Lineare Algebra und Analytische Geometrie 1

Vorlesung Wintersemester

Prof. Meinolf Geck, Lehrstuhl für Algebra, Universität Stuttgart
https://pnp.mathematik.uni-stuttgart.de/idsr/idsr1/geckmf

Dies ist mein Skript zur Vorlesung Lineare Algebra und Analytische Geometrie 1 (V4Ü2, 15 Wochen). Eines der Hauptziele ist natürlich die Vermittlung von Grundwissen und Rechenfertigkeiten in einem zentralen Teilgebiet der Mathematik. Etwas genereller geht es auch um die Vermittlung einer mathematischen Denkweise. Dazu gehört es zu lernen, wie man mathematische Sachverhalte formal korrekt aufschreibt und diese beweist, also ihre Richtigkeit nach logischen Prinzipien herleitet. Dies sind übrigens Fähigkeiten, die sich auch in diversen anderen Situationen als sehr hilfreich erweisen! Außerdem sollen natürlich Beispiele für die Nützlichkeit von mathematischen Konzepten in Anwendungen gegeben werden.

Im Durchschnitt werden pro Woche etwa 7 Seiten dieses Skriptes behandelt. (In den einführenden Abschnitten am Anfang etwas mehr.)

Kommentare sehr willkommen! (Insbesondere Druckfehler, sonstige Unklarheiten, Verbesserungsvorschläge etc.)

Stuttgart, Oktober 2021

Ziele/Inhalt der Vorlesung

- **Lösen von linearen Gleichungssystemen:**

$$\begin{array}{rcrcrcl} x_1 & + & 3x_2 & - & 2x_3 & = & 1 \\ 2x_1 & + & 2x_2 & & & = & 2 \\ 4x_1 & + & 6x_2 & + & x_3 & = & 8 \end{array}$$

  (Anwendungen in Natur- und Ingenieurwissenschaften, ...)

- **Allgemeine Theorie der Vektorräume und linearen Abbildungen**
- **Hinführung auf neue Zahlsysteme und Strukturen:**
  Zum Beispiel "binäres" Zahlensystem $\{0,1\}$ mit $1+1=0$ ($\rightsquigarrow$ Informatik).
- **Die Kapitelüberschriften:**
  - Kapitel I: Grundlagen.
  - Kapitel II: Matrizen.
  - Kapitel III: Algebraischen Strukturen.
  - Kapitel IV: Vektorräume und lineare Abbildungen.
- **Modell für den axiomatischen Aufbau einer Theorie:**
  - Festlegung von grundlegenden Begriffen und Regeln ("Axiomen"), die als wahr vorausgesetzt werden.
  - Herleiten ("Beweisen") von Aussagen aus den Axiomen sowie bereits bewiesenen Aussagen nach bestimmten logischen Regeln.
  - Präzises Formulieren und Argumentieren.
    (Anwendungen im Studium und in allen späteren Berufen!)

  (Obiges gilt genauso für die Vorlesung Analysis I.)

- **"Axiom" für diese Vorlesung:**
  - Das Zahlensystem der ganzen Zahlen, also der Zahlen $0, \pm 1, \pm 2, \pm 3, \ldots$, sowie das Rechnen mit diesen Zahlen (Addition, Multiplikation) werden als bekannt vorausgesetzt. Ebenso das Rechnen mit rationalen Zahlen, also Brüchen $\pm n/m$ mit natürlichen Zahlen n, m.
  - Mengentheoretische Sprechweisen und Grundlagen aus der mathematischen Logik werden schrittweise eingeführt wenn sie gebraucht werden.

Literatur

Besonders geeignet für diese Vorlesung:

- S. Axler, Linear Algebra done right. Undergraduate texts in mathematics, Springer-Verlag, 2015.
- G. Fischer, Lineare Algebra: Eine Einführung für Studienanfänger, Vieweg + Teubner Verlag; 17. Auflage 2010.
- B. Huppert und W. Willems, Lineare Algebra: Mit zahlreichen Anwendungen in Kryptographie, Codierungstheorie, Mathematischer Physik und Stochastischen Prozessen, Vieweg + Teubner Verlag, 2. Auflage 2010.
- M. Koecher, Lineare Algebra und analytische Geometrie, Grundwissen Mathematik, Springer-Verlag, 4. Auflage, 2002.

Zum Auffrischen von Schulwisssen und Grundlagen:

- T. Glosauser, (Hoch)Schulmathematik, Ein Sprungbrett vom Gymnasium zur Uni. Springer-Spektrum, 2015.
- M. Liebeck, A Concise Introduction to Pure Mathematics. Chapman Hall/CRC Mathematics Series, CRC Press, 3rd edition 2010.
- MINT Kolleg Baden-Württemberg, Mathematik-Vorkurs (Online), siehe `http://www.mint-kolleg.de/stuttgart/angebote/online_kurse`

Frei verfügbare mathematische Software zum Ausprobieren/Experimentieren:

- GAP - Groups, Algorithms, and Programming, siehe `http://www.gap-system.org/` (Exaktes Rechnen mit Zahlen und diskreten algebraischen Strukturen.)
- SageMath, siehe `https://www.sagemath.org/` (Basiert auf der Programmiersprache Python; siehe `https://www.python.org/`)

Einige weiterführende Texte (Auswahl, wird laufend ergänzt):

- M. Artin, Algebra. Aus dem Englischen übersetzt von Annette A'Campo. Birkhäuser Verlag, 1993.
- N. L. Biggs, Discrete Mathematics, 2nd Edition. Oxford University Press, 2002.
- N. Bourbaki, Éléments de Mathématiques. Algèbre. Chap. 1 à 3, Masson, Paris, 1970; Chap. 4 à 7, Masson, Paris, 1981.

- J. G. Broida and S. Gill Williamson, Comprehensive Introduction to Linear Algebra, 2012; Web Version, Creative Commons CC0 1.0; see `https://cseweb.ucsd.edu/~gill/CILASite/`.
- H. D. Ebbinghaus, H. Hermes, F. Hirzebruch, M. Koecher, K. Mainzer, J. Neukirch, A. Prestel und R. Remmert, Zahlen. Grundwissen Mathematik, vol. 1, Springer-Verlag, Berlin, 1983.
- S. H. Friedberg, A. J. Insel und L. E. Spence, Linear Algebra, 4th ed., Pearson, 2002.
- P. R. Halmos, Naive Mengenlehre, Vandenhoeck & Ruprecht, 5. Auflage, 1994.
- F. Lorenz, Lineare Algebra, 2 Bände. Spektrum Akademischer Verlag; 1. Band, 4. Auflage 2008; 2. Band, 3. Auflage, 1992.
- D. Poole, Linear Algebra: A Modern Introduction. Brooks Cole Pub Co., 3. Auflage, 2010.
- D. Serre, Matrices: Theory and Applications. Graduate Texts in Mathematics 216, Springer-Verlag, 2. Auflage, 2010.

Inhaltsverzeichnis

Kapitel I: Grundlagen

Mathematik beruht auf den Grundpfeilern Mengenlehre und Logik. Wir können und wollen hier keine formale Einführung in die abstrakte Mengenlehre und mathematische Logik geben. (Dazu wäre eine eigene Vorlesung nötig, die auch in einem Mathematik-Studium oft erst später angeboten wird, wenn überhaupt.) Für den Anfang und die meisten Zwecke genügt es, sich auf einige grundlegende Sprech- und Schreibweisen zu verständigen, mit denen wir im weiteren Verlauf mathematische Sachverhalte präzise formulieren und beweisen können.

1. *Mengen und Aussagen*

Eine ***Menge*** ist für uns einfach eine Zusammenfassung von bestimmten Objekten, die als ***Elemente*** der Menge bezeichnet werden. Eine solche Zusammenfassung wird durch geschweifte Klammern $\{\ldots\}$ bezeichnet, zum Beispiel:

$$S = \{ \text{ alle Einwohner von Stuttgart } \},$$
$$\mathbb{N} = \{1, 2, 3, 4, \ldots\} \quad \text{die natürlichen Zahlen},$$
$$\mathbb{N}_0 = \{0, 1, 2, 3, 4, \ldots\} \quad \text{die natürlichen Zahlen mit } 0,$$
$$\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \ldots\} \quad \text{die ganzen Zahlen}.$$

Mengen können also nur eine bestimmte Anzahl von Elementen enthalten (wie im 1. Beispiel) oder auch unendlich viele Elemente (wie im 2., 3. und 4. Beispiel).

Schreibweisen:

"$a \in A$" bedeutet: Das Objekt a ist ein Element der Menge A;
analog bedeutet "$a \notin A$", dass a nicht zu A gehört.

"$A \subseteq B$" bedeutet: Die Menge A ist eine Teilmenge der Menge B, und dies wiederum bedeutet, dass jedes Element von A auch ein Element von B ist.

"$A = B$" bedeutet: Die Menge A enthält die gleichen Elemente wie die Menge B, oder anders ausgedrückt: Es gilt $A \subseteq B$ und $B \subseteq A$.

Zum Beispiel gilt $-5 \notin \mathbb{N}$ und $\mathbb{N} \subseteq \mathbb{Z}$. Ist $A \subseteq B$ und $A \neq B$, so schreiben wir $A \subsetneq B$.

Das Symbol "$\varnothing$" steht für die ***leere Menge***, also die Menge, die überhaupt kein Element enthält. Wir können dies auch mit $\{\}$ bezeichnen. Es gilt $\varnothing \subseteq A$ für jede Menge A.

Unter einer ***Aussage*** verstehen wir einen Satz (auf deutsch, englisch oder in sonst irgendeiner Zeichensprache), der entweder wahr oder falsch ist.

BEISPIEL: Der Satz "Der 19.10.2021 ist ein Dienstag" ist eine wahre Aussage. Aber der Satz "Bitte stellen Sie Fragen, wenn etwas nicht klar ist" ist keine Aussage.

Natürlich ist ein in der mathematischen Zeichensprache verfasster Satz wie "$1+1=3$" eine Aussage, die in diesem Fall falsch ist.

Beachte: Es kann dabei sein, dass wir vielleicht nicht wissen, ob die fragliche Aussage nun wahr oder falsch ist, oder dass es extrem schwierig ist, die Antwort zu finden; es kommt nur darauf an, dass etwas gesagt wird, das entweder wahr oder falsch ist. – Beispiele:

- "Es gibt Außerirdische".
- $2^{277232917}-1$ (eine Zahl mit 23249425 Ziffern) ist eine Primzahl.

Mengenbildung mit Aussagen: Gegeben sei eine Menge A und, für jedes $a \in A$, eine Aussage $P(a)$. Dann können wir die Menge aller derjenigen $a \in A$ bilden, für die $P(a)$ wahr ist, und dies ist eine Teilmenge von A; in Zeichen:

$$\{a \in A \mid P(a) \text{ ist wahr}\} \subseteq A.$$

BEISPIEL: Sei A die Menge aller Anwesenden im Hörsaal V47.01. Für jedes $a \in A$ sei $P(a)$ die Aussage: "a trägt einen blauen Pullover". Dann ist also $\{a \in A \mid P(a) \text{ ist wahr}\}$ genau die Menge der hier Anwesenden, die einen blauen Pullover tragen.

Hier sehen wir auch die Nützlichkeit der leeren Menge: Trägt nämlich niemand einen blauen Pullover, so ist $\{a \in A \mid P(a) \text{ ist wahr}\} = \varnothing$.

BEISPIEL: Sei $A = \mathbb{N}$ und $P(n)$ die Aussage: "n ist eine gerade Zahl". Dann ist also

$$\{n \in A \mid P(n) \text{ ist wahr}\} = \{2,4,6,8,\ldots\}$$

die Menge der geraden Zahlen.

Beachten Sie: Es ist offenbar egal, ob wir $P(a)$ oder $P(n)$ schreiben, denn das Symbol "a" bzw. "n" ist hier ja nur ein Platzhalter (also so etwas wie eine lokale Variable beim Programmieren), der auf ein Element von A verweist.

Sei nun $Q(n)$ die Aussage: "$P(n)$ ist falsch". Dann ist

$$\{n \in A \mid Q(n) \text{ ist wahr}\} = \{n \in A \mid P(n) \text{ ist falsch}\} = \{1,3,5,7,\ldots\}$$

die Menge der ungeraden Zahlen.

Verknüpfung von Aussagen.

Ist P eine Aussage, so wird mit $\neg P$ die Negation von P bezeichnet.

Beispiel: Ist P : "Heute ist Dienstag", so ist $\neg P$ die Aussage "Heute ist nicht Dienstag".

Sind P und Q Aussagen, so erhalten wir neue Aussagen durch folgende Verknüpfungen:

"$P \vee Q$" ist die Aussage: "P ist wahr oder Q ist wahr oder beide sind wahr."

"$P \wedge Q$" ist die Aussage: "P ist wahr und Q ist wahr."

"$P \Rightarrow Q$" ist die Aussage: "Aus P folgt Q" oder anders ausgedrückt: "Wann immer P wahr ist, so muss auch Q wahr sein."

Es ist manchmal nützlich, diese Verknüpfungen durch ***Wahrheitstabellen*** zu beschreiben, die angeben, welchen Wahrheitswert die Verknüpfung in Abhängigkeit von den möglichen Kombinationen der Wahrheitswerte von P und Q hat, also etwa:

P	$\neg P$
1	0
0	1

P	Q	$P \vee Q$	$P \wedge Q$	$P \Rightarrow Q$
1	1	1	1	1
1	0	1	0	0
0	1	1	0	1
0	0	0	0	1

(wobei 1 für "wahr" steht und 0 für "falsch"). Vielleicht kommt Ihnen die letzte Spalte etwas ungewohnt vor! Dazu beachten Sie, dass aus falschen Aussagen durchaus wahre Aussagen gefolgert werden können; es geht ja nur darum, dass die Folgerung als solche korrekt ist.

Beispiel: Für $a, b \in \mathbb{Z}$ ist die folgende Verknüpfung eine wahre Aussage:

$$a = b \quad \Rightarrow \quad a^2 = b^2.$$

Beweis: Wenn $a = b$ gilt, so können wir im Produkt $a^2 = a \cdot a$ beide Faktoren durch b ersetzen und erhalten $b \cdot b = b^2$, also die rechte Seite.

Nehmen wir konkret $a = 2$ und $b = -2$, so ist "$a = b$" falsch, aber "$a^2 = b^2$" wahr; nehmen wir $a = 2$ und $b = 3$, so ist "$a = b$" falsch und auch "$a^2 = b^2$" falsch. Aber der obige Beweis ist natürlich immer richtig, egal in welcher Beziehung a und b zueinander stehen.

Das Beispiel $a = 2$, $b = -2$ zeigt auch, dass die Umkehrung "$a^2 = b^2 \Rightarrow a = b$" falsch ist.

Allgemein sagen wir, dass P und Q ***äquivalente Aussagen*** sind (in Zeichen: "$P \Leftrightarrow Q$"), wenn sowohl "$P \Rightarrow Q$" als auch "$Q \Rightarrow P$" wahr sind.
Wir drücken dies auch so aus, dass P genau dann gilt, wenn Q gilt.

Mit Hilfe der Werte in den entsprechenden Wahrheitstabellen stellen Sie sofort fest:

- "$P \Leftrightarrow Q$" ist äquivalent zu: Entweder P, Q beide wahr oder beide falsch.
- "$P \Rightarrow Q$" ist äquivalent zu: "$(\neg P) \vee Q$".
- "$P \Rightarrow Q$" ist auch äquivalent zu: "$(\neg Q) \Rightarrow (\neg P)$".

Letztere Verknüpfung heißt ***Kontraposition***.

Weitere Konstruktionen zum Bilden neuer Mengen: Seien A, B zwei Teilmengen einer Menge M. Dann ist die ***Durchschnittsmenge*** von A und B ist definiert durch

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

dieser besteht also genau aus den Elementen, die sowohl in A als auch in B enthalten sind.

Hierbei (und auch sonst in diesem Skript) steht der Doppelpunkt in ":=" für eine Definition: Es wird keine Gleichheit behauptet, sondern das Symbol "$A \cap B$" ist lediglich ein Name für die Menge auf der rechten Seite.

Die ***Vereinigungsmenge*** von A und B ist definiert als

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

diese besteht also genau aus den Elementen, die in A oder in B enthalten sind (oder sowohl in A als auch in B). Das ***Komplement*** von B in A bezeichnet ist definiert als

$$A \setminus B := \{x \in A \mid x \notin B\} \qquad \text{(oft auch } A^c \text{ geschrieben)}.$$

Schließlich können wir zu jeder Menge A auch ihre ***Potenzmenge*** $\mathcal{P}(A)$ bilden, d.h., die Menge aller Teilmengen von A.

Zum Beispiel besteht die Potenzmenge von $A = \{1, 2, 3\}$ aus 8 Elementen:

$$\mathcal{P}(A) = \{\varnothing,\ \{1\},\ \{2\},\ \{3\},\ \{1, 2\},\ \{1, 3\},\ \{2, 3\},\ \{1, 2, 3\}\}.$$

Hier gilt dann etwa $\{1, 2\} \in \mathcal{P}(A)$ und $\{\varnothing, \{1\}\} \subseteq \mathcal{P}(A)$, d.h., Mengen können auch selbst wieder Elemente von anderen Mengen sein.

Ein etwas komplexeres Beispiel: Sei A eine nicht-leere Menge und B eine beliebige Teilmenge von $\mathcal{P}(A)$, d.h., B ist eine Menge von Teilmengen von A. Dann können wir die Vereinigung aller $X \in B$ bilden.

Dies wird mit obigen Mengenbildungsprinzipien wie folgt begründet. Betrachte für $a \in A$ die Aussage $P(a)$: "Es gibt ein $X \in B$ mit $a \in X$".

Dann ist $\displaystyle\bigcup_{X \in B} X := \{a \in A \mid \text{es gibt ein } X \in B \text{ mit } a \in X\}$

Konkretes Beispiel: A = Menge aller Menschen auf der Erde.

$$B = \Big\{ \{\text{Menschen in Deutschland}\},\ \{\text{Menschen in Frankreich}\},$$
$$\{\text{Menschen in Polen}\},\ \ldots \text{usw. für alle (nur noch) 27 Länder der EU} \Big\}.$$

Dann ist $\displaystyle\bigcup_{X \in B} X = \{\text{alle Menschen in der EU}\}.$

Quantoren: Dies sind die mathematischen Kurzzeichen $\exists$, welches für "es existiert" steht, und $\forall$, welches für "für alle" steht. Beispiele:

Die Aussage "Es gibt eine natürliche Zahl n mit $n^3 = 8$" lässt sich kurz schreiben als: $\exists n \in \mathbb{N} : n^3 = 8$.

Die Aussage "Das Quadrat einer beliebigen ganzen Zahl ist entweder 0 oder positiv" lässt sich kurz schreiben als: $\forall n \in \mathbb{Z} : n^2 \geqslant 0$.

Etwas formaler: Gegeben sei eine Menge A und, für jedes $a \in A$, eine Aussage $P(a)$.

"$\forall a \in A : P(a)$" bedeutet, dass die Aussage $P(a)$ für alle $a \in A$ wahr ist.

"$\exists a \in A : P(a)$" bedeutet, dass es (mindestens) ein $a \in A$ gibt, für welches $P(a)$ wahr ist.

Für die Negation von Aussagen mit Quantoren gilt:

$$\neg\big(\forall a \in A : P(a)\big) \Leftrightarrow \exists\, a \in A : \neg P(a) \quad \text{und} \quad \neg\big(\exists\, a \in A : P(a)\big) \Leftrightarrow \forall a \in A : \neg P(a)$$

Im Prinzip sollte man sämtliche mathematischen Aussagen in dieser Vorlesung in einer Formelsprache ausdrücken können, in denen nur Aussagen über Elemente in Mengen, Verknüpfungen von Aussagen und Quantoren vorkommen. Aber bei komplizierteren Sachverhalten wird man der besseren Verständlichkeit halber stets versuchen, diese Sachverhalte so weit wie möglich in "normalen", möglichst einprägsamen Sätzen auszudrücken.

Schließlich erwähnen wir hier nur, dass man in logische Schwierigkeiten geraten kann, wenn man die obigen Mengenbildungsprinzipien verlässt. Berühmtes Beispiel ist die ***Russell'sche Antinomie***; siehe dazu `https://en.wikipedia.org/wiki/Russell's_paradox`. Man kann so etwas auch in der Umgangssprache formulieren:

"*Definieren wir einen Barbier als jemanden, der all jene und nur jene rasiert, die sich nicht selbst rasieren. Frage: Rasiert der Barbier sich selbst?*"

Nimmt man an, er rasiert sich selbst, so erhält man einen Widerspruch; aber ebenso, wenn man annimmt, er rasiert sich nicht selbst ...

2. *Beweistechniken und elementare Arithmetik*

Wir stellen grundlegende Beweistechniken vor und illustrieren diese durch einige Beispiele, in denen wichtige Aussagen über ganze Zahlen (die zum Teil bereits aus der Schule vertraut sein mögen) mathematisch korrekt hergeleitet werden. Dabei setzen wir lediglich die Kenntnis der Grundrechenarten für natürliche und ganze (und später auch rationale) Zahlen voraus.

Definition 2.1. Seien $n, m \in \mathbb{Z}$. Wir schreiben $n \mid m$ und sagen "n teilt m" oder "m ist ein Vielfaches von n", wenn es ein $a \in \mathbb{Z}$ gibt mit $m = a \cdot n$.

Beispiele: $2 \mid 6$ (denn $6 = 3 \cdot 2$), $5 \mid 0$ (denn $0 = 0 \cdot 5$) und $3 \nmid 10$ (denn die positiven Vielfachen von 3 sind $3, 6, 9, 12, \ldots$).

Lemma 2.2 (oder auch "Hilfssatz")**.**
(a) *Seien* $n, m, k \in \mathbb{Z}$. *Gilt* $n \mid m$ *und* $m \mid k$, *so auch* $n \mid k$.
(b) *Seien* $n, m, k \in \mathbb{Z}$ *und* $a, b \in \mathbb{Z}$. *Gilt* $n \mid m$ *und* $n \mid k$, *so auch* $n \mid (a \cdot m + b \cdot k)$.

Beweis. Dies ist ein Beispiel eines "Routine-Beweises", wo es darum geht, die Richtigkeit von vorgegebenen Formeln durch einfaches Nachrechnen zu bestätigen.

(a) Nach Voraussetzung gibt es $a, b \in \mathbb{Z}$ mit $m = a \cdot n$ und $k = b \cdot m$. Dann ist $k = b \cdot m = b \cdot (a \cdot n) = (b \cdot a) \cdot n$. (Hier haben wir benutzt, dass man Produkte von ganzen Zahlen beliebig klammern darf.) Setzen wir $c = b \cdot a \in \mathbb{Z}$, so gilt also $k = c \cdot n$ und damit $n \mid k$.

(b) Voraussetzung ist: $n \mid m$ und $n \mid k$. Also gibt es $u, v \in \mathbb{Z}$ mit $m = u \cdot n$ und $k = v \cdot n$. Dann ist

$$a \cdot m + b \cdot k = a \cdot (u \cdot n) + b \cdot (v \cdot n) = (a \cdot u) \cdot n + (b \cdot v) \cdot n = (a \cdot u + b \cdot v) \cdot n.$$

(Hier haben wir wiederum benutzt, dass man Produkte beliebig klammern darf; außerdem haben wir eine Distributivregel verwendet, die besagt, dass man in einer Summe von zwei Produkten gemeinsame Faktoren ausklammern darf.) Setzen wir $c = a \cdot u + b \cdot v \in \mathbb{Z}$, so gilt also $a \cdot m + b \cdot k = c \cdot n$ und damit $n \mid (a \cdot m + b \cdot k)$. $\square$ ($\leftarrow$ zeigt Ende des Beweises an)

Im Folgenden werden wir nicht mehr explizit wie im obigen Beweis erwähnen, wenn wir eine der üblichen Regeln beim Rechnen mit ganzen Zahlen verwenden. Außerdem lassen wir den Punkt bei der Multiplikation der besseren Lesbarkeit wegen einfach weg.

Lemma 2.3. (a) *Ist* $n \in \mathbb{N}_0$ *ungerade, so ist auch* n^2 *ungerade.*
(b) *Ist* $n \in \mathbb{N}_0$ *so dass* n^2 *gerade ist, so ist auch* n *selbst gerade.*

Beweis. (a) Da n ungerade ist, gilt $n = 2m + 1$ mit einem $m \in \mathbb{N}_0$. Damit erhalten wir $n^2 = (2m+1)^2 = 4m^2 + 4m + 1 = 2(2m^2 + 2m) + 1$. Setzen wir $k = 2m^2 + 2m \in \mathbb{N}_0$, so gilt also $n^2 = 2k + 1$, d.h., n^2 ist auch ungerade.

