\ 1 \end{pmatrix}$$

und die Lösungsabbildung ist gegeben durch

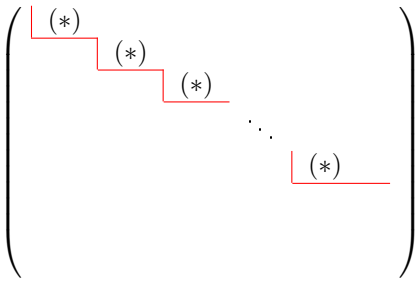
$$\begin{array}{rccc} \Phi: & \mathbb{R}^4 & \to & \text{Lös}(A,b) \\ & (\lambda_1, \ldots, \lambda_4) & \mapsto & \begin{pmatrix} \lambda_1 \\ \frac{3}{2} - 2\lambda_2 - 3\lambda_3 - \frac{5}{2}\lambda_4 \\ x_3 = \frac{1}{3} - 3\lambda_2 - 2\lambda 3 + \frac{1}{3}\lambda_4 \\ \lambda_2 \\ \lambda_3 \\ \frac{2}{3} - \frac{1}{3}\lambda_4 \\ \lambda_4 \end{pmatrix} \end{array}$$

Zum Abschluss wollen wir uns noch mit dem Spezialfall von Gleichungssystemen beschäftigen, bei denen die Anzahl der Gleichungen gleich der Anzahl der Variablen ist. Die Koeffizientenmatrix A ist dann ein Element von $\text{M}(n \times n, K)$. Bringt man so eine Matrix in Zeilenstufenform, können 2 Fälle auftreten: Entweder ist $\text{Rang}(A) = n$, oder aber $\text{Rang}(A) < n$. Schematisch:

$r \coloneqq \mathrm{Rang}(A) = n$



$r \coloneqq \mathrm{Rang}(A) < n$



Falls $r < n$ ist und $b \in \mathrm{M}(n \times 1, K)$, dann ist wie vorher $\mathrm{Lös}(A, b) = \varnothing$, falls ein $b_i \neq 0$ ist für $i \in \{r+1, \ldots, n\}$. Falls $b_{r+1} = \ldots = b_n = 0$, dann hat man wie vorher $k \coloneqq n - r$ freie Parameter und es gibt eine bijektive (Lösungs-)Abbildung $\Phi : K^k \to \mathrm{Lös}(A, b)$. Ist hingegen $r = n$, dann ist $k = 0$ und es kann also höchstens eine Lösung geben. Tatsächlich berechnet man wieder durch $x_n = \frac{b_n}{a_{nn}}, x_{n-1} = \frac{1}{a_{n-1,n-1}}(b_{n-1} - a_{n-1,n} \cdot x_n), \ldots$ eine eindeutige Lösung

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathrm{Lös}(A, b).$$

Insbesondere gilt: Ist $b = 0 \in \mathrm{M}(m \times 1, K)$, dann ist die eindeutige Lösung $x_1 = x_2 = \ldots = x_n = 0 \in K$.

Im Falle von quadratischen Matrizen (also $A \in \mathrm{M}(n \times n, K)$) kann man auch ohne das Gaußsche Eliminationsverfahren entscheiden, ob es eine eindeutige Lösung gibt, und diese dann auch berechnen. Dies erfordert einen neuen Begriff.

Definition 9.10. *Sei $A \in \mathrm{M}(n \times n, K)$ eine quadratische Matrix. Dann definieren wir die Determinante von A durch die Formel*

$$\det(A) \coloneqq \sum_{\sigma \in S_n} \mathrm{sign}\,(\sigma) \cdot a_{1\sigma(1)} \cdot \ldots \cdot a_{n\sigma(n)} \in K$$

Diese Summe hat also $n!$ Summanden und in jedem Summand nimmt man das Produkt über n Einträge der Matrix, jeweils genau einen aus jeder Zeile und aus jeder Spalte. Außerdem wird jeder Summand mit einem negativen Vorzeichen versehen, falls die Permutation $\sigma \in S_n$, welche festlegt, welche Einträge der Matrix multipliziert werden, negatives Vorzeichen (= Signum) hat.