(b) Folgt sofort aus (a) durch "Kontraposition". Sei P die Aussage "n ist ungerade" und Q die Aussage "n^2 ist ungerade". In (a) wurde gezeigt, dass "$P \Rightarrow Q$" gilt. Kontraposition bedeutet, dass dann auch "$(\neg Q) \Rightarrow (\neg P)$" gilt, also genau die Aussage in (b). □

Lemma 2.4 (Kürzungsregel)**.** *Seien* $n, m, k \in \mathbb{Z}$*. Gilt* $k \neq 0$ *und* $kn = km$*, so folgt* $n = m$*.*

Beweis. Wir betrachten die Aussagen P: "$kn = km$" und Q: "$n = m$".
Um "$P \Rightarrow Q$" zu zeigen, können wir auch genauso gut "$(\neg Q) \Rightarrow (\neg P)$" zeigen.

Nehmen wir also an, es gelte $\neg Q$, d.h., es sei $n \neq m$. Dann ist $n - m \neq 0$ und $k(n - m) \neq 0$ (weil das Produkt von zwei ganzen Zahlen ungleich 0 wieder ungleich 0 ist). Nun ist $kn - km = k(n - m) \neq 0$ also folgt $kn \neq km$, d.h., $\neg P$. □

Beweise durch Kontraposition werden auch oft als "Widerspruchsbeweise" dargestellt. Man nimmt dazu an, dass die gewünschte Aussage falsch ist, und leitet dann daraus einen Widerspruch ab (d.h., eine Aussage, von der wir bereits wissen, dass sie falsch ist). Per Kontraposition ist damit die gewünschte Aussage wahr. — Mehr Beispiele später ...

Satz 2.5. *Sei* $n \in \mathbb{N}$*. Dann gilt* $1 + 2 + 3 + \cdots + n = \frac{1}{2}n(n + 1)$*.*

Beweis. Dies ist ein Beispiel eines Beweises, bei dem es nicht nur um routine-mässiges Nachrechnen geht, sondern irgendeine Idee oder ein Trick verwendet werden muss.

Zum Umgang mit Summen führen wir zunächst die allgemeine Summenschreibweise ein: Sind $a_1, \ldots, a_n$ ganze Zahlen, so schreiben wir: $a_1 + a_2 + \ldots + a_n = \sum_{i=1}^{n} a_i$.

Mit $a_i = i$ für $i = 1, \ldots, n$ wollen wir also eine Formel für folgende Summe finden:

$$S := 1 + 2 + \ldots + n = \sum_{i=1}^{n} i.$$

Der "Trick" dieses Beweises besteht nun darin, auszunutzen, dass man die Reihenfolge in einer Summe von ganzen Zahlen beliebig ändern kann. Also gilt auch $S = n + (n-1) + \ldots + 2 + 1$. Der i-te Term in dieser Summe ist gegeben durch $b_i = n + 1 - i$; damit erhalten wir

$$S = \sum_{i=1}^{n} b_i = \sum_{i=1}^{n} (n + 1 - i).$$

Nun bilden wir
$$\begin{aligned} 2S = S + S &= (a_1 + a_2 + \ldots + a_n) + (b_1 + b_2 + \ldots + b_n) \\ &= (a_1 + b_1) + (a_2 + b_2) + \ldots + (a_n + b_n) \qquad \text{(noch einmal der Trick!)} \\ &= \sum_{i=1}^{n} (a_i + b_i) = \sum_{i=1}^{n} \big(i + (n + 1 - i)\big) = \sum_{i=1}^{n} (n + 1) = n(n + 1). \end{aligned}$$

Damit ist $2S = n(n + 1)$, also $S = \frac{1}{2}n(n + 1)$, wie gewünscht. □

Ab hier Woche 2

Die folgende Eigenschaft von $\mathbb{N}_0$ erscheint intuitiv einsichtig; sie wird explizit als "Axiom" formuliert, damit wir darauf verweisen und präzise damit argumentieren können.

Axiom 2.6 (***Peano's Induktionsaxiom***)**.** *Jede nicht-leere Teilmenge von* $\mathbb{N}_0$ *besitzt ein kleinstes Element. Oder, anders ausgedrückt mit Hilfe der Formelsprache in §1:*

$$\forall\, A \in \mathcal{P}(\mathbb{N}_0): \quad A \neq \varnothing \quad \Rightarrow \quad \big(\exists\, a \in A: \quad \big(\forall\, b \in A: a \leqslant b\big)\big).$$

Zur Erinnerung: natürliche und ganze Zahlen sind angeordnet

$$\ldots < -4 < -3 < -2 < -1 < 0 < 1 < 2 < 3 < 4 < \ldots$$

Formal: Für $a, b \in \mathbb{Z}$ gilt $a \leqslant b$, wenn es ein $c \in \mathbb{N}_0$ gibt mit $b = a + c$.

Zum Beispiel gilt $kn \geqslant n$ für alle $k, n \in \mathbb{N}$.
(Denn: Ist $k \in \mathbb{N}$, so ist $k - 1 \geqslant 0$ und damit $kn = n + \underbrace{(k-1)n}_{\geqslant 0} \geqslant n$.)

Als erste Anwendung des obigen Axioms zeigen wir folgende Aussage:

Satz 2.7 (Teilen mit Rest)**.** *Sei* $n \in \mathbb{Z}$ *und* $m \in \mathbb{N}$*. Dann gibt es* $q, r \in \mathbb{Z}$ *mit* $n = qm + r$ *und* $0 \leqslant r < m$*. Hier sind* q, r *eindeutig bestimmt. (Ist* $n \geqslant 0$*, so auch* $q \geqslant 0$*.)*

Ist $n = qm + r$ wie oben, so wird der "Rest" r auch mit $n \bmod m$ bezeichnet. Diese "mod" Funktion ist eine grundlegende arithmetische Operation; es gibt sie auch in den meisten modernen Programmierspachen, zum Beispiel `17 % 5` in Python oder C.

Beispiel. Für die Division von 17 mit Rest durch 5 erhalten wir:

$$17 = 3 \cdot 5 + 2, \qquad \text{also} \quad q = 3 \text{ und } r = 2 \quad \rightsquigarrow \quad 17 \bmod 5 = 2.$$

(Dazu zieht man so lange 5 von 17 ab, bis noch etwas $\geqslant 0$ herauskommt.)
Für die Division von -17 mit Rest durch 5 erhalten wir:

$$-17 = (-4) \cdot 5 + 3, \qquad \text{also} \quad q = -4 \text{ und } r = 3 \quad \rightsquigarrow \quad -17 \bmod 5 = 3.$$

(Dazu addiert man so lange 5 zu -17, bis man eine Zahl $\geqslant 0$ erhält.)

Dieses "so lange ... bis" scheint intuitiv klar. Typischerweise benötigt man allerdings das Peano Axiom für einen formalen Beweis. Wir führen dies hier einmal explizit aus.

Beweis von Satz 2.7. Sei zuerst $n \geqslant 0$. Dann betrachten wir die Menge

$$A := \{r \in \mathbb{N}_0 \mid \exists\, q \in \mathbb{N}_0: \; r = n - qm\}.$$

Diese Menge ist nicht leer, denn z.B. können wir $q = 0$ setzen und erhalten $r = n - 0 \cdot m = n \in A$. Nach Peano besitzt A also ein kleinstes Element; sei dieses r_0. Dazu gibt es ein $q_0 \in \mathbb{N}_0$ mit $r_0 = n - q_0 m$. Es gilt also $n = q_0 m + r_0$ und $r_0 \geqslant 0$.

Wir müssen noch zeigen, dass auch $r_0 < m$ gilt. Annahme, es wäre $r_0 \geqslant m$. Dann ist aber

$$r := n - (q_0 + 1)m = n - q_0 m - m = r_0 - m \geqslant 0, \qquad \text{also auch } r \in A.$$

Aber $r = r_0 - m < r_0$, und damit Widerspruch dazu, dass r_0 das kleinste Element von A ist. Also war die Annahme falsch, d.h., es gilt $n = q_0 m + r_0$ mit $q_0, r_0 \in \mathbb{N}_0$ und $0 \leqslant r_0 < m$.

Sei nun $n < 0$. Dann ist $-n > 0$, also wissen wir bereits, dass es $q_1, r_1 \in \mathbb{Z}$ gibt mit $-n = q_1 m + r_1$ und $0 \leqslant r_1 < m$. Dann ist $n = (-q_1)m - r_1$. Ist $r_1 = 0$, so sind wir fertig (mit $q := -q_1$ und $r := r_1 = 0$). Ist $r_1 \geqslant 1$, so erhalten wir

$$n = (-q_1)m - r_1 = (-q_1)m - m + m - r_1 = (-q_1 - 1)m + (m - r_1).$$

Mit $q := -q_1 - 1$ und $r := m - r_1$ ist $n = qm + r$ und $1 \leqslant r < m$, wie gewünscht.

Nur zur Eindeutigkeit von q, r: Es gelte also auch $n = q'm + r'$ mit $q', r' \in \mathbb{Z}$ und $0 \leqslant r' < m$. Behauptung: $q = q'$. Annahme, dies wäre falsch, also $q \neq q'$, d.h., $q < q'$ oder $q > q'$. Sei zuerst $q < q'$. Dann ist $q' - q > 0$ und damit $(q' - q)m \geqslant m$. Mit $qm + r = n = q'm + r'$ folgt auch $r - r' = q'm - qm = (q' - q)m \geqslant m$. Andererseits ist $r - r' \leqslant r < m$, Widerspruch. Analog erhält man einen Widerspruch für $q > q'$. Also war die Annahme falsch, d.h., es gilt $q = q'$ und damit auch $r = n - qm = n - q'm = r'$. □

Beispiel 2.8. Eine Anwendung: Prüfziffern bei IBAN

(Siehe `https://de.wikipedia.org/wiki/Internationale_Bankkontonummer`)

(Deutsche) Konto-Nr. 0356843503
Bankleitzahl (BLZ) 37010050

$\rightsquigarrow$ IBAN: DE12 $\underbrace{37010050}_{\text{BLZ}}\underbrace{0356843503}_{\text{Konto-Nr.}}$

"DE" steht für das Land, die "Prüfziffer" 12 wird nach folgendem Verfahren berechnet:

- Schreibe BLZ, gefolgt von Konto-Nr., Land und 00: 370100500356843503DE00.
- Wandle Buchstaben in Zahlen um:

A	B	C	D	...	Z
10	11	12	13	...	35

- Berechne $370100500356843503\underline{131400} \bmod 97 = 86$; ziehe dies von 98 ab; Ergebnis ist 12. (Falls Ergebnis einstellig, ergänze führende Null.)

Weiteres Beispiel: Formeln zur Berechnung des Osterdatums $\rightsquigarrow$ Übung 2.

Zurück zur allgemeinen Theorie. Seien $d, n \in \mathbb{Z}$ gegeben mit $d \neq 0$ und $n \neq 0$. Gilt $d \mid n$, so folgt natürlich auch $(-d) \mid n$. Um alle Teiler d von n zu bestimmen, brauchen wir also nur den Fall $d > 0$ zu betrachten. Sei nun $d > 0$. Aus $d \mid n$ folgt offenbar auch $d \leqslant |n|$ (= Absolutbetrag von n); also hat n nur endlich viele Teiler. Sind $n, m \in \mathbb{Z}$ mit $n \neq 0$ oder $m \neq 0$ gegeben, so definieren wir

$$\mathrm{ggT}(n, m) := \max\{a \in \mathbb{N} \mid a \text{ teilt } n \text{ und } a \text{ teilt } m\} \quad \text{"}\textbf{\textit{größter gemeinsamer Teiler}}\text{"}.$$

Gilt $\mathrm{ggT}(n, m) = 1$, so bezeichnen wir m und n als ***teilerfremd***.

Lemma 2.9 (Lemma von Bézout)**.** *Gegeben seien* $n, m \in \mathbb{Z}$ *mit* $n \neq 0$ *oder* $m \neq 0$*. Dann gibt es* $a, b \in \mathbb{Z}$ *mit* $\mathrm{ggT}(n, m) = an + bm$*. Ist auch* $d' \in \mathbb{Z}$ *ein gemeinsamer Teiler von* n *und* m*, so folgt* $d' \mid \mathrm{ggT}(n, m)$*.*

Beweis. Ist $n = 0$ oder $m = 0$, so ist die Aussage sehr einfach zu sehen. (Ist z.B. $n = 0$ und $m < 0$, so ist $-m = \mathrm{ggT}(n, m) = 0 \cdot n + (-1) \cdot m$.) Sei also jetzt $n \neq 0$ und $m \neq 0$. Wir beschreiben einen Algorithmus, genannt (erweiterter) ***Euklidischer Algorithmus***, zur Bestimmung von $\mathrm{ggT}(n, m)$ und $a, b \in \mathbb{Z}$ mit $\mathrm{ggT}(n, m) = an + bm$. Dazu berechnen wir rekursiv eine endliche Folge von Tripeln (r_k, a_k, b_k) für $k = 0, 1, 2, 3, \ldots$, wie folgt. Ist $n > 0$ und $m > 0$, so initialisieren wir $r_0 := n,\ a_0 := 1,\ b_0 := 0$ und $r_1 := m,\ a_1 := 0,\ b_1 := 1$. (Ist $n < 0$, so setze $r_0 := -n, a_0 := -1, b_0 := 0$; ist $m < 0$, so setze $r_1 := -m$, $a_1 := 0$, $b_1 := -1$.) In jedem Fall gilt dann $r_0 = a_0 n + b_0 m \geqslant 1$ und $r_1 = a_1 n + b_1 m \geqslant 1$. Sei nun $k \geqslant 1$ und r_i, a_i, b_i bereits konstruiert für $0 \leqslant i \leqslant k$, wobei jeweils $r_i = a_i n + b_i m \geqslant 1$ gelte. Division mit Rest liefert

$$r_{k-1} = q_k r_k + r_{k+1} \qquad \text{mit} \qquad q_k, r_{k+1} \in \mathbb{Z} \quad \text{und} \quad 0 \leqslant r_{k+1} < r_k;$$

dies definiert r_{k+1}; dann setze $a_{k+1} := a_{k-1} - q_k a_k$ und $b_{k+1} := b_{k-1} - q_k b_k$. Damit gilt wieder

$$r_{k+1} = r_{k-1} - q_k r_k = (a_{k-1} n + b_{k-1} m) - q_k (a_k n + b_k m) = a_{k+1} n + b_{k+1} m.$$

Dieses Verfahren wird so lange fortgesetzt, bis $r_{k+1} = 0$ gilt. (Wegen $r_1 > r_2 > \ldots \geqslant 0$ muss es ein solches k geben. Hier ist wieder ein solcher Fall von "so lange ... bis"; überlegen Sie sich selbst, wie man dies hier mit Hilfe des Peano Axioms formal rechtfertigt.) Dann ist $r_k > 0$ und $r_{k-1} = q_k r_k$. Im vorherigen Schritt ist $r_{k-2} = q_{k-1} r_{k-1} + r_k$; wegen $r_k \mid r_{k-1}$ folgt also auch $r_k \mid r_{k-2}$. Dies setzt sich entsprechend in alle vorherigen Schritte fort, also gilt $r_k \mid r_i$ für $0 \leqslant i \leqslant k-1$. Insbesondere ist $r_k \mid n = \pm r_0$ und $r_k \mid m = \pm r_1$, also $r_k \leqslant \mathrm{ggT}(n, m)$. Wegen $r_k = a_k n + b_k m$ folgt aber auch $d \mid r_k$ für jeden gemeinsamen Teiler d von n und m. Also ist $\mathrm{ggT}(n, m) = r_k = a_k n + b_k m$. (Für mehr Details siehe `https://en.wikipedia.org/wiki/Extended_Euclidean_algorithm`). □

Sei zum Beispiel $n = 1071$ und $m = 462$. Dann initialisieren wir $r_0 = 1071$, $a_0 = 1$, $b_0 = 0$ und $r_1 = 462$, $a_1 = 0$, $b_1 = 1$. Das obige Verfahren liefert nun nacheinander:

$$\begin{aligned}
r_0 &= 1071 = 2 \cdot 462 + 147 = q_1 r_1 + r_2, && \text{also } q_1 = 2,\ r_2 = 147 \text{ und } a_2 = 1,\ b_2 = -2,\\
r_1 &= \ \ 462 = 3 \cdot 147 + 21 \ \ = q_2 r_2 + r_3, && \text{also } q_2 = 3,\ r_3 = 21 \ \ \text{und } a_3 = -3,\ b_3 = 7,\\
r_2 &= \ \ 147 = 7 \cdot 21 + 0 \ \ \ \ = q_3 r_3 + r_4, && \text{also } q_3 = 7,\ r_4 = 0.
\end{aligned}$$

Damit bricht das Verfahren bei $k = 3$ mit $r_3 = 21$, $a_3 = -3$, $b_3 = 7$ ab und wir erhalten $21 = \mathrm{ggT}(1071, 462) = (-3) \cdot 1071 + 7 \cdot 462$. Versuchen Sie, dieses Verfahren möglichst effizient zu programmieren (in Python oder einer beliebigen anderen Programmiersprache).

Als nächstes betrachten wir die ***rationalen Zahlen*** $\mathbb{Q}$. Zur Erinnerung:

- Jedes $x \in \mathbb{Q}$ lässt sich schreiben als Bruch $x = n/m$ mit $n \in \mathbb{Z}$ und $m \in \mathbb{N}$.
- Zwei solche Brüche n/m und n'/m' sind gleich, wenn es ein $k \in \mathbb{N}$ gibt mit $n' = kn$ und $m' = km$, d.h., n/m entsteht aus n'/m', indem der Faktor k im Zähler und im Nenner gekürzt wird. (Beispiel: $x = 2/3 = 4/6 = 100/150$.)
- Ist $x = n/m \in \mathbb{Q}$ und teilt man den Zähler und Nenner durch $\mathrm{ggT}(n, m)$, so erhält man einen "gekürzten" Bruch $x = n'/m'$ mit $n' \in \mathbb{Z}$, $m' \in \mathbb{N}$ und $\mathrm{ggT}(n', m') = 1$. (Im Beispiel oben ist $2/3$ gekürzt, $4/6$ und $100/150$ sind nicht gekürzt.)
- Sei $x \in \mathbb{Q}$. Wir schreiben $x \geqslant 0$, falls $x = n/m$ mit $n \in \mathbb{N}_0$ und $m \in \mathbb{N}$.
  Sind $x, y \in \mathbb{Q}$, so schreibe $x \leqslant y$ falls $y - x \geqslant 0$ $\quad\rightsquigarrow\quad$ Anordnung von $\mathbb{Q}$.

Hier ist nun das klassische Beispiel eines Widerspruchsbeweises.

Satz 2.10 (Euklid, etwa 3. Jahrhundert v. Chr.)**.** *Es gibt keine positive rationale Zahl* $x \in \mathbb{Q}$ *mit* $x^2 = 2$.

Beweis. Nehmen wir an, es gibt doch ein $x \in \mathbb{Q}$ mit $x > 0$ und $x^2 = 2$. Wir versuchen, einen Widerspruch zu einer bekannten Aussage zu produzieren.

Wir nehmen eine gekürzte Bruchdarstellung $x = n/m$ mit $n, m \in \mathbb{N}$. Dann ist $2 = x^2 = (n/m)^2 = n^2/m^2$. Multiplizieren auf beiden Seiten mit m^2 ergibt $2m^2 = n^2$. Nun ist $2m^2$ gerade, also auch n^2. Mit Lemma 2.3(b) folgt, dass n auch selbst gerade ist, also gilt $n = 2l$ mit einem $l \in \mathbb{N}$. Dann ist aber $2m^2 = n^2 = (2l)^2 = 4l^2$. Hier können wir eine 2 auf beiden Seiten kürzen (siehe Lemma 2.4) und erhalten $m^2 = 2l^2$. Wie vorher folgt, dass m^2 gerade und dann auch m selbst gerade ist. Also sind n und m gerade, d.h., beide durch $k = 2$ teilbar, im Widerspruch zur Annahme, dass $x = n/m$ gekürzt ist. □

3. *Vollständige Induktion und Primzahlen*

In der oben formulierten Fassung ist Peano's Induktionsaxiom oftmals etwas umständlich. Sehr nützlich ist folgende Variante.

Satz 3.1 (Vollständige Induktion)**.** *Sei* $n_0 \in \mathbb{N}_0$ *fest und für jedes* $n \in \mathbb{N}_0$ *mit* $n \geqslant n_0$ *eine Aussage* $P(n)$ *gegeben. Die folgenden beiden Voraussetzungen seien erfüllt:*

(I1) *Induktionsanfang.* $P(n_0)$ *ist wahr.*

(I2) *Induktionsschritt.* $\forall n \in \mathbb{N}_0 : (n \geqslant n_0$ *und* $P(n)$ *wahr*$) \Rightarrow P(n+1)$ *wahr.*

Dann ist $P(n)$ *wahr für alle* $n \in \mathbb{N}_0$ *mit* $n \geqslant n_0$.

Beweis. Wir zeigen dies wieder mit einem Widerspruchbeweis. Angenommen, es gäbe ein $n \in \mathbb{N}_0$ mit $n \geqslant n_0$ und so, dass $P(n)$ falsch ist. Dann ist

$$A := \{n \in \mathbb{N}_0 \mid n \geqslant n_0 \text{ und } P(n) \text{ ist falsch}\} \neq \varnothing.$$

Nach Peano's Induktionsaxiom besitzt A ein kleinstes Element; sei dieses k. Wegen (I1) ist $k > n_0$. Dann ist $k-1 \geqslant n_0$ und $k-1 \notin A$, d.h., $P(k-1)$ ist wahr.
Wende (I2) auf $n = k-1$ an. Es folgt, dass auch $P(k)$ wahr ist, Widerspruch. □

Als Beispiel geben wir einen neuen Beweis von Satz 2.5, wobei wir für $n \in \mathbb{N}$ die folgende Aussage betrachten:

$$P(n): \quad 1+2+\ldots+n = \tfrac{1}{2}n(n+1).$$

Startwert ist hier $n_0 = 1$. Wir müssen nun nachweisen, dass (I1) und (I2) erfüllt sind.

Zu (I1), Induktionsanfang: Ist $n = n_0 = 1$, so ist die linke Seite von $P(1)$ gleich 1 und die rechte Seite gleich $\frac{1}{2}(1+1) = 1$. Also ist $P(1)$ wahr.

Zu (I2), Induktionsschritt: Sei $n \in \mathbb{N}_0$ mit $n \geqslant n_0 = 1$ beliebig. Wir nehmen an, dass $P(n)$ wahr ist und müssen dann zeigen, dass auch $P(n+1)$ wahr ist.

Beginnen wir mit der linken Seite von $P(n+1)$ und formen diese um:

$$\begin{aligned} 1+2+\ldots+(n+1) &= (1+2+\ldots+n)+(n+1) \\ &= \tfrac{1}{2}n(n+1)+(n+1) \quad \text{(da } P(n) \text{ als wahr vorausgesetzt ist)}, \\ &= \tfrac{1}{2}(n^2+n)+\tfrac{1}{2}(2n+2) = \tfrac{1}{2}(n^2+3n+2). \end{aligned}$$

Andererseits ist die rechte Seite von $P(n+1)$ gleich

$$\tfrac{1}{2}(n+1)\big((n+1)+1\big) = \tfrac{1}{2}(n+1)(n+2) = \tfrac{1}{2}(n^2+3n+2).$$

Also erhalten wir das gleiche Ergebnis wie voher; damit ist (I2) gezeigt. Mit Satz 3.1 folgt also, dass $P(n)$ für alle $n \geqslant 1$ wahr ist.

Bemerkung 3.2. Wir sehen hier gleichzeitig eine Stärke und eine Schwäche der vollständigen Induktion. Ist bereits bekannt, was man zeigen will, so ist dies eine sehr effiziente Beweismethode. Wenn man allerdings die Formel noch nicht kennt und erst herausfinden muss, so benötigt man in der Tat einen "Trick" – wie im ursprünglichen Beweis von Satz 2.5. Versuchen Sie etwa, Formeln für $1^2+2^2+\cdots+n^2$ und $1^3+2^3+\cdots+n^3$ zu finden. (Siehe dazu auch `https://de.wikipedia.org/wiki/Faulhabersche_Formel`)

Die folgende Variante der vollständigen Induktion ist ebenfalls sehr oft nützlich.

Satz 3.3 (Starke vollständige Induktion)**.** *Sei $n_0 \in \mathbb{N}_0$ fest und für jedes $n \in \mathbb{N}_0$ mit $n \geqslant n_0$ eine Aussage $P(n)$ gegeben. Die folgenden beiden Voraussetzungen seien erfüllt:*

(SI1) *$P(n_0)$ ist wahr.*

(SI2) *$\forall n \in \mathbb{N}_0 : (P(m)$ wahr für $n_0 \leqslant m < n) \Rightarrow P(n)$ wahr.*

Dann ist $P(n)$ wahr für alle $n \in \mathbb{N}_0$ mit $n \geqslant n_0$.

Beweis. Wir brauchen nur den Beweis von Satz 3.1 etwas zu verändern. Angenommen, es wäre $A := \{n \in \mathbb{N}_0 \mid n \geqslant n_0 \text{ und } P(n) \text{ ist falsch}\} \neq \varnothing$. Nach Peano besitzt A ein kleinstes Element; sei dieses k. Wegen (SI1) ist $k > n_0$. Sei nun $m \in \{n_0, n_0+1, \ldots, k-1\}$. Dann ist $m \notin A$, d.h., $P(m)$ ist wahr. Mit (SI2) angewandt auf $n = k$ folgt, dass auch $P(k)$ wahr ist, Widerspruch. □

Definition 3.4. Sei $n \in \mathbb{N}$, $n \geqslant 2$. Dann heißt n eine ***Primzahl***, wenn n nur durch 1 und sich selbst teilbar ist.
Zum Beispiel sind $2, 3, 5, 7, 11$ Primzahlen, aber 1 und 12 sind keine Primzahlen.

Satz 3.5 (Primfaktorzerlegung in $\mathbb{N}$)**.** *Sei $n \in \mathbb{N}$, $n \geqslant 2$. Dann lässt sich n als Produkt von Primzahlen schreiben; es gibt also $r \geqslant 1$ Primzahlen $p_1, p_2, \ldots, p_r$ mit $n = p_1 p_2 \cdots p_r$ und $p_1 \leqslant p_2 \leqslant \ldots \leqslant p_r$.*

Beweis. (Starke Induktion mit $n_0 = 2$.) Für $n \geqslant 2$ betrachten wir die Aussage:

$$P(n): \quad \text{"}n \text{ ist Produkt von Primzahlen"}.$$

Wir müssen zeigen, dass die Voraussetzungen (SI1) und (SI2) erfüllt sind.
Zu (SI1): Sei also $n = n_0 = 2$. Da 2 eine Primzahl ist, ist $n = 2$ offenbar auch ein Produkt von Primzahlen (mit nur einem Faktor).
Zu (SI2): Sei $n > 2$ und vorausgesetzt, dass $P(m)$ wahr ist für $m = 2, 3, \ldots, n-1$. Wir müssen dann zeigen, dass $P(n)$ wahr ist. Dazu unterscheiden wir zwei Fälle.
1. Fall: n ist selbst eine Primzahl. Dann ist (siehe oben) n offenbar auch ein Produkt von Primzahlen (mit nur einem Faktor), also die Behauptung gezeigt.
2. Fall: n ist keine Primzahl. Nach Definition einer Primzahl bedeutet dies, dass $n = ab$ gilt mit $a, b \in \mathbb{N}$ und $2 \leqslant a, b \leqslant n-1$. Nach Voraussetzung sind $P(a)$ und $P(b)$ wahr, also sind a und b Produkte von Primzahlen. Wir schreiben $a = p_1 p_2 \cdots p_r$ und $b = q_1 q_2 \cdots q_s$ mit $r, s \geqslant 1$ und Primzahlen p_i, q_j.
Dann ist aber auch $n = ab = p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s$ ein Produkt von Primzahlen (mit $r+s$ Faktoren). Schließlich sortieren wir die Faktoren im Endprodukt der Größe nach um. □

Satz 3.6 (Euklid)**.** *Es gibt unendlich viele Primzahlen.*

Beweis. Dies ist wieder ein klassisches Beispiel eines Widerspruchsbeweises. Angenommen, es gäbe nur endlich viele Primzahlen; seien diese $p_1, p_2, \ldots, p_r$.
Damit bilden wir $N := p_1 p_2 \cdots p_r + 1 \in \mathbb{N}$. (Dies ist der Trick des Beweises.) Es gilt sicherlich $N \geqslant 2$, also besitzt N nach Satz 3.5 eine Primfaktorzerlegung. In dieser können aber nur die Primzahlen $p_1, \ldots, p_r$ vorkommen, und mindestens eine kommt vor. Es gibt also ein $i \in \{1, \ldots, r\}$ mit $p_i \mid N$. Andererseits ist $N - 1 = p_1 p_2 \cdots p_r$, also gilt $p_i \mid N-1$. Mit Lemma 2.2(b) folgt dann aber auch $p_i \mid N - (N-1) = 1$, also $p_i = 1$, Widerspruch. □

Bemerkung 3.7. Für $n \in \mathbb{N}$ sei p_n die n-te Primzahl. Zum Beispiel $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, …, $p_{100} = 541$, … Es ist keine allgemeine Formel bekannt, mit der man zu beliebigem n die entsprechende Primzahl p_n berechnen könnte.
PIERRE DE FERMAT vermutete um 1640, dass $F_n := 2^{2^n}+1$ eine Primzahl ist für alle $n \in \mathbb{N}_0$.

n	F_n	
0	3	ok
1	5	ok
2	17	ok
3	257	ok
4	65537	ok
5	$2^{32}+1 = 4294967297$	nicht ok: $641 \cdot 6700417$ (LEONHARD EULER 1732)

Es ist bekannt, dass $F_5, \ldots, F_{32}$ keine Primzahlen sind. Für größere Werte von n ist nicht bekannt, ob F_n eine Primzahl ist oder nicht.

Lemma 3.8 ("Lemma von Euklid"). *Sei $p \in \mathbb{N}$ eine Primzahl und seien $a, b \in \mathbb{N}$. Gilt $p \mid ab$, so folgt $p \mid a$ oder $p \mid b$.*

Das Lemma von Euklid kommt in nahezu jeder Argumentation mit Primzahlen vor; es ist genau das "richtige" technische Hilfsmittel.

Beispiel. In Lemma 2.3 haben wir gezeigt: "n ungerade $\Rightarrow$ n^2 ungerade" und dann mit Kontraposition geschlossen: "n^2 gerade $\Rightarrow$ n gerade". Mit dem Lemma von Euklid folgt dies auch direkt: Ist n^2 gerade, so gilt $2 \mid n^2 = nn$, also folgt $2 \mid n$.

Beweis von Lemma 3.8. Seien $a, b \in \mathbb{N}$ gegeben mit $p \mid ab$. Nehmen wir an, es gilt $p \nmid a$. Dann müssen wir $p \mid b$ zeigen. Da p nur die Teiler 1 und p hat, ist $\mathrm{ggT}(p, a) = 1$ oder p. Also $\mathrm{ggT}(p, a) = 1$ wegen $p \nmid a$. Nach dem ***Lemma von Bézout*** gibt es $r, s \in \mathbb{Z}$ mit $1 = rp + sa$. Multiplikation mit b ergibt $b = rpb + sab$. Wegen $p \mid rpb$ und $p \mid sab$ folgt mit Lemma 2.2, dass auch $p \mid rpb + sab = b$ gilt. □

Folgerung 3.9. *Sei $p \in \mathbb{N}$ eine Primzahl, $n \in \mathbb{N}$ und seien $c_1, \ldots, c_n \in \mathbb{N}$.*
Gilt $p \mid c_1 c_2 \cdots c_n$, so gibt es ein $i \in \{1, \ldots, n\}$ mit $p \mid c_i$.

Beweis. (Vollständige Induktion über n mit Startwert $n_0 = 1$.) Induktionsanfang: Sei $n = 1$, also ist nur eine Zahl c_1 gegeben mit $p \mid c_1$. Dann gilt die Aussage. (Es ist nichts zu zeigen.)

Induktionsschritt: Sei $n \geqslant 1$ und angenommen, dass die Aussage bereits für n Zahlen gilt. Dann müssen wir zeigen, dass sie auch für $n+1$ Zahlen gilt. Gegeben seien also $c_1, \ldots, c_{n+1} \in \mathbb{N}$ mit $p \mid c_1 c_2 \ldots c_{n+1}$. Setze nun $a := c_1 c_2 \cdots c_n$. Dann ist $c_1 c_2 \cdots c_{n+1} = a c_{n+1}$ und $p \mid a c_{n+1}$. Nach Lemma 3.8 folgt also $p \mid a$ oder $p \mid c_{n+1}$. Im 2. Fall sind wir fertig. Im 1. Fall gilt $p \mid c_1 \cdots c_n$, also gibt es nach Induktionsannahme ein $i \in \{1, \ldots, n\}$ mit $p \mid c_i$, und wir sind wieder fertig. □

Satz 3.10 (Hauptsatz der elementaren Arithmetik)**.** *Die Primfaktorzerlegung einer natürlichen Zahl* $n \geqslant 2$ *(siehe Satz 3.5) ist eindeutig.*

Beweis. (Starke Induktion mit Startwert $n_0 = 2$.) Für $n \in \mathbb{N}$, $n \geqslant 2$, ist folgende Aussage $P(n)$ zu beweisen:

"Gegeben seien Primzahlen $p_1 \leqslant p_2 \leqslant \ldots \leqslant p_r$ und $q_1 \leqslant q_2 \leqslant \ldots \leqslant q_s$ (wobei $r, s \geqslant 1$) mit $n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$. Dann gilt $r = s$ und $p_i = q_i$ für $1 \leqslant i \leqslant r$."

Induktionsanfang: Sei $n = 2$. Dann ist n selbst eine Primzahl, und die Aussage ist klar nach Definition einer Primzahl.

Induktionsschritt: Sei $n > 2$ und angenommen, dass $P(m)$ bereits gilt für alle m mit $2 \leqslant m < n$. Dann müssen wir zeigen, dass auch $P(n)$ gilt. Ist n selbst eine Primzahl, so ist die Aussage wieder klar nach Definition einer Primzahl. Sei also nun n keine Primzahl und betrachten wir zwei Faktorisierungen wie oben:

$$(*) \qquad n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s \qquad (\text{mit } r, s \geqslant 2).$$

1. Fall: $p_1 = q_1$. Dann können wir p_1 auf beiden Seiten kürzen und erhalten $m := p_2 \cdots p_r = q_2 \cdots q_s$. Wegen $2 \leqslant m < n$ ist $P(m)$ nach Induktionsannahme wahr, also $r = s$ und $p_i = q_i$ für $2 \leqslant i \leqslant r$. Da auch $p_1 = q_1$ gilt, ist also $P(n)$ wahr.

2. Fall: $p_1 < q_1$. Nun ist $p_1 \mid p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$, also gibt es nach Folgerung 3.9 ein $i \in \{1, \ldots, s\}$ mit $p_1 \mid q_i$. Aber p_1 und q_i sind Primzahlen, also muss $p_1 = q_i$ gelten. Andererseits ist $p_1 < q_1 \leqslant q_2 \leqslant \ldots \leqslant q_i$, also $p_1 < q_i$, Widerspruch.

3. Fall: $p_1 > q_1$. Man erhält Widerspruch völlig analog zum 2. Fall. (Es ist $q_1 \mid p_1 \cdots p_r$ usw.)

Also treten der 2. und 3. Fall gar nicht auf. □

Ab hier Woche 3

4. *Relationen und Restklassen*

Wir führen eine weitere grundlegende mengentheoretische Konstruktion ein. Das ***kartesische Produkt*** von zwei nicht-leeren Mengen A und B wird mit $A \times B$ bezeichnet. Dies ist eine Menge, die aus allen Paaren (a, b) mit $a \in A$ und $b \in B$ besteht:

$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

Für zwei Paare (a, b) und (a', b') gilt $(a, b) = (a', b')$ genau dann, wenn $a = a'$ und $b = b'$. (Formal korrekt wird das Paar (a, b) als die Menge $\{a, \{a, b\}\}$ definiert.) Zum Beispiel ist

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

Beachten Sie, dass die Reihenfolge wichtig ist: $(2, 4)$ ist nicht das Gleiche wie $(4, 2)$. Sie sind vermutlich vertraut mit dem kartesischen Produkt $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$, das man sich üblicherweise als Ebene mit 2 Koordinatenachsen vorstellt.

Definition 4.1. Sind A, B nicht-leere Mengen, so heißt eine Teilmenge $R \subseteq A \times B$ eine ***Relation*** auf A und B. Für $a \in A$ und $b \in B$ schreiben wir $a \sim b$, wenn $(a, b) \in R$ gilt (und sagen: "a steht in Relation zu b"). Ist $A = B$, so heißt R eine Relation auf A.

Beispiel 4.2. (a) Sei A die Menge aller Punkte der Ebene und B die Menge aller Geraden in der Ebene. Die Eigenschaft, dass ein Punkt auf einer Geraden liegt, definiert eine Relation:

$$R = \{(a, b) \in A \times B \mid \text{Der Punkt } a \text{ liegt auf der Geraden } b\}.$$

(b) Hier sind Beispiele von Relationen auf $A = B = \mathbb{Z}$:

$$R_1 = \{(n, m) \in \mathbb{Z} \times \mathbb{Z} \mid n < m\},$$
$$R_2 = \{(n, m) \in \mathbb{Z} \times \mathbb{Z} \mid \ n \text{ teilt } m\},$$
$$R_3 = \{(n, m) \in \mathbb{Z} \times \mathbb{Z} \mid \ n = m \text{ oder } n + m \geqslant 0\}.$$

Beispiel 4.3. Sei wieder $A = B = \mathbb{Z}$. Für festes $m \in \mathbb{N}$ definieren wir die Relation

$$R_m := \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a \bmod m = b \bmod m\}.$$

Es gilt hier also $a \sim b$ genau dann, wenn a und b den gleichen Rest bei Division durch m haben. Wir behaupten, dass diese Relation auch wie folgt charakterisiert werden kann:

$$(a, b) \in R_m \qquad \Leftrightarrow \qquad m \mid b - a. \tag{$*$}$$

Beweis von ($*$): Seien $a, b \in \mathbb{Z}$. Es gibt $q, q', r, r' \in \mathbb{Z}$ mit $a = qm + r$, $b = q'm + r'$ und $0 \leqslant r, r' < m$. Sei zuerst $(a, b) \in R_m$, d.h., $r = r'$. Dann folgt $a - qm = r = r' = b - q'm$ und damit $b - a = (q' - q)m$; also ist $m \mid b - a$. Sei umgekehrt $m \mid b - a$, also $b - a = cm$ mit $c \in \mathbb{Z}$, also $b = cm + a = cm + qm + r = (c + q)m + r$. Aus der Eindeutigkeit des Restes folgt also $r = r'$ und damit $(a, b) \in R_m$. □

Anstelle von $(n, n') \in R_m$ schreiben wir künftig $n \equiv n' \pmod m$.
Dies wird gelesen als: "n und n' sind ***kongruent modulo*** m."
Ist etwa $m = 2$ und $n \in \mathbb{Z}$ beliebig, so ist der Rest $n \bmod 2$ entweder 0 oder 1. Also:

$$n \bmod 2 = 0 \quad \Leftrightarrow \quad n \equiv 0 \pmod 2 \quad \Leftrightarrow \quad n \text{ ist gerade,}$$
$$n \bmod 2 = 1 \quad \Leftrightarrow \quad n \equiv 1 \pmod 2 \quad \Leftrightarrow \quad n \text{ ist ungerade.}$$

Definition 4.4. Sei A eine nicht-leere Menge und $R \subseteq A \times A$ eine Relation auf A, geschrieben $a \sim b$ für $a, b \in A$. Die Relation R heißt:

- ***reflexiv***, wenn $a \sim a$ für alle $a \in A$ gilt;
- ***symmetrisch***, wenn für $a, b \in A$ aus $a \sim b$ stets $b \sim a$ folgt;
- ***anti-symmetrisch***, wenn für $a, b \in A$ aus $a \sim b$ und $b \sim a$ stets $a = b$ folgt;
- ***transitiv***, wenn für $a, b, c \in A$ aus $a \sim b$ und $b \sim c$ stets $a \sim c$ folgt.

Ist R reflexiv, symmetrisch und transitiv, so heißt R eine ***Äquivalenzrelation***.
Ist R reflexiv, anti-symmetrisch und transitiv, so heißt R eine ***Ordnungsrelation***.

Beispiel 4.5. (a) Sei $A = \mathbb{Z}$ und betrachte die Relationen R_1, R_2, R_3 in Beispiel 4.2(b).

$R_1 = \{(n, m) \in \mathbb{Z} \times \mathbb{Z} \mid n < m\}$ ist transitiv, aber weder reflexiv noch symmetrisch;

$R_2 = \{(n, m) \in \mathbb{Z} \times \mathbb{Z} \mid$ n teilt $m\}$ ist transitiv, reflexiv aber nicht symmetrisch;

$R_3 = \{(n, m) \in \mathbb{Z} \times \mathbb{Z} \mid$ $n = m$ oder $n + m \geqslant 0\}$ ist reflexiv, symmetrisch, aber nicht transitiv (denn z.B. $(-1, 2) \in R_3$, $(2, 0) \in R_3$, aber $(-1, 0) \notin R_3$).

(b) Die übliche Relation "$\leqslant$" auf $A = \mathbb{Z}$ ist eine Ordnungsrelation.

(c) Sei $A = \mathbb{Z}$ und $m \in \mathbb{N}$ fest. Wir behaupten, dass die Kongruenz-Relation R_m in Beispiel 4.3 eine Äquivalenzrelation ist. Prüfen wir dies nach. Die Relation ist

- reflexiv, denn $m \mid a - a = 0$, also $a \sim a$;
- symmetrisch, denn aus $a \sim b$ folgt $m \mid b - a$ und damit auch $m \mid -(b - a) = a - b$ (siehe Lemma 2.2(b)), also $b \sim a$;
- transitiv, denn aus $a \sim b$ und $b \sim c$ folgt $m \mid b - a$ und $m \mid c - b$; also auch $m \mid (c - b) + (b - a) = c - a$ (siehe Lemma 2.2(b)) und damit $a \sim c$.

Definition 4.6. Sei $R \subseteq A \times A$ eine Äquivalenzrelation. Für $a \in A$ heißt dann

$$K(a, R) := \{b \in A \mid (a, b) \in R\}$$

die ***Äquivalenzklasse*** von a. Dies ist also eine Teilmenge von A, d.h., ein Element von $\mathcal{P}(A)$. Sei $\mathcal{K}(A, R)$ die Menge aller Äquivalenzklassen von Elementen in A, d.h.,

$$\mathcal{K}(A, R) = \{S \in \mathcal{P}(A) \mid \exists a \in A : S = K(a, R)\}.$$

Sei zum Beispiel A die Menge aller Menschen auf dem Planeten Erde und

$$R = \{(a, b) \in A \times A \mid a \text{ und } b \text{ leben im gleichen Land}\}.$$

Sie überprüfen leicht, dass dies eine Äquivalenzrelation ist. Eine Äquivalenzklasse besteht genau aus allen Menschen, die in einem Land leben. Die Menge der Äquivalenzklassen entspricht also den verschiedenen Ländern.

In Beispiel 4.3 mit $m = 2$ ist $K(0, R_2) =$ Menge aller geraden Zahlen und $K(1, R_2) =$ Menge aller ungeraden Zahlen. Also $\mathcal{K}(\mathbb{Z}, R_2) = \{K(0, R_2), K(1, R_2)\}$.

Satz 4.7. *Sei $R \subseteq A \times A$ eine Äquivalenzrelation. Dann gilt:*
(a) *Jedes $a \in A$ liegt in einer Äquivalenzklasse.*
(b) *Zwei Äquivalenzklassen sind entweder gleich oder disjunkt.*
("disjunkt" bedeutet: der Durchschnitt ist leer).

Beweis. (a) Sei $a \in A$. Da R reflexiv ist, gilt $a \sim a$ also $a \in K(a, R)$.

(b) Seien $a, b \in A$ und $K_a = K(a, R)$, $K_b = K(b, R)$. Nehmen wir an, es ist $K_a \cap K_b \neq \varnothing$. Dann müssen wir zeigen, dass $K_a = K_b$ gilt. Sei dazu $d \in K_a \cap K_b$.

Ist $c \in K_a$ beliebig, so gilt $a \sim c$. Wegen $d \in K_a$ ist $a \sim d$ und wegen der Symmetrie dann auch $d \sim a$. Mit der Transitivität folgt $d \sim c$. Wegen $d \in K_b$ gilt $b \sim d$, also folgt mit der Transitivität schließlich $b \sim c$, d.h., $c \in K_b$. Damit ist gezeigt, dass $K_a \subseteq K_b$ gilt. Auf völlig analoge Weise wird $K_b \subseteq K_a$ gezeigt. Also gilt $K_a = K_b$, wie behauptet. □

Für $a \in A$ sei $K_a = K(a, R) = \{b \in A \mid (a, b) \in R\}$ die Äquivalenzklasse von a.
Der letzte Satz zeigt: A ist Vereinigung aller Äquivalenzklassen. In dieser Vereinigung sind im Allgemeinen viele Terme gleich. Sind $a, b \in A$, so gilt $K_a = K_b \Leftrightarrow b \in K_a$.

Definition 4.8. Sei $R \subseteq A \times A$ eine Äquivalenzrelation. Eine Teilmenge $B \subseteq A$ heißt ***Repräsentantensystem der Äquivalenzklassen***, wenn es zu jedem $a \in A$ genau ein $b \in B$ gibt mit $(b, a) \in R$. Oder anders ausgedrückt:

$$A = \bigcup_{b \in B} K(b, R), \quad \text{und in dieser Vereinigung sind die Terme alle disjunkt.}$$

Beispiel 4.9 (Konstruktion von $\mathbb{Q}$ aus $\mathbb{Z}$)**.** Sei $A = \mathbb{Z} \times \mathbb{N}$ und betrachte folgende Relation:

$$R := \big\{\big((n, m), (n', m')\big) \in A \times A \mid nm' = n'm\big\}.$$

(Nach Übung 3 ist dies eine Äquivalenzrelation.) Für $(n, m) \in A$ schreiben wir anstelle von $K((n, m), R)$ einfach kurz n/m. Mit Hilfe des ggT sieht man leicht, dass jede Äquivalenzklasse ein *gekürztes* Paar (n, m) enthält, d.h., es gibt keine natürliche Zahl $k > 1$ mit $k \mid n$ und $k \mid m$. Nach Übung 3 ist ein Repräsentantensystem der Äquivalenzklassen gegeben durch

$$B := \{(n, m) \in A \mid (n, m) \text{ ist gekürzt}\},$$

d.h., die Äquivalenzklassen entspechen genau den ***rationalen Zahlen*** ! Auf diese Weise erhält man in der Tat eine mathematisch korrekte Konstruktion: *Man definiert* $\mathbb{Q} := \mathcal{K}(A, R)$.

Eine Gleichheit wie $2/3 = 4/6 = 100/150$ entspricht dann einfach der Tatsache, dass die Paare $(2, 3)$, $(4, 6)$, $(100, 150)$ zur gleichen Äquivalenzklasse gehören.
Ist $n \in \mathbb{Z}$, so schreiben wir einfach n anstelle von $n/1$. Vermöge dieser Identifizierung ist dann $\mathbb{Z} \subseteq \mathbb{Q}$. (Überlegen Sie sich selbst, wie man auf ähnliche Weise $\mathbb{Z}$ aus $\mathbb{N}$ konstruiert.)

Beispiel 4.10. Sei $A = \mathbb{Z}$ und $m \in \mathbb{N}$. Die Äquivalenzklassen bezüglich der Äquivalenzrelation R_m (siehe Beispiel 4.3) werden auch als ***Restklassen*** (modulo m) bezeichnet.
Sofern m fest vorgegeben ist, werden wir die Restklasse von $n \in \mathbb{Z}$ einfach mit $\overline{n}$ bezeichnen, also $\quad \overline{n} = \{a \in \mathbb{Z} \mid m \text{ teilt } n - a\} = \{a \in \mathbb{Z} \mid a \bmod m = n \bmod m\}$.

Repräsentantensystem? Ein solches ist gegeben durch $B = \{0, 1, 2, \ldots, m - 1\}$, denn bei der Division mit Rest durch m kommen nur die Reste $0, 1, 2, \ldots, m - 1$ vor (und der Rest ist eindeutig bestimmt). Anders formuliert: Für jedes $n \in \mathbb{Z}$ gibt es genau ein $r \in B$ mit $n \bmod m = r$, also $n \in \overline{r}$ und $\overline{n} = \overline{r}$. Es gilt also

$$\mathbb{Z} = \overline{0} \cup \overline{1} \cup \overline{2} \cup \ldots \cup \overline{(m-1)} \qquad \text{(disjunkte Vereinigung).}$$

Ist etwa $m = 5$, so gilt $\mathbb{Z} = \overline{0} \cup \overline{1} \cup \overline{2} \cup \overline{3} \cup \overline{4}$.
Es ist $-17 \in \overline{3}$ und $38 \in \overline{3}$ (weil -17 und 38 beide den Rest 3 modulo 5 haben).