Beispiele zu Determinanten:

Sei $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \in \mathrm{M}(2 \times 2, \mathbb{R})$, dann ist $\det(A) = a_{11} \cdot a_{22} - a_{21} \cdot a_{12} = 1 \cdot 4 - 3 \cdot 2 = 4 - 6 = -2$.

Sei $A = \begin{pmatrix} a \end{pmatrix} \in \mathrm{M}(1 \times 1, K)$, dann ist $\det(A) = a \in K$.

Sei $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \in \mathrm{M}(3 \times 3, \mathbb{R})$, dann hat die Formel zur Berechnung von $\det(A)$ sechs Summanden ($|S_3| = 6$), es gilt:

$$\begin{aligned} \det(A) &= 1 \cdot 5 \cdot 9 + 2 \cdot 6 \cdot 7 + 3 \cdot 4 \cdot 8 - 7 \cdot 5 \cdot 3 - 8 \cdot 8 \cdot 1 - 9 \cdot 4 \cdot 2 \\ &= 45 + 84 + \underbrace{96 - 105}_{-9} - 48 - 72 \\ &= 36 + \underbrace{84 - 48}_{36} - 72 = 0 \end{aligned}$$

Der folgende Satz verbindet die Determinante mit der Multiplikation von Matrizen. Man beachte, dass für $A, B \in \mathrm{M}(n \times n, K)$ gilt: $A \cdot B, B \cdot A \in \mathrm{M}(n \times n, K)$.

Satz 9.11. *Seien $A, B \in \mathrm{M}(n \times n, K)$, dann gilt*

$$\det(A \cdot B) = \det(B \cdot A) = \det(A) \cdot \det(B).$$

hier ohne Beweis.

Achtung: Im Allgemeinen ist $A \cdot B \neq B \cdot A$, wie das folgende Beispiel zeigt: $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$. Dann gilt:

$A \cdot B$	$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$	$B \cdot A$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{matrix} 3 & 4 \\ 1 & 2 \end{matrix}$	$\begin{pmatrix} 1 & 2 \\ 4 & 3 \end{pmatrix}$	$\begin{matrix} 2 & 1 \\ 4 & 3 \end{matrix}$

Also ist $A \cdot B \neq B \cdot A$. Hingegen gilt $\det(A \cdot B) = \det(B \cdot A) = 3 \cdot 2 - 1 \cdot 4 = 2$ und $\det(A) = 0 - 1 = -1$, $\det(B) = 4 - 6 = -2$.

Mithilfe der Determinante können wir jetzt die folgende Aussage zur Lösbarkeit von quadratischen Gleichungssystemen formulieren.

Satz 9.12. *Sei $A \in \mathrm{M}(n \times n, K)$ mit $\det(A) \neq 0$. Dann gilt Rang$(A) = n$. Außerdem hat in diesem Fall $\mathrm{Lös}(A, b)$ genau ein Element, egal welches $b \in \mathrm{M}(n \times 1, K)$ man als konstanten Vektor wählt. Insbesondere gilt für $b = 0 \in \mathrm{M}(n \times 1, K)$: $\mathrm{Lös}(A, b) = \{0\} \subset \mathrm{M}(1 \times n, K)$. Falls $\det(A) = 0$ ist, dann ist Rang$(A) < n$ und es gibt 2 Möglichkeiten:*

1. *Rang$(A, b) =$ Rang$(A) = r$. Dann ist $\mathrm{Lös}(A, b) \neq \varnothing$ und es existiert eine bijektive Abbildung*
$$\Phi \colon K^{n-r} \to \mathrm{Lös}(A, b).$$
2. *Rang$(A, b) >$ Rang(A). Dann ist $\mathrm{Lös}(A, b) = \varnothing$.*

hier ohne Beweis.