Genauso, wie man Brüche (also letztlich gewisse Äquivalenzklassen) addieren und multiplizieren kann, werden wir sehen, dass man auch Restklassen modulo m addieren und multiplizieren kann. Grundlage dafür ist:

Lemma 4.11. *Sei $m \in \mathbb{N}$. Wie oben bezeichnen wir die Restklasse (modulo m) von $n \in \mathbb{Z}$ mit $\overline{n}$. Seien $a, b, c, d \in \mathbb{Z}$. Gilt $\overline{a} = \overline{c}$ und $\overline{b} = \overline{d}$, so folgt $\overline{a+b} = \overline{c+d}$ und $\overline{ab} = \overline{cd}$.*

Beweis. Sei $\overline{a} = \overline{c}$ und $\overline{b} = \overline{d}$, also $m \mid c - a$ und $m \mid d - b$. Seien $r, s \in \mathbb{Z}$ mit $c - a = rm$ und $d - b = sm$, also $c = a + rm$ und $d = b + sm$. Damit erhalten wir

$$(c + d) - (a + b) = (a + rm) + (b + sm) - a - b = rm + sm = (r + s)m,$$

also $m \mid (c + d) - (a + b)$, d.h., $\overline{a+b} = \overline{c+d}$. Außerdem ist

$$\begin{aligned} cd - ab &= (a + rm)(b + sm) - ab = (ab + asm + rmb + rmsm) - ab \\ &= asm + rmb + rmsm = (as + rb + rsm)m, \end{aligned}$$

also $m \mid cd - ab$, d.h., $\overline{ab} = \overline{cd}$. □

Sei zum Beispiel $m = 6$. Wir wollen $(17 \cdot 14) \bmod 6$ berechnen.
Dazu: Es gilt $17 \bmod 6 = 5$ und $14 \bmod 6 = 2$, also $\overline{17} = \overline{5}$ und $\overline{14} = \overline{2}$. Damit

$$\overline{17 \cdot 14} = \overline{5 \cdot 2} = \overline{10} = \overline{4}$$

wobei wir Lemma 4.11 für die 1. Gleichheit benutzt haben. Also gilt $(17 \cdot 14) \bmod 6 = 4$. (Man muss also nicht erst $17 \cdot 14$ ausrechnen und dann mit Rest durch 6 teilen.)

Beispiel 4.12. Ist 7513 durch 3 teilbar? Nach der (vielleicht bekannten) ***Dreierregel*** müssten wir uns dazu nur die Quersumme von 7513 anschauen:
Diese ist $7 + 5 + 1 + 3 = 16$, und wegen $3 \nmid 16$ folgt auch $3 \nmid 7513$.

Begründung: Sei $m = 3$ und betrachte $\overline{7513} = \overline{7 \cdot 1000 + 5 \cdot 100 + 1 \cdot 10 + 3}$.
Nun ist $10 \bmod 3 = 1$, also $\overline{10} = \overline{1}$. Mit Lemma 4.11 folgt daher auch $\overline{100} = \overline{10 \cdot 10} = \overline{1 \cdot 1} = \overline{1}$; genauso $\overline{1000} = \overline{10 \cdot 100} = \overline{1 \cdot 1} = \overline{1}$, und damit

$$\overline{7513} = \overline{7 \cdot 1000 + 5 \cdot 100 + 1 \cdot 10 + 3} = \overline{7 \cdot 1 + 5 \cdot 1 + 1 \cdot 1 + 3} = \overline{7 + 5 + 1 + 3} = \overline{16}.$$

D.h., die Zahl 7513 hat den gleichen Rest (modulo 3) wie ihre Quersumme.

5. *Abbildungen und die Mächtigkeit von Mengen*

Seien A, B nicht-leere Mengen. Eine ***Abbildung*** f von A nach B ist eine Zuordnung, die jedem Element von A genau ein Element von B zuordnet. In Zeichen $f \colon A \to B$, $a \mapsto f(a)$.

Das ***Bild*** von f ist definiert als $\mathrm{Bild}(f) := \{b \in B \mid \exists a \in A : f(a) = b\}$. Für eine beliebige Teilmenge $A' \subseteq A$ sei $f(A') := \{b \in B \mid \exists a \in A' : f(a) = b\}$. Damit ist also $\mathrm{Bild}(f) = f(A)$.

Die Abbildung f heißt ***surjektiv***, wenn $f(A) = B$ gilt.
Die Abbildung f heißt ***injektiv***, wenn für alle $a, a' \in A$ gilt: Aus $f(a) = f(a')$ folgt $a = a'$. (Oder umgekehrt: Gilt $a \neq a'$, so auch $f(a) \neq f(a')$.)
Die Abbildung heißt ***bijektiv***, wenn sie sowohl injektiv als auch surjektiv ist.

Ist $A = \mathbb{N}$, so bezeichnet man f auch als ***Folge*** und schreibt vereinfachend $f = (a_n)_{n\in\mathbb{N}}$, wobei $a_n = f(n)$ für alle $n \in \mathbb{N}$. (Analog für $A = \mathbb{N}_0$.)

Bemerkung 5.1. (a) Implizit haben wir bereits Abbildungen betrachtet. Zum Beispiel ist die Addition in $\mathbb{N}$ eine Abbildung $\alpha\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $(n, n') \mapsto n + n'$.

(b) Ist $f\colon A \to B$ eine Abbildung, so heißt $\quad \mathcal{G}(f) := \{(a, f(a)) \mid a \in A\} \subseteq A \times B$ der ***Graph*** von f. Dies ist also eine Relation auf $A \times B$.

(c) Umgekehrt: Formal korrekt ist eine Abbildung $f\colon A \to B$ durch eine Relation $R \subseteq A \times B$ gegeben, welche folgende Bedingungen erfüllt:

(i) Zu jedem $a \in A$ gibt es ein $b \in B$ mit $(a, b) \in R$;

(ii) sind $a \in A$ und $b, b' \in B$ mit $(a, b) \in R$ und $(a, b') \in R$ gegeben, so folgt $b = b'$.

Diese beiden Bedingungen besagen gerade, dass zu jedem $a \in A$ genau ein $b \in B$ gehört, und dieses b wird dann mit $f(a)$ bezeichnet. Dann ist $R = \mathcal{G}(f)$.
Also: Eine Abbildung $f\colon A \to B$ ist eine Relation mit speziellen Eigenschaften.

Beispiel 5.2. (a) Die Abbildung $f\colon \mathbb{Z} \to \mathbb{Z}$, $n \mapsto n^2$, ist weder injektiv noch surjektiv, denn es gilt zum Beispiel $f(1) = 1 = f(-1)$ und $2 \notin f(\mathbb{Z})$.

(b) Sei $A = \{n \in \mathbb{Z} \mid n \text{ gerade}\}$ und $B = \{n \in \mathbb{Z} \mid n \text{ ungerade}\}$. Dann erhalten wir eine Abbildung $f\colon A \to B$, $n \mapsto n + 1$. Diese Abbildung ist bijektiv (wie Sie selbst leicht zeigen).

(c) Die Abbildung $f\colon \mathbb{N}_0 \to \mathbb{N}_0$, $n \mapsto 2n$, ist injektiv aber nicht surjektiv.

(d) Seien $k, n \in \mathbb{N}_0$. Dann ist $2^k(2n + 1) \geqslant 1$, also $2^k(2n + 1) - 1 \in \mathbb{N}_0$. Damit erhalten wir eine Abbildung $\quad f\colon \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0, \qquad (k, n) \mapsto 2^k(2n + 1) - 1$.
Wir überlassen es als Übung zu zeigen, dass diese Abbildung bijektiv ist.

Definition 5.3. Seien A, B nicht-leere Mengen und $f\colon A \to B$ eine Abbildung.
Für $b \in B$ heißt $f^{-1}(b) := \{a \in A \mid f(a) = b\}$ das ***Urbild*** von b. Allgemeiner:
Ist $B' \subseteq B$ eine Teilmenge, so ist $f^{-1}(B') := \{a \in A \mid f(a) \in B'\}$ das Urbild von B'.

• Sei $b \in B$. Dann gilt: $\quad f^{-1}(b) \neq \varnothing \quad \Leftrightarrow \quad b \in f(A)$.
Beispiel: Für $f\colon \mathbb{N} \to \mathbb{N}$, $n \mapsto 2n$, gilt $f^{-1}(3) = \varnothing$.

• Ist f injektiv und $b \in f(A)$, so gilt $|f^{-1}(b)| = 1$.

• Seien $b, b' \in B$ und $b \neq b'$. Dann ist $f^{-1}(b) \cap f^{-1}(b') = \varnothing$.

• Sei f surjektiv. Dann ist $f^{-1}(b) \neq \varnothing$ für alle $b \in B$ und $A = \bigcup_{b \in B} f^{-1}(b)$.

Beispiel: $f\colon \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0$, $(n, m) \mapsto n + m$, ist surjektiv. Es gilt

$f^{-1}(0) = \{(0,0)\}$, $f^{-1}(2) = \{(2,0), (1,1), (0,2)\}$,

$f^{-1}(\{\text{gerade Zahlen}\}) = \{(n, m) \in \mathbb{N}_0 \times \mathbb{N}_0 \mid n, m \text{ beide gerade oder } n, m \text{ beide ungerade}\}$.

Definition 5.4. Seien A, B, C nicht-leere Mengen und $f\colon A \to B$, $g\colon B \to C$ Abbildungen. Durch ***Hintereinanderausführung*** erhalten wir auch eine Abbildung

$$g \circ f\colon A \to C, \qquad a \mapsto g\big(f(a)\big).$$

Wir bezeichnen mit $\mathrm{id}_A\colon A \to A$ die ***identische Abbildung***, d.h., $\mathrm{id}_A(a) = a$ für alle $a \in A$.

Lemma 5.5. *Sei $f\colon A \to B$ eine Abbildung. Dann gilt:*

(a) *Gibt es eine Abbildung $g\colon B \to A$ mit $g \circ f = \mathrm{id}_A$, so ist f injektiv.*

(b) *Gibt es eine Abbildung $g\colon B \to A$ mit $f \circ g = \mathrm{id}_B$, so ist f surjektiv.*

(c) *f ist bijektiv $\Leftrightarrow$ es gibt eine Abbildung $g\colon B \to A$ mit $g \circ f = \mathrm{id}_A$ und $f \circ g = \mathrm{id}_B$.*

*In diesem Fall heißt g die **Umkehrabbildung** von f.*

Beweis. (a) Sei also angenommen, dass es $g\colon B \to A$ gibt mit $g \circ f = \mathrm{id}_A$. Wir wollen zeigen, dass f injektiv ist. Seien $a, a' \in A$ mit $f(a) = f(a')$. Dann folgt

$$a = \mathrm{id}_A(a) = (g \circ f)(a) = g\big(f(a)\big) = g\big(f(a')\big) = (g \circ f)(a') = \mathrm{id}_A(a') = a'.$$

(b) Es gebe $g\colon B \to A$ mit $f \circ g = \mathrm{id}_B$. Wir wollen zeigen, dass f surjektiv ist. Sei dazu $b \in B$ und setze $a := g(b) \in A$. Dann gilt $f(a) = f\big(g(b)\big) = (f \circ g)(b) = \mathrm{id}_B(b) = b$.

(c) Wir müssen die beiden Richtungen der Äquivalenz zeigen. Nehmen wir zuerst an, dass es $g\colon B \to A$ gibt mit $g \circ f = \mathrm{id}_A$ und $f \circ g = \mathrm{id}_B$. Also erfüllt g die Bedingungen in (a) und (b). Dann ist f injektiv und surjektiv, also bijektiv.

Umgekehrt sei nun f als bijektiv angenommen. Wir müssen zeigen, dass es $g\colon B \to A$ gibt mit $g \circ f = \mathrm{id}_A$ und $f \circ g = \mathrm{id}_B$. Wir definieren g wie folgt. Sei $b \in B$. Da f surjektiv ist, gibt es ein $a \in A$ mit $f(a) = b$. Da f injektiv ist, gibt es nur eine Möglichkeit für dieses a; wir setzen $g(b) := a$. Dann folgt $g\big(f(a)\big) = a$ für alle $a \in A$ und $f\big(g(b)\big) = b$ für alle $b \in B$. □

Für jedes $n \in \mathbb{N}$ können wir die Menge $\{k \in \mathbb{N} \mid k \leqslant n\} = \{1, 2, \ldots, n\}$ bilden, diese hat offenbar genau n Elemente. Allgemein definieren wir:

Definition 5.6. (a) Seien A, B nicht leere Mengen. Dann heißen A, B ***gleichmächtig***, wenn es eine bijektive Abbildung $f\colon A \to B$ gibt. Wir schreiben in diesem Fall $|A| = |B|$.

(b) Gibt es ein $n \in \mathbb{N}$, so dass A gleichmächtig zu $\{1, \ldots, n\}$ ist, so schreiben wir einfach $|A| = n$ und sagen, dass A eine ***endliche Menge*** ist. Es gibt dann also eine bijektive Abbildung $f\colon \{1, \ldots, n\} \to A$, und A besteht genau aus den n Elementen $f(1), \ldots, f(n)$.

(c) Wenn es kein n wie in (b) gibt, so schreiben wir $|A| = \infty$. In diesem Fall hat A unendlich viele Elemente. Schließlich: Ist $A = \varnothing$, so setzen wir $|A| = 0$.

Zum Beispiel ist $\mathbb{N} \subsetneqq \mathbb{N}_0$, aber dennoch $|\mathbb{N}| = |\mathbb{N}_0|$, denn $f\colon \mathbb{N}_0 \to \mathbb{N}$, $n \mapsto n+1$, ist eine Bijektion ($\rightsquigarrow$ "Hilberts Hotel"). Bleiben wir zunächst bei endlichen Mengen.

Bemerkung 5.7. Seien A und B nicht-leere endliche Mengen. Dann ist auch $A \cup B$ endlich.
(a) Gilt $A \cap B = \varnothing$, so folgt $|A \cup B| = |A| + |B|$.
(b) Im Allgemeinen ist $|A \cup B| = |A| + |B| - |A \cap B|$.

Beweis. (a) Sei $n \in \mathbb{N}$ so, dass es eine bijektive Abbildung $f\colon \{1, \dots, n\} \to A$ gibt. Sei $m \in \mathbb{N}$ so, dass es eine bijektive Abbildung $g\colon \{1, \dots, m\} \to B$ gibt. Definiere dann die Abbildung $h\colon \{1, \dots, n+m\} \to A \cup B$ durch $h(i) := \begin{cases} f(i) & \text{falls } 1 \leqslant i \leqslant n, \\ g(i-n) & \text{falls } n < i \leqslant n+m. \end{cases}$
Man prüft sofort nach, dass h eine bijektive Abbildung ist.

(b) Sei $A' := A \setminus (A \cap B)$. Dann gilt $A = A' \cup (A \cap B)$, und die Vereingung ist disjunkt. Mit (a) folgt $|A| = |A'| + |A \cap B|$. Außerdem ist $A \cup B = A' \cup B$, und die Vereinigung ist disjunkt. Damit $|A \cup B| = |A'| + |B| = |A| - |A \cap B| + |B|$. □

Lemma 5.8. *Seien A, B nicht-leere, endliche Mengen und $f\colon A \to B$ eine Abbildung.*
(a) *Ist f injektiv, so gilt $|A| \leqslant |B|$.*
(b) *Ist f surjektiv, so gilt $|A| \geqslant |B|$.*
(c) *Es gelte $|A| = |B|$. Ist f injektiv oder surjektiv, so ist f bijektiv.*

Beweis. Sei $|A| = n \in \mathbb{N}$ und $|B| = m \in \mathbb{N}$. Also ist $A = \{a_1, \dots, a_n\}$ und $B = \{b_1, \dots, b_m\}$.

(a) Ist f injektiv, so sind $f(a_1), \dots, f(a_n)$ alle verschieden, also ist $|f(A)| = n$. Wegen $f(A) \subseteq B$ folgt $|A| = n = |f(A)| \leqslant |B|$.
(b) Ist f surjektiv, so wähle zu jedem $j \in \{1, \dots, m\}$ ein $i_j \in \{1, \dots, n\}$ mit $f(a_{i_j}) = b_j$. Dann sind $a_{i_1}, \dots, a_{i_m} \in A$ alle verschieden, also $|A| \geqslant m = |B|$.
(c) Sei $|A| = |B|$. Ist f injektiv, so ist wie oben $|A| = |f(A)|$. Wegen $|A| = |B|$ folgt also $|f(A)| = |B|$, und damit $f(A) = B$, d.h., f ist auch surjektiv. Ist f surjektiv, so folgt $A = f^{-1}(b_1) \cup \ldots \cup f^{-1}(b_m)$, wobei jedes $f^{-1}(b_j)$ nicht leer ist und die Vereinigung disjunkt ist. Damit $m = |A| = |f^{-1}(b_1)| + \ldots + |f^{-1}(b_m)|$ (siehe Bemerkung 5.7), wobei jeder Summand $\geqslant 1$ ist. Da die ganze Summe gleich m ist, muss jeder Summand gleich 1 sein, also f injektiv. □

Im Folgenden bestimmen wir nun noch die Mächtigkeiten von endlichen Mengen bei einigen weiteren Konstruktionen.

Beispiel 5.9. Seien A, B nicht-leere Mengen. Mit $\mathrm{Abb}(A, B)$ bezeichnen wir die Menge aller Abbildungen $f\colon A \to B$. Seien nun A, B endlich. Dann gilt $|\mathrm{Abb}(A, B)| = |B|^{|A|}$.

Denn: Seien $|A| = n$ und $|B| = m$; sei $A = \{a_1, \ldots, a_n\}$. Um $f\colon A \to B$ zu definieren, haben wir für $f(a_1)$ genau m Möglichkeiten (nämlich eines der m Elemente von B), ebenso für $f(a_2)$ und so fort. Also insgesamt m^n Möglichkeiten.

Beispiel 5.10. Seien A, B nicht-leere, endliche Mengen. Dann gilt $|A \times B| = |A| \cdot |B|$.
Denn: Seien $|A| = n$ und $|B| = m$. Für $(a, b) \in A \times B$ gibt es n Möglichkeiten für die erste Komponente $a \in A$, und für jede Wahl von $a \in A$ dann jeweils m Möglichkeiten für die zweite Komponente, also insgesamt nm Möglichkeiten.

Beispiel 5.11. Seien A_1, A_2, A_3 nicht-leere Mengen. Dann definieren wir $A_1 \times A_2 \times A_3 := (A_1 \times A_2) \times A_3$, und schreiben $\big((a_1, a_2), a_3\big)$ einfach als (a_1, a_2, a_3). Die Elemente von $A_1 \times A_2 \times A_3$ sind damit Tripel (a_1, a_2, a_3) mit $a_1 \in A_1$, $a_2 \in A_2$, $a_3 \in A_3$. Allgemeiner: Ist $n \geqslant 2$ und sind $A_1, A_2, \ldots, A_n$ nicht-leere Mengen, so definieren wir rekursiv $A_1 \times A_2 \times \ldots \times A_n := (A_1 \times \ldots \times A_{n-1}) \times A_n$. Die Elemente von $A_1 \times \ldots \times A_n$ schreiben wir als $(a_1, \ldots, a_n)$ mit $a_i \in A_i$ für $1 \leqslant i \leqslant n$; diese Elemente heißen n-***Tupel***. Mit einer einfachen vollständigen Induktion nach n folgt: Sind $A_1, \ldots, A_n$ endlich, so gilt $|A_1 \times \ldots \times A_n| = |A_1| \cdot |A_2| \cdot \ldots \cdot |A_n|$.

Bemerkung 5.12. Sei $n \in \mathbb{N}$ und seien $A_1, \ldots, A_n$ nicht-leere Mengen. Rekursiv haben wir oben $A_1 \times \ldots \times A_n = \{(a_1, \ldots, a_n) \mid a_i \in A_i \text{ für } 1 \leqslant i \leqslant n\}$ definiert. Wir sehen nun:

Sei $A := A_1 \cup \ldots \cup A_n$. Dann können wir ein n-Tupel $(a_1, \ldots, a_n)$ auch als Abbildung $f\colon \{1, \ldots, n\} \to A$ auffassen, mit $a_i = f(i) \in A_i$ für $1 \leqslant i \leqslant n$.
Mit dieser Identifizierung können wir auch definieren:

$$A_1 \times A_2 \times \ldots \times A_n := \{f \in \mathrm{Abb}(\{1, 2, \ldots, n\}, A) \mid f(i) \in A_i \text{ for } 1 \leqslant i \leqslant n\}.$$

Ab hier Woche 4

Definition 5.13. Seien $n \in \mathbb{N}$ und $k \in \mathbb{N}_0$. Dann bezeichnen wir mit dem Symbol $\binom{n}{k}$ die Anzahl der Teilmengen von $\{1, \ldots, n\}$ mit genau k Elementen. Für $n = 0$ setzen wir $\binom{0}{0} = 1$, und $\binom{0}{k} = 0$ falls $k \geqslant 1$. Die Symbole $\binom{n}{k}$ heissen ***Binomialkoeffizienten***.

Beispiele: $\binom{n}{0} = 1 = \binom{n}{n}$ für alle $n \in \mathbb{N}_0$. Ist $k > n$, so gilt offenbar $\binom{n}{k} = 0$.
Es gilt $\binom{4}{2} = 6$, denn es gibt 6 Teilmengen von $\{1, 2, 3, 4\}$ mit 2 Elementen, nämlich $\{1, 2\}$, $\{1, 3\}$, $\{1, 4\}$, $\{2, 3\}$, $\{2, 4\}$, $\{3, 4\}$.

Satz 5.14 (***Pascal–Dreieck***, um 1655)**.** *Für alle* $n, k \in \mathbb{N}$ *gilt* $\displaystyle\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.

Beweis. Ist $n = 1$, so gilt $\binom{1}{0} = \binom{1}{1} = 1$ und die Formel folgt mit den obigen Konventionen für $\binom{0}{k}$. Wir führen folgende Bezeichnungen ein:

$$\begin{aligned}
T(n, k) &:= \text{Menge der Teilmengen von } \{1, \ldots, n\} \text{ mit genau } k \text{ Elementen},\\
T_1(n, k) &:= \{S \in T(n, k) \mid n \in S\}.\\
T_0(n, k) &:= \{S \in T(n, k) \mid n \notin S\} = T(n-1, k) \qquad (\text{für } n \geqslant 2).
\end{aligned}$$

Sei nun $n \geqslant 2$. Es ist offenbar $T(n,k) = T_1(n,k) \cup T_0(n,k)$ und die Vereinigung ist disjunkt. Mit Bemerkung 5.7 erhalten wir

$$\binom{n}{k} = |T(n,k)| = |T_1(n,k)| + |T_0(n,k)| = |T_1(n,k)| + |T(n-1,k)| = |T_1(n,k)| + \binom{n-1}{k}.$$

Wir müssen jetzt noch zeigen, dass $|T_1(n,k)| = \binom{n-1}{k-1}$ gilt. Nun ist die rechte Seite gleich $|T(n-1,k-1)|$, also bleibt $|T_1(n,k)| = |T(n-1,k-1)|$ zu zeigen. Dazu definieren wir Abbildungen:

$$\begin{array}{llllll} f\colon & T(n-1,k-1) & \to & T_1(n,k), & S & \mapsto & S \cup \{n\}, \\ g\colon & T_1(n,k) & \to & T(n-1,k-1), & S' & \mapsto & S' \setminus \{n\}. \end{array}$$

Dann sind $f \circ g$ und $g \circ f$ jeweils die identischen Abbildungen, also ist f bijektiv (siehe Lemma 5.5(c)) und damit $|T_1(n,k)| = |T(n-1,k-1)| = \binom{n-1}{k-1}$. □

Für $m \in \mathbb{N}$ heißt $m! := 1 \cdot 2 \cdot \ldots \cdot m$ die ***Fakultät*** von m; Konvention: $0! := 1$.

Folgerung 5.15. *Für alle* $n, k \in \mathbb{N}_0$ *mit* $0 \leqslant k \leqslant n$ *gilt* $\displaystyle\binom{n}{k} = \frac{n!}{k!(n-k)!}$.

Beweis. (Vollständige Induktion über n mit Startwert $n_0 = 1$.) Induktionsanfang: Für $n = 1$ $\binom{1}{1} = 1!/(1!0!)$ und $\binom{1}{0} = 1!/(0!1!)$. Induktionsschritt: Sei nun $n \geqslant 2$ und die Behauptung bereits für $n-1$ bewiesen. Sei $0 \leqslant k \leqslant n$. Ist $k = n$, so gilt $\binom{n}{n} = 1 = n!/(n!0!)$, also die Behauptung. Sei nun $0 \leqslant k \leqslant n-1$. Nach Induktion und mit Satz 5.14 erhält man

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k} = \frac{(n-1)!}{(k-1)!((n-1)-(k-1))!} + \frac{(n-1)!}{k!(n-1-k)!}.$$

Mit einer einfachen Rechnung sieht man, dass die rechte Seite gleich $n!/(k!(n-k)!)$ ist. □

Lemma 5.16. *Sei* $n \in \mathbb{N}$. *Dann ist* $n! = |\{f\colon \{1,\ldots,n\} \to \{1,\ldots,n\} \mid f \text{ bijektiv }\}|$.

Beweis. Um eine injektive Abbildung $f\colon \{1,\ldots,n\} \to \{1,\ldots,n\}$ zu definieren, gibt es zunächst n Möglichkeiten für $f(1)$ (nämlich irgendeine der Zahlen $1,\ldots,n$).
Damit f injektiv wird, gibt es dann noch $n-1$ Möglichkeiten für $f(2)$ (nämlich irgendeine der Zahlen $1,\ldots,n$ außer $f(1)$).
Für $f(3)$ gibt es dann noch $n-2$ Möglichkeiten (alle Zahlen außer $f(1), f(2)$).
Nach $n-1$ Schritten sind dann bereits $n-1$ Zahlen für die Werte $f(1),\ldots,f(n-1)$ verbraucht, also bleibt für $f(n)$ noch genau eine Möglichkeit übrig.

Damit hat man also insgesamt $n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 1 = n!$ Möglichkeiten für f. Mit Lemma 5.8 ist jedes solche injektive f automatisch bijektiv. □

Für mehr dazu siehe auch `https://de.wikipedia.org/wiki/Abzählende_Kombinatorik`.