Als nächste Aussage haben wir noch den folgenden Satz, welcher die lineare Algebra mit der Gruppentheorie verbindet.

Satz 9.13.

1. *Sei $A \in \mathrm{M}(n \times n, K)$ mit $\det(A) \neq 0$. Dann existiert eine eindeutig bestimmte Matrix $B \in \mathrm{M}(n \times n, K)$, so dass gilt: $A \cdot B = B \cdot A = E_n$, wobei*
$$E_n := \begin{pmatrix} 1 & 0 & \dots & \dots & \dots & 0 \\ 0 & 1 & 0 & \dots & \dots & 0 \\ \vdots & 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & & \ddots & & \vdots \\ \vdots & \vdots & \vdots & 0 & 1 & 0 \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}$$
Man schreibt für die Matrix B auch A^{-1} (dies macht Sinn, weil B eindeutig bestimmt ist). Außerdem ist für alle $C \in \mathrm{M}(n \times n, K)$:
$$E_n \cdot C = C \cdot E_n = C.$$

2.) Die Menge $\mathrm{GL}_n(K) := \{A \in \mathrm{M}(n \times n, K) \mid \det(A) \neq 0\}$ *ist bezüglich der Matrizenmultiplikation eine Gruppe, welche im Allgemeinen nicht abelsch ist.*

Beweis. (teilweise)

1.) Wir geben eine Möglichkeit an, mit welcher man B konstruiert, ohne Beweis. Sei $A = (a_{ji}) \in \mathrm{M}(n \times n, K)$ gegeben, dann bezeichnen wir für alle $p, q \in \{1, \ldots, n\}$ mit A^{pq} die $(n-1)\times(n-1)$-Matrix, welche aus A durch Entfernen der p-ten Zeile und der q-ten Spalte entsteht. Beispiel: $A = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$, dann ist $A^{12} = \begin{pmatrix} 0 & 2 \\ 0 & 1 \end{pmatrix}, A^{31} = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$ etc... Setze $\tilde{b}_{pq} := (-1)^{p+q} \cdot \det(A^{pq})$ (Achtung: Die Reihenfolge der Indizes p und q wurde vertauscht!) und definiere die $n \times n$-Matrix $\tilde{B} := \begin{pmatrix} \tilde{b}_{11} & \ldots & \tilde{b}_{1n} \\ \vdots & & \vdots \\ \tilde{b}_{n1} & \ldots & \tilde{b}_{nn} \end{pmatrix}$. Dann gilt

$$A \cdot \tilde{B} = \tilde{B} \cdot A \overset{!}{=} \begin{pmatrix} \det(A) & 0 & \ldots & 0 \\ 0 & \det(A) & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \ldots & 0 & \det(A) \end{pmatrix} = \det(A) \cdot E_n$$

(„$\overset{!}{=}$“ ohne Beweis). $\tilde{B}$ heißt die Komplementärmatrix von A. Falls also $\det(A) \neq 0$ ist, dann setzen wir $B := (\det(A))^{-1} \cdot \tilde{B} \Rightarrow A \cdot B = B \cdot A = E_n$.

2.) Die Eigenschaft G1) (Assoziativgesetz), also $(A \cdot B) \cdot C = A \cdot (B \cdot C)$, kann man mit der Definition 9.3 explizit beweisen (die auftretenden Indizes sind allerdings etwas kompliziert). Genauso zeigt man $\forall A \in \mathrm{M}(n \times n, K)$: $A \cdot E_n = E_n \cdot A = A$. Sei z. B. $A = (a_{ij})$, dann gilt: $A \cdot E_n = (c_{kl})$ mit $c_{kl} = \sum_{r=1}^{n} a_{kr} \cdot e_{rl}$ und $e_{rl} = \begin{cases} 1 & , r = l \\ 0 & , r \neq l \end{cases}$. Also $c_{kl} = a_{kl} \Rightarrow A \cdot E_n = A$. Damit ist E_n das neutrale Element bezüglich der Multiplikation und Axiom G2) gilt. Wie eben bewiesen, gibt es für alle $A \in \mathrm{GL}_n(K)$ ein $B \in \mathrm{M}(n \times n, K)$ mit $A \cdot B = B \cdot A = E_n$. Aus Satz 9.11 folgt dann $\det(A) \cdot \det(B) = \det(E_n)$, aber nach Definition 9.10 der Determinante ist $\det(E_n) = 1$, also $\det(B) = (\det(A))^{-1} \neq 0 \Rightarrow B \in \mathrm{GL}_n(K)$, also gilt G3).