6. *Unendliche Mengen*

In diesem (kurzen) Abschnitt stellen wir einige Aussagen und Beispiele zu Mengen mit unendlich vielen Elementen zusammen, die teilweise ziemlich verblüffend sind. Zunächst gibt es zwei Arten von "Unendlichkeit". Eine nicht-leere, unendliche Menge A, die gleichmächtig zu $\mathbb{N}$ ist (oder zu $\mathbb{N}_0$), heißt ***abzählbar unendlich***. Sonst heißt A ***überabzählbar***. Ist A abzählbar, so gibt es eine Bijektion $f\colon \mathbb{N} \to A$. Setzen wir $a_n := f(n)$ für alle $n \in \mathbb{N}$, so ist also $A = \{a_1, a_2, a_3, \ldots\}$ eine "Aufzählung" der Elemente von A.

- $\mathbb{Z}$ ist abzählbar unendlich, denn wir können eine bijektive Abbildung $f\colon \mathbb{Z} \to \mathbb{N}$ zum Beispiel wie folgt definieren: $$f(n) = \begin{cases} 2n+1 & \text{falls } n \geqslant 0, \\ -2n & \text{falls } n < 0. \end{cases}$$
- $\mathbb{N}_0 \times \mathbb{N}_0$ ist abzählbar, siehe Beispiel 5.2(d);
- $\mathbb{Q}$ ist ebenfalls abzählbar (siehe Übungen).

In der Analysis-Vorlesung wird gezeigt, dass $\mathbb{R}$ überabzählbar ist. Weiteres Beispiel (das wirklich Erstaunliche am folgenden Satz ist der genial einfache Beweis):

Satz 6.1 (Georg Cantor, um 1880)**.** *Ist A eine nicht-leere Menge, so gibt es keine surjektive Abbildung $f\colon A \to \mathcal{P}(A)$. Also kann A auch nicht gleichmächtig zu $\mathcal{P}(A)$ sein.*
Insbesondere ist die Potenzmenge $\mathcal{P}(\mathbb{N})$ überabzählbar.

Beweis. Annahme, es gibt eine surjektive Abbildung $f\colon A \to \mathcal{P}(A)$. Betrachte dann die Menge $B := \{x \in A \mid x \notin f(x)\} \in \mathcal{P}(A)$. Da f surjektiv ist, gibt es ein $a \in A$ mit $B = f(a)$. Nun gilt aber: $a \in f(a) \Leftrightarrow a \in B \Leftrightarrow a \notin f(a)$. Also erhalten wir einen Widerspruch.

Nun betrachte $A = \mathbb{N}$. Die Abbildung $f\colon \mathbb{N} \to \mathcal{P}(\mathbb{N})$, $n \mapsto \{n\}$, ist injektiv, also ist $\mathcal{P}(\mathbb{N})$ unendlich. Da $\mathbb{N}$ nicht gleichmächtig zu $\mathcal{P}(\mathbb{N})$ ist, folgt also, dass $\mathcal{P}(\mathbb{N})$ überabzählbar ist. □

Die Frage, ob $\mathcal{P}(\mathbb{N})$ gleichmächtig zu $\mathbb{R}$ ist, wird als ***Kontinuumshypothese*** bezeichnet, siehe `https://de.wikipedia.org/wiki/Kontinuumshypothese`.

Satz 6.2. *Sei A eine unendliche Menge. Dann gibt es eine injektive Abbildung $f\colon \mathbb{N}_0 \to A$, d.h., setzt man $a_n := f(n)$ für $n \in \mathbb{N}_0$, so erhält man eine unendliche Folge von paarweise verschiedenen Elementen $a_0, a_1, a_2, \ldots$ in A.*

Idee des Beweises: Zuerst wähle irgendeinen Startwert $a_0 \in A$.

- Jetzt betrachte $A_1 := A \setminus \{a_0\}$. Dann ist immer noch $|A_1| = \infty$, also $A_1 \neq \varnothing$. Wähle irgendein $a_1 \in A_1$; dann ist auch $a_1 \neq a_0$.
- Jetzt betrachte $A_2 := A_1 \setminus \{a_1\} = A \setminus \{a_0, a_1\}$. Dann ist immer noch $|A_2| = \infty$, also $A_2 \neq \varnothing$. Wähle irgendein $a_2 \in A_2$; dann ist auch $a_2 \neq a_0$ und $a_2 \neq a_1$.
- Jetzt betrachte $A_3 := A_2 \setminus \{a_2\} = A \setminus \{a_0, a_1, a_2\}, \ldots$ usw. usw.

Aber das Problem ist hier das "usw. usw." ! Wie macht man so etwas präzise? Dazu brauchen wir zwei Hilfsmittel (auf die wir aber nur kurz eingehen werden).

Das erste dieser Hilfsmittel hat mit ***rekursiven Definitionen*** zu tun, mit denen Sie vermutlich vertraut sind. Als Beispiel betrachten wir die Folge $(a_n)_{n\in\mathbb{N}}$ von natürlichen Zahlen, die nach folgendem Schema gebildet wird. Sei $a_1 \in \mathbb{N}$ ein fest gewählter Startwert und dann

$$a_{n+1} = \begin{cases} 3a_n + 1 & \text{falls } a_n \text{ ungerade,} \\ a_n/2 & \text{falls } a_n \text{ gerade.} \end{cases}$$

Mit $a_1 = 19$ erhält man z.B. die Folge $19, 58, 29, 88, 44, 22, 11, 34, 17, 52, 26, 13, 40, 20, 10, 5, 16, 8, 4, 2, 1, 4, 2, 1, 4, 2, 1, \ldots$ (Übrigens: Versuchen Sie das Gleiche mit einem anderen a_1; fällt Ihnen etwas auf? Siehe dazu auch `https://de.wikipedia.org/wiki/Collatz-Problem`.)

Wenn man sich eine solche "Definition" genauer anschaut, so haben wir streng genommen lediglich eine Vorschrift, mit der man das jeweils nächste Folgenglied aus dem vorherigen berechnet. Dass man damit eine auf ganz $\mathbb{N}$ definierte Abbildung erhält, ist zunächst — und überhaupt — nicht klar. Die formale Begründung wird durch folgenden Satz geliefert.

Satz 6.3 (Rekursionssatz)**.** *Sei A eine nicht-leere Menge, $a_0 \in A$ fest. Für jedes $n \in \mathbb{N}_0$ sei eine Abbildung $h_n \colon A \to A$ gegeben. Dann gibt es genau eine Abbildung $F \colon \mathbb{N}_0 \to A$ mit*

$$F(0) = a_0 \qquad \textit{und} \qquad F(n+1) = h_n\big(F(n)\big) \quad \textit{für alle } n \in \mathbb{N}_0.$$

(Für einen formalen Beweis siehe §12 im Buch von Halmos.) Weiteres Beispiel:
Sei $A = \mathbb{Q}_{>0} := \{x \in \mathbb{Q} \mid x > 0\}$ und $h \colon \mathbb{Q}_{>0} \to \mathbb{Q}_{>0}$ gegeben durch

$$h(x) = \tfrac{1}{2}\big(x + \tfrac{2}{x}\big) \qquad \text{für alle } x \in \mathbb{Q},\ x > 0.$$

Sei $a_0 = 2$ und $h_n = h$ für $n \in \mathbb{N}_0$. Sei F die zugehörige Abbildung aus Satz 6.3. Setze $a_n := F(n)$ für $n \in \mathbb{N}$. Dann ist $(a_n)_{n\in\mathbb{N}_0}$ eine Folge mit $a_0 = 2$ und

$$a_{n+1} = F(n+1) = h(F(n)) = h(a_n) = \frac{1}{2}\Big(a_n + \frac{2}{a_n}\Big) \quad \text{für alle } n \geqslant 0.$$

Diese Folge kommt Ihnen vielleicht bekannt vor: Sie konvergiert gegen $\sqrt{2}$. (Mehr dazu in der Analysis-Vorlesung.)
Die Abbildungen h_n sind also die Vorschriften, mit denen man das jeweils nächste Folgenglied aus dem vorherigen berechnet; diese Abbildungen können sogar selbst von n abhängen.

Beispiel 6.4 (Siehe auch `https://de.wikipedia.org/wiki/Fibonacci-Folge`)**.**
Sei $(f_n)_{n\in\mathbb{N}_0}$ die von Leonardo Fibonacci (um 1202!) rekursiv definierte Folge mit

$$f_0 := 0, \qquad f_1 := 1 \qquad \text{und} \qquad f_{n+1} := f_n + f_{n-1} \quad \text{für alle } n \geqslant 1.$$

Also $0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, \ldots, 12586269025\ (n = 50), \ldots$
Hier braucht mal also jeweils zwei vorhergehende Folgenglieder, um ein neues Folgenglied

auszurechnen. — Wie passt dies in den Rekursionssatz?
Dazu sei $A := \mathbb{N}_0 \times \mathbb{N}_0$; definiere $h\colon A \to A$ durch $h(i,j) := (j, i+j)$ für alle $(i,j) \in \mathbb{N}_0 \times \mathbb{N}_0$. Nach dem Rekursionssatz gibt es eine Abbildung $F\colon \mathbb{N}_0 \to A$ mit $F(0) = (0,1)$ und $F(n+1) = h(F(n))$ für alle $n \geqslant 0$. Dann erhält man:

$$F(1) = h(F(0)) = h(0,1) = (1,1), \qquad F(2) = h(F(1)) = h(1,1) = (1,2),$$
$$F(3) = h(F(2)) = h(1,2) = (2,3), \qquad F(4) = h(F(3)) = h(2,3) = (3,5), \qquad \dots$$

Schreibe nun $F(n) = (x_n, y_n)$ für alle $n \in \mathbb{N}_0$. Dann ist $x_0 = 0$, $y_0 = 1$ und $y_n = x_{n+1} = x_n + x_{n-1}$ für alle $n \geqslant 1$. Also ist $f_n = x_n$ für alle $n \in \mathbb{N}_0$.

Das zweite Hilfsmittel ist ein weiteres, berühmtes Axiom der Mengenlehre.

Axiom 6.5 (***Auswahlaxiom***, Ernst Zermelo 1904)**.** *Sei A eine nicht-leere Menge und $\mathcal{P}(A)^\natural := \mathcal{P}(A) \setminus \{\varnothing\}$. Dann gibt es eine Abbildung $\alpha\colon \mathcal{P}(A)^\natural \to A$ mit $\alpha(B) \in B$ für alle nicht-leeren Teilmengen $B \subseteq A$.*

Eine solche Abbildung α heißt ***Auswahlfunktion***, denn sie "wählt" aus jeder nicht-leeren Teilmenge $B \subseteq A$ ein Element $\alpha(B) \in B$ aus.

Beispiel. Sei $A = \mathbb{N}$. Hier ist eine Auswahlfunktion $\alpha\colon \mathcal{P}(\mathbb{N})^\natural \to \mathbb{N}$ durch Peano's Induktionsaxiom gegeben: $\alpha(B) = \min(B)$ für jede nicht-leere Teilmenge $B \subseteq \mathbb{N}$.

Hier sehen wir jetzt, wo das Problem liegt: Versuchen Sie, eine Auswahlfunktion für $A = \mathbb{R}$ hinzuschreiben — Das ist bisher noch niemandem gelungen !

Das Auswahlaxiom garantiert also die Existenz von Etwas, das man in vielen Fällen (vor allem wenn man mit unendlichen Mengen zu tun) gar nicht konkret hinschreiben oder mit einer expliziten Formel bestimmen kann. Für eine weitere Diskussion siehe

`https://de.wikipedia.org/wiki/Auswahlaxiom`

Skizzieren wir kurz, wie man damit Satz 6.2 beweist. Sei also $A \neq \varnothing$ und $|A| = \infty$. Zu zeigen: Es gibt eine injektive Abbildung $f\colon \mathbb{N}_0 \to A$. Nun, nach dem Auswahlaxiom gibt es eine Auswahlfunktion $\alpha\colon \mathcal{P}(A)^\natural \to A$. Sei $a_0 := \alpha(A)$. Mit Hilfe des Rekursionssatzes können wir dann eine Folge $(a_n)_{n\in\mathbb{N}_0}$ definieren mit

$$a_{n+1} = \alpha(A \setminus \{a_0, a_1, \dots, a_n\}) \qquad \text{für alle } n \geqslant 0.$$

Dann gilt $a_{n+1} \notin \{a_0, a_1, \dots, a_n\}$ für alle $n \geqslant 0$, also sind die Elemente $a_0, a_1, a_2, \dots$ in A alle verschieden. Damit ist $f\colon \mathbb{N}_0 \to A$, $n \mapsto a_n$, die gesuchte injektive Abbildung. □

Folgerung 6.6. (a) *Sei $A \subseteq \mathbb{N}_0$ nicht-leer und $|A| = \infty$. Dann ist A abzählbar unendlich.*
(b) *Sei A eine nicht-leere, unendliche Menge und $g\colon \mathbb{N}_0 \to A$ eine surjektive Abbildung. Dann ist auch A abzählbar unendlich.*

Damit lassen sich bereits viele Beweise zu abzählbar unendlichen Mengen führen; Beispiele in den Übungen.

Beweis. (a) Für $A \subseteq \mathbb{N}_0$ ist eine Auswahlfunktion $\alpha\colon \mathcal{P}(A)^\natural \to A$ gegeben durch $\alpha(B) = \min(B)$ für alle $B \in \mathcal{P}(A)^\natural$. Wir erhalten eine injektive Abbildung $f\colon \mathbb{N}_0 \to A$ mit $f(0) = \min(A)$ und $f(n+1) = \min(A \setminus \{f(0), f(1), \ldots, f(n)\}) \in A$ für alle $n \geqslant 0$. Dann folgt sofort $A = f(\mathbb{N}_0)$. (Denn für ein gegebenes $n_0 \in A$ ist die Menge $B := \{k \in \mathbb{N}_0 \mid n_0 \leqslant f(k)\}$ nicht leer und dann $n_0 = f(m_0)$, wobei $m_0 := \min(B)$.) Also ist f bijektiv und damit $|A| = |\mathbb{N}_0|$.

(b) Da $g\colon \mathbb{N}_0 \to A$ surjektiv ist, gilt $\mathbb{N}_0 = \bigcup_{a\in A} g^{-1}(a)$ mit $g^{-1}(a) \neq \varnothing$ für alle $a \in A$. Für $a \in A$ sei $n_a := \min\bigl(g^{-1}(a)\bigr) \in \mathbb{N}_0$; damit erhalten wir eine Abbildung $f\colon A \to \mathbb{N}_0$, $a \mapsto n_a$. Es gilt $(g \circ f)(a) = g\bigl(f(a)\bigr) = g(n_a) = a$ für alle $a \in A$. Also ist $g \circ f = \mathrm{id}_A$ und damit ist f injektiv, siehe Lemma 5.5(a). Setze nun $B := f(A) = \{n_a \mid a \in A\} \subseteq \mathbb{N}_0$. Dann ist $f\colon A \to B$ eine bijektive Abbildung, also $|A| = |B|$. Nun ist B eine unendliche Teilmenge von $\mathbb{N}_0$, also nach (a) selbst abzählbar unendlich. Also ist auch A abzählbar unendlich. □

Zum Schluss noch eine weitere verblüffende Eigenschaft von unendlichen Mengen:

Folgerung 6.7 (Richard Dedekind, um 1888)**.** *Sei A eine nicht-leere Menge. Dann ist A unendlich genau dann, wenn es eine echte Teilmenge $B \subsetneqq A$ gibt mit $|A| = |B|$.*

Beweis. Sei zuerst angenommen, dass es eine Teilmenge $B \subsetneqq A$ mit $|B| = |A|$ gibt. Dann ist $f\colon B \to A$, $b \mapsto b$, injektiv. Wäre A endlich, so müsste f auch surjektiv sein (siehe Satz 5.9(c)), Widerspruch. Also ist A unendlich.

Umgekehrt: Sei A als unendlich angenommen. Nach Satz 6.2 gibt es eine injektive Abbildung $f\colon \mathbb{N}_0 \to A$. Sei $a_n := f(n)$ für alle $n \in \mathbb{N}_0$, und $A' := f(\mathbb{N}_0) = \{a_0, a_1, a_2, \ldots\} \subseteq A$.

Setze nun $B := A \setminus \{a_0\}$. Wir definieren eine Abbildung $g\colon A \to B$ durch

$$g(a) := \begin{cases} a & \text{falls } a \notin A', \\ a_{n+1} & \text{falls } a \in A' \text{ und } a = a_n. \end{cases}$$

Man sieht sofort, dass g injektiv und surjektiv ist. Also ist $|A| = |B|$ aber $B \subsetneqq A$. □

Kapitel II: Algebraische Strukturen

7. *Verknüpfungen*

Sei A eine nicht-leere Menge. Eine Abbildung $A \times A \to A$, $(a, b) \mapsto a \star b$, heißt eine ***Verknüpfung*** auf A. Eine solche Verknüpfung heißt:

- ***assoziativ***, wenn $a \star (b \star c) = (a \star b) \star c$ für alle $a, b, c \in A$ gilt;
- ***kommutativ***, wenn $a \star b = b \star a$ für alle $a, b \in A$ gilt.

Ein Element $e \in A$ heißt ***neutrales Element*** bezüglich dieser Verknüpfung, wenn $a \star e = e \star a = a$ für alle $a \in A$ gilt. Gibt es ein solches neutrales Element e und ist $a \in A$, so heißt ein Element $b \in A$ ein ***Inverses*** zu a, wenn $a \star b = b \star a = e$ gilt.

Zum Beispiel ist die Addition auf $\mathbb{Z}$ assoziativ und kommutativ; $0 \in \mathbb{Z}$ ist das neutrale Element bezüglich "+" und jedes $n \in \mathbb{Z}$ besitzt ein Inverses, nämlich $-n$.

In $\mathbb{N}$ gibt es weder ein neutrales Element noch inverse Elemente bezüglich "+".

Bemerkung 7.1. (a) Gibt es ein neutrales Element, so ist dieses eindeutig bestimmt. Denn sind $e, e' \in A$ neutrale Elemente, so gilt $e' = e \star e' = e$, wobei die erste Gleichheit gilt, weil e ein neutrales Element ist, und die zweite, weil e' ein neutrales Element ist.

(b) Nehmen wir an, dass $\star$ assoziativ ist und es ein neutrales Element $e \in A$ gibt.
Gibt es zu $a \in A$ ein inverses Element $b \in A$, so ist dieses eindeutig bestimmt. Denn ist auch $c \in A$ invers zu a, so folgt $c = c \star e = c \star (a \star b) = (c \star a) \star b = e \star b = b$. Das Inverse zu a werde nun mit a' bezeichnet.

(c) Die Voraussetzungen seien wie in (b). Seien $a, b \in A$ und es gebe inverse Elemente $a' \in A$, $b' \in A$. Dann ist $b' \star a'$ das Inverse zu $a \star b$, d.h., $(a \star b)' = b' \star a'$. Denn es gilt

$$(a \star b) \star (b' \star a') = \big(a \star (b \star b')\big) \star a' = (a \star e) \star a' = a \star a' = e,$$

und genauso $(b' \star a') \star (a \star b) = e$.

Definition 7.2. Sei A eine nicht-leere Menge und $\star\colon A \times A \to A$ eine Verknüpfung. Dann heißt $(A, \star)$ eine ***Gruppe***, wenn $\star$ assoziativ ist, es ein neutrales Element $e \in A$ gibt und jedes $a \in A$ ein Inverses besitzt. Eine Gruppe heißt ***abelsch*** (zu Ehren von H. N. Abel), wenn die Verknüpfung kommutativ ist.

Zum Beispiel sind $(\mathbb{Z}, +)$ und $(\mathbb{Q} \setminus \{0\}, \cdot)$ abelsche Gruppen. Gruppen, die nicht abelsch sind, werden wir im nächsten Kapitel kennen lernen.

Definition 7.3. Sei A eine abelsche Gruppe; die Verknüpfung werde dabei mit "+" bezeichnet, das neutrale Element mit 0 und das Inverse von $a \in A$ mit $-a$. Es sei eine weitere

Verknüpfung $\cdot\colon A \times A \to A$ gegeben. Dann heißt $(A, +, \cdot)$ ein ***Ring***, wenn "$\cdot$" assoziativ ist und die Distributivregeln gelten, d.h.:

$$a \cdot (b + c) = a \cdot b + a \cdot c \qquad \text{und} \qquad (a + b) \cdot c = a \cdot c + b \cdot c \qquad \text{für alle } a, b, c \in A.$$

Sei $(A, +, \cdot)$ ein Ring. Gibt es ein neutrales Element $1 \in A$ bezüglich "$\cdot$", so heißt A ein ***Ring mit*** 1. Ist die Multiplikation "$\cdot$" kommutativ, so heißt A ein ***kommutativer Ring***.

Ein kommutativer Ring A mit 1, in dem $1 \neq 0$ gilt und jedes Element $0 \neq a \in A$ ein Inverses bezüglich "$\cdot$" besitzt, heißt ein ***Körper***. In diesem Fall wird das Inverse von $a \neq 0$ bezüglich der Multiplikation meist mit a^{-1} bezeichnet (manchmal auch $1/a$).

Zum Beispiel ist $(\mathbb{Z}, +, \cdot)$ ein kommutativer Ring mit 1, aber kein Körper; $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ sind Körper. Die Menge der geraden Zahlen $2\mathbb{Z} := \{2n \mid n \in \mathbb{Z}\}$ ist mit der üblichen Addition und Multiplikation ein kommutativer Ring, aber ohne 1.

Bemerkung 7.4. Sei $(R, +, \cdot)$ ein Ring. Dann gilt $0 \cdot r = r \cdot 0 = 0$ für alle $r \in R$. Denn

$$0 = (0 \cdot r) - (0 \cdot r) = (0 + 0) \cdot r - (0 \cdot r) = (0 \cdot r + 0 \cdot r) - (0 \cdot r) = 0 \cdot r$$

und genauso $r \cdot 0 = 0$. Sei nun R ein Ring mit 1. In der Definition wurde nicht ausgeschlossen, dass $1 = 0$ gilt. Ist dies der Fall, so folgt aber $r = r \cdot 1 = r \cdot 0 = 0$ für $r \in A$, d.h., $R = \{0\}$.

Lemma 7.5 (Nullteilerfreiheit)**.** *Sei $(K, +, \cdot)$ ein Körper und seien $a, b \in K$. Gilt $a \cdot b = 0$, so folgt $a = 0$ oder $b = 0$. Umgekehrt: Ist $a \neq 0$ und $b \neq 0$, so folgt $a \cdot b \neq 0$. Noch einmal anders ausgedrückt: Für festes $0 \neq a \in K$ ist die Abbildung $f\colon K \to K, \quad x \mapsto a \cdot x, \quad$ injektiv.*

Beweis. Es gelte $a \cdot b = 0$. Nehmen wir an, es ist auch $a \neq 0$. Dann müssen wir zeigen, dass $b = 0$ gilt. Dazu: Wegen $a \neq 0$ gibt es ein Inverses $a^{-1} \in K$.

Dann folgt $b = 1 \cdot b = (a^{-1} \cdot a) \cdot b = a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 = 0,$ wobei die letzte Gleichheit aus Bemerkung 7.4 folgt. Sei schließlich $0 \neq a \in K$ fest. Seien $x, y \in K$ mit $f(x) = f(y)$. Aus $a \cdot x = f(x) = f(y) = a \cdot y$ folgt $a \cdot (x - y) = a \cdot x - a \cdot y = 0$, also $x - y = 0$ (weil $a \neq 0$) und damit $x = y$. Also ist f injektiv. □

Sie kennen vermutlich schon die Formel im folgenden Satz (für reelle Zahlen a, b); nachdem die obigen Begriffe eingeführt sind, können wir diese für beliebige Ringe mit 1 beweisen.

Satz 7.6 (***Binomischer Lehrsatz***)**.** *Sei R ein Ring mit 1. Seien $a, b \in R$ mit $a \cdot b = b \cdot a$. Dann gilt für alle $n \in \mathbb{N}_0$:*

$$(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k \cdot b^{n-k} \qquad \textit{(Konvention: } r^0 = 1 \textit{ für alle } r \in R\textit{).}$$

Außerdem benutzen wir hier folgende Konvention, bezüglich des Produkts von $\binom{n}{k} \in \mathbb{N}_0$ und $a, b \in R$. Seien $m \in \mathbb{N}_0$ und $r \in R$. Dann setze $mr := 0$ falls $m = 0$; ist $m \geqslant 1$, so setze $mr := r + \ldots + r$, mit m Summanden.

Beweis. (Vollständige Induktion mit Startwert $n_0 = 0$.)

• Induktionsanfang. Sei $n = 0$. Dann ist die linke Seite $(a+b)^0$; die Summe auf der rechten Seite hat nur einen Term, nämlich $\binom{0}{0} a^0 b^0$. Beides Mal erhalten wir 1 als Ergebnis (mit unseren Konventionen zu $\binom{0}{0}$ und r^0).

• Induktionsschritt. Sei $n \geqslant 0$ und angenommen, die Formel gilt bereits für $(a+b)^n$. Nun

$$(a+b)^{n+1} = (a+b)^n \cdot (a+b) = \Big(\sum_{k=0}^{n} \binom{n}{k} a^k \cdot b^{n-k}\Big) \cdot (a+b)$$

$$= \Big(\sum_{k=0}^{n} \binom{n}{k} a^k \cdot b^{n-k} \cdot a\Big) + \Big(\sum_{k=0}^{n} \binom{n}{k} a^k \cdot b^{n-k} \cdot b\Big) = A + B,$$

wobei $\quad A = \sum_{k=0}^{n} \binom{n}{k} a^{k+1} \cdot b^{n-k} \quad$ und $\quad B = \sum_{k=0}^{n} \binom{n}{k} a^k \cdot b^{n+1-k}.$

(Hier haben wir benutzt, dass a und b miteinander vertauschbar sind.) Jetzt machen wir in A die Variablensubstitution $l = k+1$. Dann ist $k = l-1$, $n-k = n+1-l$; und nun läuft l von 1 bis $n+1$. Damit erhalten wir:

$$A = \sum_{l=1}^{n+1} \binom{n}{l-1} a^l \cdot b^{n+1-l} = \sum_{k=1}^{n+1} \binom{n}{k-1} a^k \cdot b^{n+1-k}.$$

Jetzt sehen die Terme, über die summiert wird, in A genauso aus wie in B, im neuen A läuft k von 1 bis $n+1$, in B weiterhin von 0 bis n. Also

$$A = \sum_{k=1}^{n+1} \binom{n}{k-1} a^k \cdot b^{n+1-k} = \Big(\sum_{k=1}^{n} \binom{n}{k-1} a^k \cdot b^{n+1-k}\Big) + \binom{n}{n} a^{n+1},$$

$$B = \sum_{k=0}^{n} \binom{n}{k} a^k \cdot b^{n+1-k} = \binom{n}{0} b^{n+1} + \Big(\sum_{k=1}^{n} \binom{n}{k} a^k \cdot b^{n+1-k}\Big).$$

Damit erhalten wir

$$A + B = \binom{n}{0} b^{n+1} + \Big(\sum_{k=1}^{n} \Big(\underbrace{\binom{n}{k-1} + \binom{n}{k}}_{= \binom{n+1}{k} \text{ Pascal–Dreieck}} \Big) a^k \cdot b^{n+1-k}\Big) + \binom{n}{n} a^{n+1}$$

$$= b^{n+1} + \Big(\sum_{k=1}^{n} \binom{n+1}{k} a^k \cdot b^{n+1-k}\Big) + a^{n+1}$$

Wegen $\binom{n+1}{0} = \binom{n+1}{n+1} = 1$ ist dies genau die gewünschte Summe auf der rechten Seite. $\square$

Ab hier Woche 5

Beispiel 7.7. Sei A eine endliche Menge mit $|A| = n \in \mathbb{N}$. Dann gilt $|\mathcal{P}(A)| = 2^n$.

Dazu: Wegen $|A| = n$ ist $A = \{a_1, a_2, \ldots, a_n\}$. Die Teilmengen von A entsprechen dann genau den Teilmengen von $\{1, 2, \ldots, n\}$, also gilt $|\mathcal{P}(A)| = |\mathcal{P}(\{1, 2, \ldots, n\})|$. Wir brauchen also nur den Fall $A = \{1, 2, \ldots, n\}$ zu behandeln. Wie im Beweis von Satz 5.14 (***Pascal–Dreieck***) sei $T(n, k) :=$ Menge der Teilmengen von $\{1, \ldots, n\}$ mit genau k Elementen, für $0 \leqslant k \leqslant n$.

Dann ist $\mathcal{P}(\{1, 2, \ldots, n\}) = T(n, 0) \cup T(n, 1) \cup \ldots \cup T(n, n)$, und diese Vereinigung ist disjunkt. Also folgt $|\mathcal{P}(\{1, 2, \ldots, n\})| = |T(n, 0)| + |T(n, 1)| + \ldots + |T(n, n)|$

$$= \binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{n} = \sum_{k=0}^{n} \binom{n}{k} = \sum_{k=0}^{n} \binom{n}{k} 1^k 1^{n-k} = (1+1)^n = 2^n,$$

wobei wir den Binomischen Lehrsatz mit $R = \mathbb{Z}$ und $a = b = 1$ verwenden. □

Folgerung 7.8 (***Kleiner Satz von Fermat***; um 1640)**.**
Sei p eine Primzahl. Dann gilt $n^p \equiv n \pmod{p}$ für alle $n \in \mathbb{Z}$.

Beweis. Sei zuerst $n \geqslant 0$. Dann zeigen wir die Aussage mit vollständiger Induktion nach n. Für $n = 0$ ist dies klar. Sei nun $n \geqslant 0$ beliebig und angenommen, die Aussage gelte bereits für n. Dann müssen wir $n + 1$ betrachten. Mit dem Binomischen Lehrsatz erhalten wir:

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

Betrachte nun $\binom{p}{k} = \frac{p(p-1)(p-2)\cdots(p-k+1)}{1 \cdot 2 \cdot \ldots \cdot k} \in \mathbb{N}$ für $k \in \{1, \ldots, p-1\}$. Der Zähler dieses Bruches ist durch p teilbar, aber wegen $1 \leqslant k \leqslant p-1$ ist der Nenner nicht durch p teilbar. Also folgt $p \mid \binom{p}{k}$ für alle diese k und die geklammerte Summe in obiger Formel ist $\equiv 0 \bmod p$. Nach Induktion ist $n^p \equiv n \bmod p$. Damit folgt $(n+1)^p \equiv 1 + n^p \equiv 1 + n \bmod p$, wie gewünscht.

Sei nun $n < 0$. Dann ist $-n > 0$, also wissen wir bereits, dass $(-1)^p n^p \equiv (-n)^p \equiv -n \bmod p$ gilt. Schließlich ist $(-1)^p \equiv -1 \bmod p$ für alle Primzahlen p (unterscheide die Fälle $p = 2$ und $p > 2$), also folgt auch hier $n^p \equiv n \bmod p$. □

8. *Die ganzen und rationalen Zahlen und die Ringe* $\mathbb{Z}/m\mathbb{Z}$

Wir haben bereits oben festgehalten, dass $\mathbb{Z}$ ein kommutativer Ring mit 1 und $\mathbb{Q}$ ein Körper ist, jeweils mit der üblichen Addition und Multiplikation; außerdem ist natürlich $\mathbb{Z} \subseteq \mathbb{Q}$ (indem wir $n \in \mathbb{Z}$ mit dem Bruch $n/1 \in \mathbb{Q}$ identifizieren).

In den meisten modernen Programmiersprachen kann man mit beliebig großen ganzen Zahlen exakt rechnen. Für rationale Zahlen ist dies auch möglich, indem man jedes $x \in \mathbb{Q}$ als gekürzten Bruch darstellt, also $x = n/m$ mit $n \in \mathbb{Z}$, $m \in \mathbb{N}$ und $\mathrm{ggT}(n, m) = 1$. Kommt in

einer Zwischenrechnung ein ungekürzter Bruch vor, so teilt man Zähler und Nenner durch ihren ggT und erhält wiederum einen gekürzten Bruch. Zum Beispiel:

$$3/22 + 9/10 = (3 \cdot 10 + 9 \cdot 22)/(22 \cdot 10) = (30 + 198)/220 = 228/220 = \ldots = 57/55.$$

In Python muss dazu ein extra-Paket geladen werden:

```
Python 3.9.7 (default, Aug 30 2021, 00:00:00)
>>> from fractions import Fraction
>>> Fraction(3,22)+Fraction(9,10)
Fraction(57, 55)
```

In GAP ist dies bereits eingebaut:

```
GAP 4.11.1 of 2021-03-02
gap> 3/22+9/10;
57/55
gap> Factorial(50);
30414093201713378043612608166064768844377641568960512000000000000
```

Nach all unseren Vorbereitungen im vorherigen Kapitel über den "mod" Operator, Kongruenzen usw. können wir hier nun eine neue Klasse von Ringen und Körpern einführen.

Zur Erinnerung: Sei $m \in \mathbb{N}$ fest. Für $n \in \mathbb{Z}$ sei $\overline{n}$ die Restklasse von n (modulo m), also $\overline{n} = \{a \in \mathbb{Z} \mid m \text{ teilt } n - a\} = \{a \in \mathbb{Z} \mid a \bmod m = n \bmod m\}$. Wie in Beispiel 4.10 ist $\{0, 1, \ldots, m-1\}$ ein Repräsentantensystem der Restklassen. Die Menge der Restklassen bezeichnen wir nun mit $\mathbb{Z}/m\mathbb{Z} := \{\overline{0}, \overline{1}, \ldots, \overline{(m-1)}\}$.

Satz 8.1. *Mit obigen Bezeichnungen können wir für alle $a, b \in \mathbb{Z}$ wie folgt eine Addition und eine Multiplikation für die zugehörigen Restklassen definieren:*

$$\overline{a} + \overline{b} := \overline{a+b} \qquad \textit{und} \qquad \overline{a} \cdot \overline{b} := \overline{ab}.$$

Mit diesen Verknüpfungen erhalten wir:

(a) $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ *ist ein kommutativer Ring mit Eins-Element* $\overline{1}$.

(b) *Sei $m \geqslant 2$. Dann gilt:* $\mathbb{Z}/m\mathbb{Z}$ *ist ein Körper* $\Leftrightarrow$ m *ist eine Primzahl.*

Beweis. Seien $a, b \in \mathbb{Z}$. Dann können wir $\overline{a+b}$ und $\overline{ab}$ bilden. Sind auch $c, d \in \mathbb{Z}$ mit $\overline{a} = \overline{c}$ und $\overline{b} = \overline{d}$ gegeben, so können wir entsprechend $\overline{c+d}$ und $\overline{cd}$ bilden. Damit es überhaupt Sinn macht, die Restklassen selbst zu addieren und zu multiplizieren, muss sichergestellt sein, dass bei den obigen beiden Rechnungen jeweils das gleiche Ergebnis herauskommt; aber dies ist gerade die Aussage von Lemma 4.11. Damit haben wir "wohl-definierte" Verknüpfungen

$$+ : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \qquad \text{und} \qquad \cdot : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}.$$

($\rightsquigarrow$ Hinweis auf "Topfrechnen")

(a) Zu den Ringaxiomem: Aufgrund der obigen Definition ist klar, dass $\overline{0}$ neutrales Element bezüglich "+" und $\overline{1}$ neutrales Element bezüglich "$\cdot$" ist. Jedes $\overline{a} \in \mathbb{Z}/m\mathbb{Z}$ hat ein Inverses bezüglich "+", nämlich $\overline{-a}$ (wegen $\overline{a} + \overline{(-a)} = \overline{a-a} = \overline{0}$). Nun müssen noch die weiteren Regeln gezeigt werden, also für alle $a, b, c \in \mathbb{Z}$:

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

Diese Regeln folgen aber unmittelbar aus den entsprechenden Regeln für $\mathbb{Z}$; zum Beispiel:

$$\overline{a} \cdot (\overline{b} + \overline{c}) = \overline{a} \cdot \overline{(b+c)} = \overline{a(b+c)} = \overline{ab + ac} = \overline{ab} + \overline{ac} = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c},$$

wobei beim 3. Gleichheitszeichen die Regel $a(b+c) = ab + ac$ für $a, b, c \in \mathbb{Z}$ verwendet wurde. Der Beweis der anderen Regeln verläuft analog und sei als Übung überlassen. Damit ist $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ ein kommutativer Ring mit 1.

(b) Sei nun $m \geqslant 2$. Dann ist jedenfalls $\overline{0} \neq \overline{1}$. Sei zuerst angenommen, dass $\mathbb{Z}/m\mathbb{Z}$ ein Körper ist. Dann müssen wir zeigen, dass m eine Primzahl ist. Nehmen wir an, m ist keine Primzahl, d.h., $m = ab$ mit $2 \leqslant a, b < m$. Dann gilt $\overline{a} \neq \overline{0}$ und $\overline{b} \neq \overline{0}$, aber auch $\overline{a} \cdot \overline{b} = \overline{ab} = \overline{m} = \overline{0}$, Widerspruch zu Lemma 7.5. Also war die Annahme falsch, d.h., m ist eine Primzahl.

Zum Beispiel gilt für $m = 4$: $\quad \overline{2} \cdot \overline{2} = \overline{4} = \overline{0}$, $\qquad$ oder für $m = 6$: $\quad \overline{2} \cdot \overline{3} = \overline{6} = \overline{0}$.

Umgekehrt sei nun $m = p$ eine Primzahl und $\overline{0} \neq \overline{a} \in \mathbb{Z}/p\mathbb{Z}$. Wir müssen zeigen: Es gibt ein Inverses zu $\overline{a}$ (bezüglich der Multiplikation). Dazu: Wegen $\overline{a} \neq \overline{0}$ ist $p \nmid a$, also $\mathrm{ggT}(p, a) = 1$. Nach dem ***Lemma von Bézout*** gibt es $r, s \in \mathbb{Z}$ mit $1 = rp + sa$. Dann ist aber $\overline{1} = \overline{rp + sa} = \overline{r} \cdot \overline{p} + \overline{s} \cdot \overline{a} = \overline{r} \cdot \overline{0} + \overline{s} \cdot \overline{a} = \overline{s} \cdot \overline{a}$, also ist $\overline{s} = \overline{a}^{-1}$ das gesuchte Inverse. □

Definition 8.2. Ist $m = p \in \mathbb{N}$ eine Primzahl, so wird $\mathbb{Z}/p\mathbb{Z}$ auch mit $\mathbb{F}_p = \{\overline{0}, \overline{1}, \ldots, \overline{(p-1)}\}$ bezeichnet und heißt ***endlicher Körper mit*** p ***Elementen***.

Zum Beispiel ist $\mathbb{F}_2 = \{\overline{0}, \overline{1}\}$ mit den Verknüpfungstabellen:

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

und

$\cdot$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

Dieser Körper spielt in der Informatik und in der Kodierungstheorie eine wichtige Rolle.

Beispiel 8.3. (a) Für $m = 1$ ist $\mathbb{Z}/1\mathbb{Z} = \{\overline{0}\}$ und natürlich $\overline{0} + \overline{0} = \overline{0} = \overline{0} \cdot \overline{0}$.

(b) Für $m = 3, 4$ sind die Verknüpfungstabellen wie folgt gegeben:

$m = 3$:

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

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

(also $\overline{2}^{-1} = \overline{2}$)

$m = 4$:

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

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

(kein Körper)

(c) In $\mathbb{F}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ gilt: $\overline{1}^{-1} = \overline{1}$, $\overline{2}^{-1} = \overline{3}$, $\overline{3}^{-1} = \overline{2}$, $\overline{4}^{-1} = \overline{4}$.

Beispiel 8.4. Wir können nun auch einen neuen Beweis für den ***Kleinen Satz von Fermat*** geben. Sei also p eine Primzahl und $n \in \mathbb{Z}$. Zu zeigen: $n^p \equiv n \bmod p$, oder anders ausgedrückt $\overline{n} = \overline{n^p} = \overline{n}^p$, wobei wir im Körper $\mathbb{F}_p$ rechnen.

Ist $\overline{n} = \overline{0}$, so ist die Aussage klar. Sei nun $\overline{n} \neq \overline{0}$. Dann betrachten wir die Abbildung $f\colon \mathbb{F}_p \to \mathbb{F}_p$, $\overline{x} \mapsto \overline{n} \cdot \overline{x}$. Diese ist injektiv nach Lemma 7.5 und Satz 8.1(b). Also ist f bijektiv nach Lemma 5.8(c), d.h.,

$$\{\overline{0},\ \overline{1},\ \overline{2},\ \ldots,\ \overline{(p-1)}\} = f(\mathbb{F}_p) = \{\overline{n}\cdot\overline{0},\ \overline{n}\cdot\overline{1},\ \overline{n}\cdot\overline{2}, \ldots,\ \overline{n}\cdot\overline{(p-1)}\}.$$

Auf beiden Seiten kommt hier $\overline{0} = \overline{n} \cdot \overline{0}$ vor (siehe Bemerkung 7.4), also ist auch

$$\{\overline{1},\ \overline{2},\ \ldots,\ \overline{(p-1)}\} = \{\overline{n}\cdot\overline{1},\ \overline{n}\cdot\overline{2},\ \ldots,\ \overline{n}\cdot\overline{(p-1)}\}.$$

Bilde das Produkt aller dieser Elemente:

$$\overline{1}\cdot\overline{2}\cdot\ldots\cdot\overline{(p-1)} = (\overline{n}\cdot\overline{1})\cdot(\overline{n}\cdot\overline{2})\cdot\ldots\cdot\big(\overline{n}\cdot\overline{(p-1)}\big) = \overline{n}^{p-1}\cdot\big(\overline{1}\cdot\overline{2}\cdot\ldots\cdot\overline{(p-1)}\big).$$

Wegen $\overline{1}\cdot\overline{2}\cdot\ldots\cdot\overline{(p-1)} \neq \overline{0}$ (Lemma 7.5) können wir diesen Faktor auf beiden Seiten kürzen (noch einmal Lemma 7.5) und erhalten $\overline{1} = \overline{n}^{p-1}$, also $\overline{n} = \overline{n}^p$, wie gewünscht. □

9. *Polynome und Polynomfunktionen*

Sei K ein Körper. Eine Funktion $f\colon K \to K$ heißt ***Polynomfunktion***, wenn es ein $n \in \mathbb{N}_0$ und Koeffizienten $a_0, a_1, a_2, \ldots, a_n \in K$ gibt mit

$$(*) \qquad f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \qquad \text{für alle } x \in K.$$

Ein bekanntes Beispiel ist sicherlich die Funktion $f\colon \mathbb{R} \to \mathbb{R}$ mit $f(x) = x^2$ für alle $x \in \mathbb{R}$.

Sei $P(K)$ die Menge aller Polynomfunktionen $f\colon K \to K$. Für $n \in \mathbb{N}_0$ sei $P_n(K) \subseteq P(K)$ die Teilmenge aller f wie oben, so dass $(*)$ gilt mit Koeffizienten $a_0, a_1, \ldots, a_n$. Sei $\hat{P}_n(K) \subseteq P_n(K)$ die Teilmenge aller f, so dass $(*)$ gilt mit $a_n \neq 0$.

Satz 9.1 (***Horner–Schema***). *Sei $n \geqslant 1$ und $f \in \hat{P}_n(K)$, d.h., es gibt $a_0, a_1, \ldots, a_n \in K$ mit $a_n \neq 0$ und $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ für alle $x \in K$. Sei $c \in K$ fest und definiere rekursiv wie folgt Elemente in K:*

$$b_{n-1} := a_n, \qquad b_{n-2} := a_{n-1} + b_{n-1}c, \qquad b_{n-3} := a_{n-2} + b_{n-2}c,$$
$$\ldots, \qquad b_1 := a_2 + b_2c, \qquad b_0 := a_1 + b_1c, \qquad r := a_0 + b_0c.$$

Sei $g \in \hat{P}_{n-1}(K)$ *definiert durch* $g(x) := b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \ldots + b_1x + b_0$ *für alle* $x \in K$. *Dann gilt* $f(x) = (x-c)g(x) + r$ *für alle* $x \in K$. *Insbesondere also* $f(c) = r$.

Beweis. Im Wesentlichen einfaches Nachrechnen. Für $x \in K$ gilt:

$$(x-c)g(x) = (x-c)\sum_{i=0}^{n-1} b_ix^i = \sum_{i=0}^{n-1} b_ix^{i+1} - \sum_{i=0}^{n-1} b_icx^i = \sum_{i=1}^{n} b_{i-1}x^i - \sum_{i=0}^{n-1} b_icx^i$$
$$= \underbrace{b_{n-1}}_{=a_n}x^n - \underbrace{b_0c}_{r-a_0} + \sum_{i=1}^{n-1} \underbrace{(b_{i-1} - b_ic)}_{=a_i}x^i = f(x) - r. \qquad \square$$

Bemerkung. Rechnet man $c, c^2, \ldots, c^n$ aus und dann $f(c) = a_nc^n + a_{n-1}c^{n-1} + \ldots + a_1c + a_0$, so braucht man insgesamt n Additionen und $2n-1$ Multiplikationen. Benutzt man das Horner-Schema, so benötigt man auch n Additionen, aber nur n Multiplikationen!
Sei zum Beispiel $f(x) = 2x^3 + 5x^2 - 11x - 3$ und $c = 2$, wobei $K = \mathbb{Q}$.

Horner-Schema:

Koeffs von f:	2	5	-11	-3
$c = 2$:	$\downarrow$	$+2 \cdot 2 = 4$	$+2 \cdot 9 = 18$	$+2 \cdot 7 = 14$
g:	2	9	7	$\boxed{11}$

Dann ist $g(x) = 2x^2 + 9x + 7$ und $r = f(2) = 11$. — Nachrechnen:
$(x-2)(2x^2 + 9x + 7) = 2x^3 + 9x^2 + 7x - 4x^2 - 18x - 14 = f(x) - 11$.

Folgerung 9.2. *Sei* $n \geqslant 1$ *und* $f \in \hat{P}_n(K)$. *Dann hat* f *höchstens* n *Nullstellen in* K.
(Nach Definition ist eine ***Nullstelle*** *von* f *ein Element* $c \in K$ *mit* $f(c) = 0$.*)*

Beweis. (Vollständige Induktion nach n.) Für $n = 1$ ist $f(x) = a_1x + a_0$ mit $a_1 \neq 0$. Also gibt es genau $n = 1$ Nullstelle, nämlich $c = -a_0a_1^{-1}$. Sei nun $n \geqslant 2$ und die Aussage bereits gezeigt für alle $g \in \hat{P}_{n-1}(K)$. Sei $f \in \hat{P}_n(K)$. Annahme: Es gibt paarweise verschiedene $c_1, \ldots, c_{n+1} \in K$ mit $f(c_i) = 0$ für $1 \leqslant i \leqslant n+1$. Nach Lemma 9.1 gibt es ein $g \in \hat{P}_{n-1}(K)$ mit $f(x) = (x - c_{n+1})g(x)$ für alle $x \in K$. Nach Induktion hat g höchstens $n-1$ Nullstellen. Für $1 \leqslant i \leqslant n$ gilt dann aber $0 = f(c_i) = (c_i - c_{n+1})g(c_i)$. Wegen $c_i \neq c_{n+1}$ folgt also $g(c_i) = 0$ für $1 \leqslant i \leqslant n$, d.h., g hat n Nullstellen, Widerspruch. $\square$

Folgerung 9.3. *Sei* $n \geqslant 1$ *und* $|K| > n$. *Dann lässt sich jedes* $f \in P_n(K)$ *auf eindeutige Weise wie in* $(*)$ *schreiben, d.h., es gibt eindeutige Koeffizienten* $a_0, a_1, \ldots, a_n \in K$ *mit* $f(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ *für alle* $x \in K$.

Beweis. Sei $f \in P_n(K)$. Gegeben seien $a_i, b_j \in K$ mit

$$f(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 = b_nx^n + b_{n-1}x^{n-1} + \ldots + b_1x + b_0 \quad \text{für alle } x \in K.$$

Setze $c_i := a_i - b_i$ für alle i und definiere eine Polynomfunktion $g\colon K \to K$ durch $g(x) := c_n x^n + c_{n-1}x^{n-1} + \ldots + c_1 x + c_0$ für alle $x \in K$. Dann gilt $g(x) = 0$ für alle $x \in K$.

Annahme, es gibt ein i mit $a_i \neq b_i$, also $c_i \neq 0$. Sei dann $m := \max\{i \mid c_i \neq 0\}$. Wegen $m \leqslant n$, $c_m \neq 0$ und $c_i = 0$ für alle $i > m$ folgt $g \in \hat{P}_m(K)$. Nach Folgerung 9.2 hat g höchstens m Nullstellen. Aber alle Elemente von K sind Nullstellen von g; also muss $|K| \leqslant m \leqslant n$ gelten, Widerspruch zur Voraussetzung. □

Die Aussage in Folgerung 9.3 wird tatsächlich falsch, wenn K zu klein ist. Sei z.B. $K = \mathbb{F}_2$ und $f(x) = x^2 + x$ für alle $x \in K$. Dann ist $f \in P_2(\mathbb{F}_2)$ mit $f(\overline{0}) = \overline{0}$ und $f(\overline{1}) = \overline{1} + \overline{1} = \overline{0}$, d.h., es gilt $f(x) = \overline{0}$ für alle $x \in K$. Damit hat f zwei Darstellungen wie in $(*)$; einmal mit Koeffizienten $(a_0, a_1, a_2) = (\overline{0}, \overline{1}, \overline{1})$ und einmal mit Koeffizienten $(b_0, b_1, b_2) = (\overline{0}, \overline{0}, \overline{0})$.