□

Beispiel: Sei $A = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 3 & 2 \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{M}(3 \times 3, \mathbb{R})$ gegeben. Wir berechnen:

$$\det(A) = 1 \cdot 3 \cdot 1 + 2 \cdot 2 \cdot 0 + 1 \cdot 0 \cdot 0 - 0 \cdot 3 \cdot 1 - 0 \cdot 2 \cdot 1 - 1 \cdot 0 \cdot 2 = 3.$$

Also ist $A \in \mathrm{GL}_3(\mathbb{R})$. Wir berechnen die Komplementärmatrix, es ist $\tilde{b}_{11} = \det \begin{pmatrix} 3 & 2 \\ 0 & 1 \end{pmatrix} = 3$, $\tilde{b}_{21} = -\det \begin{pmatrix} 0 & 2 \\ 0 & 1 \end{pmatrix} = 0, \tilde{b}_{31} = \det \begin{pmatrix} 0 & 3 \\ 0 & 0 \end{pmatrix} = 0, \tilde{b}_{12} = -\det \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} = -2, \tilde{b}_{22} = \det \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = 1$, $\tilde{b}_{32} = -\det \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix} = 0, \tilde{b}_{13} = \det \begin{pmatrix} 2 & 1 \\ 3 & 2 \end{pmatrix} = 2 \cdot 2 - 3 \cdot 1 = 1, \tilde{b}_{23} = -\det \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} = -2, \tilde{b}_{33} = \det \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} = 3$, also ist

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

Es gilt

$$\begin{array}{c|c} & \begin{pmatrix} 1 & 2 & 1 \\ 0 & 3 & 2 \\ 0 & 0 & 1 \end{pmatrix} = A \\ \hline B = \begin{pmatrix} 1 & -\frac{2}{3} & \frac{1}{3} \\ 0 & \frac{1}{3} & -\frac{2}{3} \\ 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \end{array}$$

und analog $A \cdot B = E_3$.

Wir wollen ganz zum Abschluss noch eine Formel zur Lösung von quadratischen Gleichungssystemen angeben, und zwar für den Fall, dass es eine eindeutige Lösung gibt. Sei also eine erweiterte Koeffizientenmatrix $(A, b) \in \mathrm{M}(n \times (n+1), K)$ gegeben. Satz 9.12 sagt, dass eine eindeutige Lösung existiert, falls $\det(A) \neq 0$ ist.

Satz 9.14 (Cramersche Regel)**.** *Sei $(A, b) \in \mathrm{M}(n \times (n+1), K)$ mit $\det(A) \neq 0$ gegeben, dann ist der eindeutige Lösungsvektor $x \in \mathrm{M}(n \times 1, K)$ gegeben durch*

$$x = \frac{1}{\det(A)} \cdot \tilde{B} \cdot b.$$

Außerdem gilt: Sei $\forall i \in \{1, \ldots, n\}$ die Matrix A_i^b gegeben, indem man in A die i-te Spalte durch b ersetzt, dann ist $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ mit $x_i = \frac{\det(A_i^b)}{\det(A)}$.

Beweis. (teilweise)

$$Ax = b \Rightarrow A^{-1}Ax = x \overset{!}{=} A^{-1}b = (\det(A))^{-1}\tilde{B}b.$$

□