Folgerung 9.4 (Polynominterpolation)**.** *Sei $n \in \mathbb{N}$. Gegeben seien paarweise verschiedene Elemente $x_1, \ldots, x_{n+1} \in K$ und beliebige Elemente $y_1, \ldots, y_{n+1} \in K$. Dann gibt es genau eine Polynomfunktion $f \in P_n(K)$ mit $f(x_i) = y_i$ für $i = 1, \ldots, n+1$.*

Beweis. Zur Existenz: Für $i = 1, 2, \ldots, n+1$ definieren wir $L_i \in P_n(K)$ durch

$$L_i(x) := \prod_{j \in \{1,\ldots,n+1\}\setminus\{i\}} \frac{x - x_j}{x_i - x_j} \qquad \text{für alle } x \in K.$$

(Beachte, dass man durch Ausmultiplizieren wirklich eine Polynomfunktion in $P_n(K)$ erhält.) Diese Funktionen heißen ***Lagrange–Polynomfunktionen***; sie haben folgende Werte, wie man sofort sieht: $L_i(x_j) = \begin{cases} 1 & \text{falls } i = j, \\ 0 & \text{falls } i \neq j. \end{cases}$

Definieren wir also $f \in P_n(K)$ durch $f(x) := \sum_{i=1}^{n+1} y_i L_i(x)$ für alle $x \in K$, so gilt $f(x_i) = y_i$ für $i = 1, \ldots, n+1$, wie gewünscht.

Zur Eindeutigkeit: Sind $f, g \in P_n(K)$ mit $f(x_i) = y_i = g(x_i)$ für $i = 1, \ldots, n+1$, so ist die Differenz $f - g$ eine Polynomfunktion in $P_n(K)$, die $n+1$ Nullstellen hat, muss also gleich 0 sein nach Folgerung 9.2. □

Beispiel: Sei $n = 3$ und folgende Werte gegeben:

i	1	2	3	4
x_i	-2	-1	1	2
y_i	1	3	-3	2

. Dann ist

$L_1(x) = \frac{(x+1)(x-1)(x-2)}{(-1)\cdot(-3)\cdot(-4)}$, $L_2(x) = \frac{(x+2)(x-1)(x-2)}{1\cdot(-2)\cdot(-3)}$, $L_3(x) = \frac{(x+2)(x+1)(x-2)}{3\cdot2\cdot(-1)}$, $L_4(x) = \frac{(x+2)(x+1)(x-1)}{4\cdot3\cdot1}$

und damit $f(x) = 1 \cdot L_1(x) + 3 \cdot L_2(x) - 3 \cdot L_3(x) + 2 \cdot L_4(x) = \ldots = \frac{13}{12}x^3 + \frac{1}{2}x^2 - \frac{49}{12}x - \frac{1}{2}$.

Aus verschiedenen Gründen (etwa um die obigen Schwierigkeiten mit zu kleinen Körpern zu vermeiden) ist es sinnvoll, "abstrakte" Polynome anstelle von Polynomfunktionen einzuführen. Was hat man darunter zu verstehen? — Informelle Antwort: Ein "formaler" Ausdruck der Form $x^3 + x$, wobei man für x irgendwelche Werte einsetzen kann. Man kann solche Ausdrücke addieren und multiplizieren (mit den üblichen Rechenregeln), zum Beispiel:

$(2x^2 - 1) + (x^3 + x) = x^3 + 2x^2 + x - 1$ und

$(2x^2 - 1) \cdot (x^3 + x) = 2x^5 + 2x^3 - x^3 - x = 2x^5 + x^3 - x.$

Aber was genau ist ein "formaler" Ausdruck, und woraus soll man Werte einsetzen können? Vielleicht hilft es, sich die allgemeine Form eines solchen Ausdrucks vorzustellen; diese sollte so aussehen: $a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$, wobei $n \in \mathbb{N}_0$ und $a_0, a_1, \ldots, a_n \in K$. Letztlich relevant scheinen also eigentlich nur die Koeffizienten $a_0, a_1, a_2, \ldots, a_n$ zu sein. Diese Beobachtung wird tatsächlich zur Grundlage einer ordentlichen Definition.

Sei K beliebiger Körper; wir betrachten die Menge $\mathcal{F} = \mathrm{Abb}(\mathbb{N}_0, K)$. Jedes $f \in \mathcal{F}$ schreiben wir als Folge $f = (a_n)_{n\geqslant 0}$ (oder einfach (a_n)), wobei $a_n = f(n)$ für alle $n \geqslant 0$. Addition und Multiplikation mit einem Skalar $s \in K$ seien gegeben durch:

$$(a_n) \ + \ (b_n) := (a_n + b_n) \qquad \text{und} \qquad s.(a_n) := (sa_n).$$

Man rechnet leicht nach, dass damit $(\mathcal{F}, +)$ eine abelsche Gruppe ist. Das neutrale Element bezüglich der Addition ist $\underline{0} = (0, 0, 0, \ldots)$. Für $f, g \in \mathcal{F}$ definieren wir auch ein Produkt $f * g \in \mathcal{F}$ wie folgt: Seien $f = (a_n)$ und $g = (b_n)$; für $n \geqslant 0$ sei

$$c_n := \sum_{i=0}^{n} a_i b_{n-i} = a_0b_n + a_1b_{n-1} + a_2b_{n-2} + \ldots + a_{n-1}b_1 + a_nb_0.$$

Dann setze $f * g := (c_n)$. Diese Verknüpfung heißt ***Konvolution***, oder auch ***Faltung***.

Beispiel: $(-1, 0, 2, 0, 0, \ldots) * (0, 1, 0, 1, 0, 0, \ldots) = (0, -1, 0, 1, 0, 2, 0, 0, \ldots)$, denn $c_0 = a_0b_0 = 0$, $c_1 = a_0b_1 + a_1b_0 = -1$, $c_2 = a_0b_2 + a_1b_1 + a_2b_0 = 0$, usw.

Ab hier Woche 6

Wir sagen, dass $f = (a_n) \in \mathcal{F}$ endlich ist, wenn es ein $n_0 \geqslant 0$ gibt mit $a_n = 0$ für alle $n > n_0$. In diesem Fall schreiben wir f einfach als $f = (a_0, a_1, \ldots, a_{n_0}, 0, \ldots)$. Ist $f \neq \underline{0}$, so heißt $\mathrm{Grad}(f) := n_0 = \max\{n \in \mathbb{N}_0 \mid a_n \neq 0\}$ der ***Grad*** von f und a_{n_0} der ***Leitkoeffizient*** von f. Ist hier $a_{n_0} = 1$, so heißt f ***normiert***.

Lemma 9.5. *Sei* $\mathcal{F}_0 := \{f \in \mathcal{F} \mid f \text{ ist endlich}\} \subseteq \mathcal{F}$. *Seien* $f, g \in \mathcal{F}_0$. *Dann gilt:*

(a) *Es ist auch* $s.f \in \mathcal{F}_0$ *für* $s \in K$, $f + g \in \mathcal{F}_0$ *und* $f * g \in \mathcal{F}_0$.

(b) *Sind* $f, g \neq \underline{0}$ *und* $f + g \neq \underline{0}$, *so gilt* $\mathrm{Grad}(f + g) \leqslant \max\{\mathrm{Grad}(f), \mathrm{Grad}(g)\}$.

(c) *Sind* $f, g \neq \underline{0}$, *so gilt* $f * g \neq 0$ *und* $\mathrm{Grad}(f * g) = \mathrm{Grad}(f) + \mathrm{Grad}(g)$.

Beweis. Seien $f = (a_n)$ und $g = (b_n)$ in $\mathcal{F}_0$. Ist $f = \underline{0} = (0, 0, \ldots)$, so ist $f + g = g \in \mathcal{F}_0$ und $s.f = \underline{0} \in \mathcal{F}_0$; ebenso $f * g = \underline{0} \in \mathcal{F}_0$. Analog: Ist $g = \underline{0}$, so sind $f + g = f \in \mathcal{F}_0$ und $f * g = \underline{0} \in \mathcal{F}_0$. Seien nun also $f \neq \underline{0}$ und $g \neq \underline{0}$.

Seien $n_0 = \mathrm{Grad}(f)$ und $m_0 = \mathrm{Grad}(g)$; also $f = (a_0, a_1, \ldots, a_{n_0}, 0, \ldots)$ mit $a_{n_0} \neq 0$, und $g = (b_0, b_1, \ldots, b_{m_0}, 0, \ldots)$ mit $b_{m_0} \neq 0$. Dann ist offensichtlich $s.f = (sa_0, sa_1, \ldots, sa_{n_0}, 0, \ldots) \in \mathcal{F}_0$ für $s \in K$. Ist $d_0 = \max\{n_0, m_0\}$, so gilt $f+g = (a_0+b_0, a_1+b_1, \ldots, a_{d_0}+b_{d_0}, 0, \ldots) \in \mathcal{F}_0$. Ist $f + g \neq \underline{0}$, so ist damit $\mathrm{Grad}(f + g) \leqslant d_0$, also gilt (b).

Nun betrachte $f * g = (c_n)$. Ist $c_n = \sum_{i=0}^{n} a_i b_{n-i} \neq 0$, so gibt es ein i mit $a_i \neq 0$ und $b_{n-i} \neq 0$, d.h., $i \leqslant n_0$ und $n - i \leqslant m_0$, also $n \leqslant m_0 + i \leqslant m_0 + n_0$. Also folgt $f * g = (c_0, c_1, \ldots, c_{n_0+m_0}, 0, \ldots) \in \mathcal{F}_0$, d.h., es gilt (a). Betrachten wir nun den Koeffizienten $c_{n_0+m_0} = \sum_{i=0}^{n_0+m_0} a_i b_{n_0+m_0-i}$. Ist in dieser Summe $i > n_0$, so folgt $a_i = 0$. Ist $i < n_0$, so ist $n_0 + m_0 - i > m_0$, also $b_{n_0+m_0-i} = 0$. Also bleibt nur $i = n_0$ übrig und es folgt $c_{n_0+m_0} = a_{n_0} b_{m_0} \neq 0$. Also $f * g \neq \underline{0}$ und $\mathrm{Grad}(f * g) = n_0 + m_0$. Damit gilt auch (c). □

Bemerkung 9.6. (a) $e := (1, 0, 0, \ldots) \in \mathcal{F}_0$ ist das neutrale Element bezüglich $*$.
(b) Ist $X := (0, 1, 0, 0, \ldots) \in \mathcal{F}_0$, so gilt $X * (a_n) = (0, a_0, a_1, a_2, \ldots)$.

Beweis. (a) Es gilt $e * (a_n) = (c_n)$ mit $c_n = \sum_{i=0}^{n} e_i a_{n-i} = e_0 a_n + e_1 a_{n-1} + \ldots + e_n a_0 = a_n$.
(b) Es ist $X * (a_n) = (c_n)$ mit $c_n = \sum_{i=0}^{n} X_i a_{n-i} = X_0 a_n + X_1 a_{n-1} + X_2 a_{n-2} + \ldots + X_n a_0$. Dies ist gleich 0 falls $n = 0$, und gleich a_{n-1} falls $n \geqslant 1$. □

Definition 9.7 ("Abstrakte" Polynome über K)**.** Bezeichnen wir $X := (0, 1, 0, 0, \ldots) \in \mathcal{F}_0$ wie oben, so schreiben wir auch $K[X] := \mathcal{F}_0$. Dann definieren wir $X^0 := e = (1, 0, 0, \ldots)$ und $X^n := X * X^{n-1}$ für alle $n \in \mathbb{N}$, also

$$X^1 := X, \quad X^2 := X * X = (0, 0, 1, 0, 0, \ldots), \quad X^3 := X * X^2 = (0, 0, 0, 1, 0, 0, \ldots), \quad \ldots$$

Ist $f = (a_n) \in \mathcal{F}_0$ und $n_0 \geqslant 0$ mit $f = (a_0, a_1, \ldots, a_{n_0}, 0, \ldots)$, so erhalten wir eine eindeutige Darstellung $f = \sum_{i=0}^{n_0} a_i X^i = a_{n_0} X^{n_0} + a_{n_0-1} X^{n_0-1} + \ldots + a_1 X + a_0$.
(Hier schreiben wir einfach $a_i X^i$ anstelle von $a_i.X^i$; außerdem werden die Terme $a_i X^i$ meist nach absteigendem Exponenten von X geschrieben, aber die Reihenfolge ist letztlich egal.)
Die Elemente von $K[X] = \mathcal{F}_0$ heißen ***Polynome*** in der ***Unbestimmten*** X. (Wir könnten auch irgendein anderes Symbol anstelle von X nehmen; dies ist immer nur ein Name für die Folge $(0, 1, 0, 0, \ldots) \in \mathcal{F}_0$.) Schließlich: Wir fassen K als Teilmenge von $K[X] = \mathcal{F}_0$ auf, indem wir ein Element $a \in K$ mit $ae = aX^0 = (a, 0, 0, \ldots) \in \mathcal{F}_0$ identifizieren.

Lemma 9.8. *Mit den oben definierten Verknüpfungen "+" und "$*$" ist $K[X] = \mathcal{F}_0$ ein kommutativer Ring mit 1. Sind $f, g \in \mathcal{F}_0$ und $s \in K$, so gilt $(s.f) * g = s.(f * g) = f * (s.g)$.*

Beweis. Etwas langwieriges (aber letztlich einfaches) Nachrechnen aller Ringaxiome. □

Gegeben seien Polynome $f = a_{n_0}X^{n_0} + a_{n_0-1}X^{n_0-1} + \ldots + a_1X + a_0$ und $g = b_{m_0}X^{m_0} + b_{m_0-1}X^{m_0-1} + \ldots + b_1X + b_0$. Die Tatsache, dass $K[X]$ ein Ring ist und die Formeln in Lemma 9.8 gelten, bedeutet dann, dass wir $f * g$ einfach wie folgt ausmultiplizieren können:

$$f * g = \sum_{i=0}^{n_0}\sum_{j=0}^{m_0}(a_iX^i) * (b_jX^j) = \sum_{i=0}^{n_0}\sum_{j=0}^{m_0}(a_ib_j)(X^i * X^j) = \sum_{i=0}^{n_0}\sum_{j=0}^{m_0} a_ib_jX^{i+j}.$$

Am Ende fasst man die Terme $a_ib_jX^{i+j}$ mit gleichem Exponenten von X zusammen. (Man braucht sich also gar nicht an die genaue Definition von $*$ zu erinnern.)

Bemerkung 9.9. Sei $f = a_{n_0}X^{n_0} + a_{n_0-1}X^{n_0-1} + \ldots + a_1X + a_0 \in K[X]$. Dann erhalten wir eine Polynomfunktion $\dot{f} \in P(K)$ mit $\dot{f}(x) := a_{n_0}x^{n_0} + a_{n_0-1}x^{n_0-1} + \ldots + a_1x + a_0$ für $x \in K$.

Zum Beispiel: Ist $K = \mathbb{F}_2$ und $f = X^2 + X \in K[X]$, so ist $\dot{f}(x) = x^2 + x = 0$ für $x \in K$. Hier ist $f \neq \underline{0}$, aber $\dot{f}$ ist die Null-Funktion. (Unterschied Polynome $\leftrightarrow$ Polynomfunktionen!)

Ist $s \in K$, so schreiben wir auch einfach $f(s)$ anstelle von $\dot{f}(s)$. In diesem Sinne haben wir also s in f "eingesetzt". Für dieses Einsetzen gelten die Regeln $(f + g)(s) = f(s) + g(s)$ und $(f * g)(s) = f(s)g(s)$ für alle $f, g \in K[X]$ (wie man leicht nachrechnet).

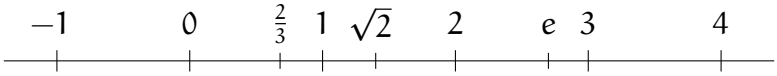
Bemerkung 9.10. Analog zu Satz 9.1 gibt es auch ein Horner-Schema für Polynome: Ist $\underline{0} \neq f \in K[X]$ mit $n = \mathrm{Grad}(f) \geqslant 1$, so gilt $f = (X - c) * g + f(c)$, wobei $\underline{0} \neq g \in K[X]$ mit $\mathrm{Grad}(g) = n - 1$. Ist $f(c) = 0$, so heißt c eine ***Nullstelle*** von f; in diesem Fall ist also $f = (X - c) * g$. Wie in Folgerung 9.2 sieht man, dass f höchstens n Nullstellen hat.

Noch einmal: Polynome in $K[X] = \mathcal{F}_0$ und Polynomfunktionen in $P(K)$ sind zwei völlig verschiedene Objekte! Ein Polynom in $K[X]$ ist letztlich nur die Folge $f = (a_0, a_1, \ldots, a_{n_0}, 0, \ldots)$ seiner Koeffizienten, und keine Funktion $K \to K$! Genauso werden Polynome in Computer-Algebra-Systemen (wie z.B. GAP oder Sage) realisiert, nämlich intern durch endlich lange Listen der Koeffizienten; Rechnungen mit Polynomen sind dann letztlich Manipulationen dieser Listen. Das Ergebnis solcher Rechnungen wird nicht als Liste ausgegeben, sondern als "formaler" Ausdruck wie oben mit einer Unbestimmten X gedruckt. (Man kann natürlich auch andere Buchstaben anstelle von "X" wählen.) Beispiel:

```
gap> t:=Indeterminate(Rationals,"t");;      # "t"= Name der Unbestimmten
gap> f:=(3*t^4-1)*(t^8-t^5+17);
3*t^12-3*t^9-t^8+t^5+51*t^4-17
gap> CoefficientsOfUnivariatePolynomial(f);
[ -17, 0, 0, 0, 51, 1, 0, 0, -1, -3, 0, 0, 3 ]    # beachte Reihenfolge!
gap> Value(f,11)                                   # s=11 in f eingesetzt
9407997835934
```

10. *Die reellen und die komplexen Zahlen*

Die reellen Zahlen $\mathbb{R}$ bilden einen Körper mit $\mathbb{Q} \subseteq \mathbb{R}$; die üblichen Rechen-Operationen (also Addition, Multiplikation, Anordnung $\leqslant$) werden dabei von $\mathbb{Q}$ auf $\mathbb{R}$ fortgesetzt. Wir geben hier keine formale Definition oder Konstruktion (dazu siehe zum Beispiel Kapitel 2 im Buch von Ebbinghaus et al.), sondern stellen uns $\mathbb{R}$ als Zahlengerade vor:



Elemente von $\mathbb{R}\backslash\mathbb{Q}$ heißen ***irrationale Zahlen***; wir haben bereits gesehen, dass $\sqrt{2}$ irrational ist (Satz 2.10). Ein anderes Beispiel ist die oben in der Zahlengeraden genannte ***Eulersche Zahl*** $e \approx 2{,}71828\ldots$; wie man solche Zahlen mathematisch präzise konstruiert und damit umgeht, ist Thema der Analysis-Vorlesung und wird hier nicht weiter behandelt.

Die komplexen Zahlen $\mathbb{C}$ bilden einen Körper mit $\mathbb{R} \subseteq \mathbb{C}$. Konkret kann man als Menge $\mathbb{C} := \{(a, b) \mid a, b \in \mathbb{R}\}$ nehmen und darauf folgende Verknüpfungen definieren:

$$(a, b) + (a', b') := (a + a', b + b') \qquad \text{und} \qquad (a, b) \cdot (a', b') := (aa' - bb', ab' + a'b)$$

für alle $a, a', b, b' \in \mathbb{R}$. Man muss dann zeigen, dass die Körperaxiome erfüllt sind. (Dazu sind viele kleinere Rechnungen zu machen, die aber alle nicht besonders schwierig sind; siehe z.B. §9.3 im Buch von Glosauer für die Details.) Das Paar $(0, 0)$ ist das neutrale Element bezüglich der Addition; das Paar $(1, 0)$ ist das neutrale Element bezüglich der Multiplikation. Die Inversen von $z := (a, b) \in \mathbb{C}$ bezüglich Addition und Multiplikation sind gegeben durch

$$-z = (-a, -b) \in \mathbb{C} \qquad \text{und} \qquad z^{-1} = \Big(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2}\Big) \in \mathbb{C},$$

wobei wir für z^{-1} natürlich $z \neq (0, 0)$ voraussetzen müssen, d.h., $a \neq 0$ oder $b \neq 0$; beachte, dass in diesem Fall $a^2 + b^2$ eine positive reelle Zahl ist. Wir können $\mathbb{R}$ als Teilmenge von $\mathbb{C}$ auffassen, indem wir $a \in \mathbb{R}$ mit $(a, 0) \in \mathbb{C}$ identifizieren. Setzen wir außerdem $i := (0, 1) \in \mathbb{C}$, so folgt $i^2 = -(1, 0) = -1$ und $(a, b) = (a, 0) + (0, b) = a + b \cdot (0, 1) = a + bi$; hier heißt a der ***Realteil*** und b der ***Imaginärteil***. Also erhalten wir die übliche Schreibweise $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$; das Rechnen mit solchen Ausdrücken erfolgt dann ebenfalls nach den üblichen Reglen, wobei man sich nur daran erinnern muss, dass $i^2 = -1$ gilt. Zum Beispiel:

$$\frac{2 + 3i}{-5 + i} = \frac{2 + 3i}{-5 + i} \cdot \frac{-5 - i}{-5 - i} = \frac{(2 + 3i)(-5 - i)}{25 + 1} = \frac{-10 - 2i - 15i - 3i^2}{26} = -\frac{7}{2} - \frac{17}{26}i \in \mathbb{C}.$$

Bemerkung 10.1. Ist $z = a + bi \in \mathbb{C}$ so heißt $\overline{z} := a - bi \in \mathbb{C}$ die ***konjugiert-komplexe Zahl***. Dann ist $z\overline{z} = a^2 + b^2$ eine nicht-negative reelle Zahl und wir nennen

$$|z| := \sqrt{z\overline{z}} = \sqrt{a^2 + b^2} \in \mathbb{R}$$

den Absolutbetrag von z. Damit gilt $z^{-1} = (|z|^2)^{-1}\overline{z}$ für $0 \neq z \in \mathbb{C}$. Weiterhin gilt:

$$\overline{\overline{z}} = z, \qquad \overline{z_1 + z_2} = \overline{z}_1 + \overline{z}_2, \qquad \overline{z_1 \cdot z_2} = \overline{z}_1 \cdot \overline{z}_2, \qquad z \in \mathbb{R} \Leftrightarrow \overline{z} = z,$$

$$\tfrac{1}{2}(z + \overline{z}) = \text{Realteil von } z, \qquad \tfrac{1}{2i}(z - \overline{z}) = \text{Imaginärteil von } z,$$

für alle $z, z_1, z_2 \in \mathbb{C}$. (Beweis durch leichtes Nachrechnen.)

Bemerkung 10.2. Wie oben diskutiert, setzen sich Addition und Multiplikation von $\mathbb{R}$ auf $\mathbb{C}$ fort. Aber die Anordnung $\leqslant$ auf $\mathbb{R}$ lässt sich nicht sinnvollerweise auf $\mathbb{C}$ fortsetzen. Natürlich kann man $\mathbb{C}$ irgendwie anordnen, aber dies sollte auch mit den Körperoperationen zusammenpassen (genauso wie in $\mathbb{R}$), also zum Beispiel $x + y > 0$ und $x \cdot y > 0$, wenn $x > 0$ und $y > 0$. Daraus folgt sofort $x^2 = x \cdot x = (-x) \cdot (-x) > 0$ für jedes $x \neq 0$; inbesondere $1 = 1^2 > 0$. Gäbe es eine solche Anordnung auf $\mathbb{C}$, so wäre $-1 = i^2 > 0$, Widerspruch.

Bemerkung 10.3. In $\mathbb{R}$ hat die Gleichung $x^2 = -1$ keine Lösung, aber in $\mathbb{C}$ sehr wohl, nämlich $x = \pm i$. Es gilt sogar, dass jedes $z \in \mathbb{C}$ eine Quadratwurzel in $\mathbb{C}$ besitzt, nämlich

$$z = \Big(\sqrt{\tfrac{1}{2}\big(\sqrt{a^2 + b^2} + a\big)} \pm i\sqrt{\tfrac{1}{2}\big(\sqrt{a^2 + b^2} - a\big)}\Big)^2 \quad \text{wobei} \quad z = a + bi \quad \text{mit } a, b \in \mathbb{R}$$

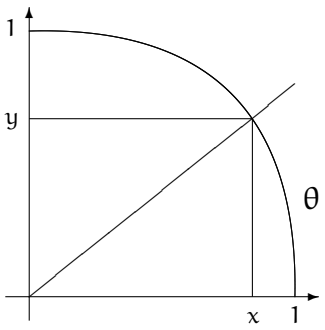
und das Vorzeichen gleich "+" ist, falls $b \geqslant 0$, und gleich "−", falls $b < 0$. (Einfaches Nachrechnen.) Damit hat auch jede quadratische Gleichung der Form $x^2 + px + q = 0$ mit $p, q \in \mathbb{C}$ Lösungen in $\mathbb{C}$, nämlich $x_{1,2} = \frac{1}{2}\big(-p \pm \sqrt{p^2 - 4q}\big) \in \mathbb{C}$.

Man hätte erwarten können, dass für Lösungen von Gleichungen vom Grad $3, 4, \ldots$ noch größere Körper als $\mathbb{C}$ konstruiert werden müssten. Aber es gilt:

Satz 10.4 (***Fundamentalsatz der Algebra***)**.** *Sei* $n \in \mathbb{N}$ *und* $0 \neq f \in \mathbb{C}[X]$ *ein Polynom mit* $\mathrm{Grad}(f) = n$*. Dann zerfällt* f *in Linearfaktoren über* $\mathbb{C}$*, d.h., es gibt* $a, z_1, \ldots, z_n \in \mathbb{C}$ *mit* $a \neq 0$ *und* $f = a(X - z_1)(X - z_2)\cdots(X - z_n)$*. Insbesondere hat jedes nicht-konstante Polynom* $f \in \mathbb{C}[X]$ *eine Nullstelle in* $\mathbb{C}$*.*

Für diverse Beweise und mehr zur (interessanten) Geschichte dieses Satzes und seine Bedeutung in der Mathematik insgesamt siehe Kapitel 4 im Buch von Ebbinhaus et al.
Im Mathematik-Studium wird dieser Satz üblicherweise in einer Analysis-Vorlesung oder der Vorlesung Algebra 1 (im 3. Semester) bewiesen).

Zum Schluss geben wir noch eine geometrisch etwas anschaulichere Beschreibung der Multiplikation in $\mathbb{C}$. Dazu setzen wir die übliche (reelle) ***Sinus-Funktion*** und die ***Cosinus-Funktion*** als bekannt voraus (mehr dazu in der Analysis-Vorlesung). Für einen Winkel θ sind $\sin(\theta)$ und $\cos(\theta)$ anschaulich wie in folgender Zeichnung definiert, wobei wir den Kreis mit Radius 1 und Mittelpunkt im Ursprung von $\mathbb{R}^2$ betrachten:



$$x = \cos(\theta) \quad \text{oder} \quad \theta = \arccos(x)$$
$$y = \sin(\theta) \quad \text{oder} \quad \theta = \arcsin(y)$$
$$\sin(\theta)^2 + \cos(\theta)^2 = 1 \qquad \text{(Pythagoras)}$$

Der Winkel θ wird hierbei im ***Bogenmaß*** angegeben, d.h., durch die Länge des Kreisbogens zwischen den Punkten $(1,0) \in \mathbb{R}^2$ und $(x,y) \in \mathbb{R}^2$. Da der gesamte Kreis den Umfang 2π hat, ist $\theta \in [0, 2\pi]$; es gilt $\sin(\theta) \in [-1,1]$ und $\cos(\theta) \in [-1,1]$. Hier sind einige oft gebrauchte Werte von sin und cos:

θ	0	$\frac{\pi}{6}$	$\frac{\pi}{4}$	$\frac{\pi}{3}$	$\frac{\pi}{2}$	π
$\sin(\theta)$	0	$\frac{1}{2}$	$\frac{\sqrt{2}}{2}$	$\frac{\sqrt{3}}{2}$	1	0
$\cos(\theta)$	1	$\frac{\sqrt{3}}{2}$	$\frac{\sqrt{2}}{2}$	$\frac{1}{2}$	0	-1

Die Funktionen sin and cos können auf ganz $\mathbb{R}$ fortgesetzt werden, wobei sich die Werte mit Periode 2π wiederholen, also

$$\sin(x + 2\pi) = \sin(x) \qquad \text{und} \qquad \cos(x + 2\pi) = \cos(x) \qquad \text{für alle } x \in \mathbb{R}.$$

Hierbei gilt $\sin(-x) = -\sin(x)$ und $\cos(-x) = \cos(x)$ für alle $x \in \mathbb{R}$. Außerdem gelten die folgenden ***Additionstheoreme*** für alle $x, y \in \mathbb{R}$:

$$\begin{aligned} \sin(x+y) &= \sin(x)\cos(y) + \cos(x)\sin(y), \\ \cos(x+y) &= \cos(x)\cos(y) - \sin(x)\sin(y). \end{aligned}$$

Satz 10.5 (Polardarstellung komplexer Zahlen)**.** *Für jedes $z \in \mathbb{C}$ existieren eindeutige reelle Zahlen $r, \theta \in \mathbb{R}$ mit $z = r\big(\cos(\theta) + \sin(\theta)i\big)$ wobei $r = |z| \geqslant 0$ und $\theta \in [0, 2\pi)$ (und wir die Konvention benutzen, $\theta = 0$ für $z = 0$ zu nehmen).*

Anstelle eines formalen Beweises illustrieren wir dies mit einem Beispiel. Sei also etwa $z = \sqrt{2} - \sqrt{2}\mathrm{i} \in \mathbb{C}$. Dann ist $r = |z| = \sqrt{(\sqrt{2})^2 + (-\sqrt{2})^2} = 2$. Damit ist $z = 2(\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}\mathrm{i})$. Jetzt müssen wir noch $\theta \in [0, 2\pi)$ finden mit $\cos(\theta) = \frac{1}{\sqrt{2}}$ und $\sin(\theta) = -\frac{1}{\sqrt{2}}$. Mit obiger Tabelle und den Regeln $\sin(-x) = -\sin(x)$, $\cos(-x) = \cos(x)$ sieht man, dass man die richtigen Werte für $x = -\frac{\pi}{4}$ erhält. Um einen Winkel im Intervall $[0, 2\pi)$ zu erhalten, addieren wir 2π, was zu $\theta = 2\pi - \frac{\pi}{4} = \frac{7}{4}\pi$ führt. Damit erhalten wir die Polardarstellung:

$$z = \sqrt{2} - \sqrt{2}\mathrm{i} = 2\big(\cos(\tfrac{7}{4}\pi) + \sin(\tfrac{7}{4}\pi)\mathrm{i}\big).$$

Nach diesen Vorbereitungen kommen wir nun zur versprochenen anschaulichen Beschreibung der Multiplikation in $\mathbb{C}$. Seien $z, z' \in \mathbb{C}$ mit Polardarstellungen

$$z = r\big(\cos(\theta) + \sin(\theta)\mathrm{i}\big) \qquad \text{und} \qquad z' = r'\big(\cos(\theta') + \sin(\theta')\mathrm{i}\big).$$

Multiplikation ergibt

$$\begin{aligned} z \cdot z' &= rr'\big((\cos(\theta)\cos(\theta') - \sin(\theta)\sin(\theta')) + (\sin(\theta)\cos(\theta') + \cos(\theta)\sin(\theta'))i\big) \\ &= rr'\big(\cos(\theta+\theta') + \sin(\theta+\theta')i\big) \end{aligned}$$

wobei wir die obigen Additionstheoreme verwendet haben. D.h. wir erhalten die Polardarstellung von $z \cdot z'$, indem wir r, r' multiplizieren und die Winkel θ, θ' einfach addieren. Mit einer vollständigen Induktion nach n folgt dann auch sofort

$$z^n = r^n\big(\cos(n\theta) + \sin(n\theta)i\big) \qquad \text{für alle } n \in \mathbb{N}.$$

Beispiel 10.6. Sei $n \geqslant 1$ und $f_n := X^n - 1 \in \mathbb{C}[X]$. In diesem Fall kann man die Nullstellen von f_n explizit beschreiben. Dazu teilen wir den Kreis (in der Ebene $\mathbb{C} = \mathbb{R}^2$) mit Radius 1 und Mittelpunkt im Ursprung in genau n gleiche Stücke ein; die entsprechenden Punkte auf diesem Kreis sind gegegen durch

$$\zeta_k := \cos(\theta_k) + \sin(\theta_k)i \in \mathbb{C} \qquad \text{für } k = 0, 1, 2, \ldots, n-1,$$

wobei $\theta_0 := 0,\ \theta_1 := \frac{2\pi}{n},\ \theta_2 := 2\theta_1 = 2\frac{2\pi}{n},\ \ldots,\ \theta_{n-1} := (n-1)\theta_1 = (n-1)\frac{2\pi}{n}$. Mit Hilfe der obigen Formeln erhalten wir dann für $k = 0, 1, 2, \ldots, n$:

$$\begin{aligned} \zeta_k^n &= \cos(n\theta_k) + \sin(n\theta_k)i = \cos\big(\tfrac{2\pi k n}{n}\big) + \sin\big(\tfrac{2\pi k n}{n}\big)i \\ &= \cos(2\pi k) + \sin(2\pi k)i = \cos(0) + \sin(0)i = 1. \end{aligned}$$

D.h., die n komplexen Zahlen $\zeta_0, \zeta_1, \ldots, \zeta_{n-1} \in \mathbb{C}$ sind alle Nullstellen von f_n. Damit folgt

$$f_n = X^n - 1 = (X - \zeta_0)(X - \zeta_1)\cdots(X - \zeta_{n-1}).$$

Die Zahlen ζ_k heißen n-te ***Einheitswurzeln***.

Kapitel III: Matrizen

Matrizen spielen eine einzigartige Rolle nicht nur in der Mathematik selbst (Matrix-Theorie ist immer noch ein aktives Forschungsgebiet), sondern auch in zahlreichen Anwendungen in den Natur- und Ingenieurwissenschaften — immer dort, wo "lineare" Probleme auftreten. In diesem Kapitel führen wir die grundlegenden Definitionen und Operationen mit Matrizen ein, und betrachten auch erste Anwendungen.

11. *Definition, Operationen mit Matrizen*

Sei R ein kommutativer Ring mit 1 (zum Beispel $R = \mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z}/m\mathbb{Z}$). Seien $m, n \in \mathbb{N}$. Ein recht-eckiges Schema der Form

$$\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix}$$

mit m Zeilen und n Spalten heißt eine $m \times n$-***Matrix***. Für $1 \leqslant i \leqslant m$ und $1 \leqslant j \leqslant n$ ist a_{ij} der Eintrag an der Position (i, j), also in der i-ten Zeile und j-ten Spalte. Es sei $R^{m\times n}$ die Menge aller $m \times n$-Matrizen mit Einträgen in R. Ist $A \in R^{m\times n}$, so bezeichnen wir mit A_{ij} die einzelnen Einträge von A, oder schreiben explizit $A = [a_{ij}]_{1\leqslant i\leqslant m, 1\leqslant j\leqslant n}$.

Formal ist eine $m \times n$-Matrix also einfach eine Abbildung $f\colon \{1, \dots, m\} \times \{1, \dots, n\} \to R$, deren Wert an der Stelle (i, j) mit $f(i, j) = f_{ij}$ bezeichnet wird.

Beispiel 11.1. (a) $A = \begin{bmatrix} 2 & 1 & 0 \\ 1 & 3 & 5 \end{bmatrix}$ ist eine 2×3-Matrix mit Einträgen in $\mathbb{Z}$.

(b) Ist $n = m$ (gleich viele Zeilen wie Spalten), so erhalten wir quadratische Matrizen und benutzen als Bezeichnung oft $M_n(R)$ anstelle von $R^{n\times n}$.

(c) Ist $m = 1$ (d.h., nur 1 Zeile), so ist $A = [a_1, \dots, a_n]$; wir nennen dies einen ***Zeilenvektor***. Analog, ist $n = 1$ (d.h., nur 1 Spalte), so erhalten wir einen ***Spaltenvektor***

$$A = \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{bmatrix}.$$

Ist $m = n = 1$, so ist $A = [a]$; wir identifizieren dann einfach a mit $[a]$. Als Konvention bezeichnen wir noch mit $R^n = R^{n\times 1}$ die Menge der Spaltenvektoren der Länge n.

Definition 11.2. Für $A, B \in R^{m\times n}$ definieren wir die ***Matrixsumme*** $A + B$ als die $m \times n$-Matrix mit Eintrag $A_{ij} + B_{ij}$ an der Stelle (i, j). Ist $s \in R$, so definieren wir das ***skalare Matrixprodukt*** sA als die $m \times n$-Matrix mit Eintrag sa_{ij} an der Stelle (i, j).

Beispiele: $\begin{bmatrix}2&1&0\\1&3&5\end{bmatrix}+\begin{bmatrix}1&0&3\\4&-3&1\end{bmatrix}=\begin{bmatrix}3&1&3\\5&0&6\end{bmatrix}$ und $(-2)\begin{bmatrix}2&1&0\\1&3&5\end{bmatrix}=\begin{bmatrix}-4&-2&0\\-2&-6&-10\end{bmatrix}$.

Bemerkung 11.3. Es gelten die folgenden Rechenregeln.
(a) Seien $A, B, C \in R^{m\times n}$. Dann gilt $A+B = B+A$ und $(A+B)+C = A+(B+C)$. Die Menge $R^{m\times n}$ zusammen mit der oben definierten Matrixaddition ist eine ***abelsche Gruppe***. Das neutrale Element ist $0_{m\times n}$, die Matrix, die nur aus Nullen besteht; das zu $A = [a_{ij}] \in R^{m\times n}$ inverse Element (bezüglich der Addition) ist die Matrix $-A = [-a_{ij}]$.
(b) Es gilt $1 \cdot A = A$ und $(s+t)A = sA + tA$, $(st)A = s(tA)$, $s(A+B) = sA + sB$ für alle $s, t \in R$.

Beweis. Einfaches Nachrechnen mit den entsprechenden Regeln für R. □

Ab hier Woche 7

Definition 11.4. Seien $m, n, p \in \mathbb{N}$ und $A \in R^{m\times n}$, $B \in R^{n\times p}$. Dann ist das ***Matrixprodukt*** $A \cdot B \in R^{m\times p}$ definiert als die Matrix mit (i,j)-Eintrag

$$(A \cdot B)_{ij} := \sum_{k=1}^{n} a_{ik} b_{kj} \qquad \text{für } 1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant p.$$

Um das Produkt bilden zu können, muss also die erste Matrix genauso viele Spalten haben, wie die zweite Matrix Zeilen hat. Beispiel:

$$\begin{bmatrix}1&0&5\\0&1&7\end{bmatrix} \cdot \begin{bmatrix}2&3&1&1\\4&1&0&0\\0&1&1&0\end{bmatrix} \text{ ist eine } 2\times 4\text{-Matrix, nämlich gleich } \begin{bmatrix}2&8&6&1\\4&8&7&0\end{bmatrix};$$

zum Beispiel ergibt sich der Eintrag an der Stelle $(2,3)$ als $7 = 0\cdot 1 + 1\cdot 0 + 7\cdot 1$.

Spezialfall $m = 1$, $p = 1$ ("Zeile mal Spalte"): $\begin{bmatrix}3&1&2\end{bmatrix} \cdot \begin{bmatrix}1\\-1\\4\end{bmatrix} = [3\cdot 1 + 1\cdot(-1) + 2\cdot 4] = [10]$
und nach unserer Vereinbarung in Beispiel 11.1 schreiben wir dies einfach als 10.
Damit gilt allgemein für $A \in R^{m\times n}$ und $B \in R^{n\times p}$: Sind $Z_1, \ldots, Z_m \in R^{1\times n}$ die Zeilen von A und $S_1, \ldots, S_p \in R^{m\times 1}$ die Spalten von B, so folgt:

$$\text{Der } (i,j)\text{-Eintrag von } A \cdot B \text{ ist gleich } Z_i \cdot S_j \qquad \text{für } 1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant p.$$

Außerdem: $A \cdot S_j = j\text{-te Spalte von } A \cdot B$ und $Z_i \cdot B = i\text{-te Zeile von } A \cdot B$.

Zum Beispiel in GAP werden Matrizen einfach als Listen von Listen realisiert:

```
gap> a:=[[1,0,5],[0,1,7]];;
gap> b:=[[2,3,1,1],[4,1,0,0],[0,1,1,0]];;
gap> a*b;
[ [ 2, 8, 6, 1 ], [ 4, 8, 7, 0 ] ]
```

Bemerkung 11.5. (a) Seien $A \in R^{m\times n}$, $B \in R^{n\times p}$, $C \in R^{p\times q}$. Dann gilt $(A\cdot B)\cdot C = A\cdot(B\cdot C)$.
(b) Seien $A, B \in R^{m\times n}$, $C \in R^{n\times l}$, $D \in R^{q\times m}$. Dann gilt $(A+B)\cdot C = A\cdot C + B\cdot C$ und

$D \cdot (A + B) = D \cdot A + D \cdot B$.
(c) Seien $A \in R^{m\times n}$ und $B \in R^{n\times p}$. Dann gilt $s(A \cdot B) = (sA) \cdot B = A \cdot (sB)$ für alle $s \in K$.

Beweis. Wiederum einfaches Nachrechnen; wir gehen durch die Einzelheiten in (a), weil dies eine gute Übung im Umgang mit den obigen Formeln ist. Sei $X := A{\cdot}B \in R^{m\times p}$. Dann ist

$$\big((A{\cdot}B){\cdot}C\big)_{ij} = (X{\cdot}C)_{ij} = \sum_{k=1}^{p} X_{ik}C_{kj} \qquad \text{und} \qquad X_{ik} = \sum_{l=1}^{n} A_{il}B_{lk}$$

und damit:
$$\big((A{\cdot}B){\cdot}C\big)_{ij} = \sum_{k=1}^{p}\Big(\sum_{l=1}^{n} A_{il}B_{lk}\Big)C_{kj} = \sum_{k=1}^{p}\sum_{l=1}^{n}(A_{il}B_{lk})C_{kj}. \tag{1}$$

Analog erhält man

$$\big(A{\cdot}(B{\cdot}C)\big)_{ij} = \sum_{k=1}^{n} A_{ik}\Big(\sum_{l=1}^{p} B_{kl}C_{lj}\Big) = \sum_{k=1}^{n}\sum_{l=1}^{p} A_{ik}(B_{kl}C_{lj}) = \sum_{l=1}^{n}\sum_{k=1}^{p} A_{il}(B_{lk}C_{kj}), \tag{2}$$

wobei im letzten Schritt die Symbole k und l vertauscht werden. Weil die Multiplikation in R assoziativ ist, sind die Ausdrücke (1) und (2) gleich. Der Beweis von (b), (c) geht analog. □

Satz 11.6. *Sei $m = n$. Dann ist $(M_n(R), +, \cdot)$ ein Ring mit Einselement gegeben durch*

$$I_n := \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1 \end{bmatrix} \qquad \textit{“}\boldsymbol{Einheitsmatrix}\textit{”}.$$

Für $n = 1$ ist $M_n(R)$ kommutativ; für $n \geqslant 2$ ist $M_n(R)$ nicht kommutativ.

Beweis. Nach Bemerkung 11.3 ist $(M_n(R), +)$ eine abelsche Gruppe. Nach Bemerkung 11.5 ist die Multiplikation assoziativ und es gelten die Distributivregeln. Schließlich überzeugt man sich davon, dass $A \cdot I_n = I_n \cdot A = A$ für alle $A \in M_n(R)$ gilt, also I_n das neutrale Element bezüglich der Multiplikation ist.

Für $n = 1$ ist $M_1(R) = \{[a] \mid a \in R\}$ und $[a] \cdot [b] = [ab]$ für alle $a, b \in R$. Damit folgt sofort $[a] \cdot [b] = [b] \cdot [a]$, also ist $M_1(R)$ kommutativ.

Für $n = 2$ ist z.B. $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ und $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, also ist $M_2(R)$ nicht kommutativ. Für $n > 3$ erhält man analog:

$$\begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & 0 \end{bmatrix},$$

$$\begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & 0 \end{bmatrix},$$

also ist $M_n(R)$ nicht kommutativ. □

Beispiel 11.7. Seien $m, n \in \mathbb{N}$. Seien $1 \leqslant i \leqslant m$ und $1 \leqslant j \leqslant n$.

Dann heißt die Matrix $E_{ij}^{(m,n)} = \begin{bmatrix} 0 & \dots & 0 \\ \vdots & 1 & \vdots \\ 0 & \dots & 0 \end{bmatrix} \in R^{m\times n}$ die (i,j)-***Standardmatrix***;

hier ist der Eintrag 1 an der Position (i,j), alle anderen Einträge sind 0.

Für $A = [a_{ij}] \in R^{m\times n}$ gilt dann die Gleichung $A = \sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}E_{ij}^{(m,n)}$.

Ist $n = 1$ oder $m = 1$, so erhalten wir die ***Standardvektoren***

$$e_i := E_{i1}^{(m,1)} = \begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix} \in R^{m\times 1} \qquad \text{und} \qquad f_j := E_{1j}^{(1,n)} = \begin{bmatrix} 0 & \dots & 1 & \dots & 0 \end{bmatrix} \in R^{1\times n},$$

wobei in e_i die 1 an der i-ten und in f_j die 1 an der j-ten Stelle steht (und alle anderen Einträge jeweils wieder 0 sind). Ist auch $p \in \mathbb{N}$, so gilt die Produktformel

$$E_{ij}^{(m,n)} \cdot E_{kl}^{(n,p)} = \delta_{jk}E_{il}^{(m,p)} \in R^{m\times p} \qquad \text{für alle erlaubten } i,j,k,l;$$

hier heißt δ_{jk} das ***Kronecker-Delta***; dies ist 1 falls $j = k$, und 0 für $j \neq k$.

Ist $B \in R^{n\times m}$ (also n Zeilen und m Spalten) so erhält man die nützlichen Formeln

$$B \cdot e_i = \text{ } i\text{-te Spalte von } B \qquad \text{und} \qquad f_j \cdot B = \text{ } j\text{-te Zeile von } B.$$

Bemerkung 11.8. Seien $n, m \in \mathbb{N}$ beliebig und $A = [a_{ij}] \in R^{m\times n}$. Sei dann $A^{tr} \in R^{n\times m}$ die Matrix mit Eintrag a_{ji} an der Position (i,j), wobei $1 \leqslant i \leqslant n$ und $1 \leqslant j \leqslant m$.

Die Matrix A^{tr} heißt ***transponierte Matrix***. Zum Beispiel ist $\begin{bmatrix} 2 & 1 & 0 \\ 1 & 3 & 5 \end{bmatrix}^{tr} = \begin{bmatrix} 2 & 1 \\ 1 & 3 \\ 0 & 5 \end{bmatrix}$.

Für das Transponieren gelten die folgenden Regeln (Beweis durch leichtes Nachrechnen):

(a) Es gilt offenbar $(A^{tr})^{tr} = A$.

(b) Für $B \in R^{m\times n}$ und $s \in R$ gelten $(A + B)^{tr} = A^{tr} + B^{tr}$ und $(sA)^{tr} = s(A^{tr})$.

(c) Ist auch $p \in \mathbb{N}$ und $B \in R^{n\times p}$, so gilt $(A \cdot B)^{tr} = B^{tr} \cdot A^{tr}$.

Ist $n = m$, so heißt A eine ***symmetrische Matrix***, wenn $A = A^{tr}$ gilt. Aufgrund der obigen Regeln sind Summen und skalare Vielfache von symmetrischen Matrizen wieder symmetrisch.

Definition 11.9. Sei $m = n$. Eine Matrix $A \in M_n(R)$ heißt ***invertierbar*** (oder ***nicht-singulär***), wenn es eine Matrix $B \in M_n(R)$ gibt mit $A \cdot B = B \cdot A = I_n$.

Zum Beispiel ist $A = \begin{bmatrix} 2 & 1 \\ 5 & 3 \end{bmatrix} \in M_2(\mathbb{Q})$ nicht-singulär, denn mit $B = \begin{bmatrix} 3 & -1 \\ -5 & 2 \end{bmatrix}$ gilt $A \cdot B = B \cdot A = I_2$. Ebenso ist $A = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \in M_2(\mathbb{Q})$ nicht-singulär, denn mit $B = \begin{bmatrix} 1 & 0 \\ 0 & 1/2 \end{bmatrix}$ gilt $A \cdot B = B \cdot A = I_2$. (Beachten Sie: Dieses A hat Einträge in $\mathbb{Z}$, aber A ist nicht invertierbar in $M_2(\mathbb{Z})$.) Die Matrix $A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ ist nicht invertierbar, denn ist $B \in M_2(R)$ beliebig, so besteht die zweite Zeile von $A \cdot B$ nur aus Nullen, also $A \cdot B \neq I_2$.

Satz 11.10. *Sei $m = n$. Dann ist $GL_n(R) := \{A \in M_n(R) \mid A$ nicht-singulär$\}$ eine Gruppe bezüglich der Matrixmultiplikation. Das neutrale Element ist die Einheitsmatrix I_n; die inverse Matrix zu A wird mit A^{-1} bezeichnet.*

Beweis. Nach Satz 11.6 ist die Matrixmultiplikation assoziativ, und I_n ist ein neutrales Element. Sind $A, B \in M_n(R)$ nicht-singulär, so ist auch $A \cdot B$ nicht-singulär, mit inverser Matrix $B^{-1} \cdot A^{-1}$ (siehe Bemerkung 7.1(c)). Also gilt: $A, B \in GL_n(R) \Rightarrow A \cdot B \in GL_n(R)$. Damit sind alle Axiome in Definition 7.2 erfüllt. □

Bemerkung 11.11. (a) Sei $m = n$ und $R = K$ ein Körper. Wir werden später noch effiziente Methoden kennenlernen, um zu testen ob $A \in M_n(K)$ invertierbar ist und dann auch A^{-1} zu berechnen. Außerdem werden wir sehen: Ist $B \in M_n(K)$ mit $A \cdot B = I_n$, so folgt automatisch $B \cdot A = I_n$. — Dies ist nicht offensichtlich!

(b) Für $n = 2$ ist $GL_n(R)$ nicht abelsch. Für $n = 2$ betrachte z.B. die Matrizen $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ und $B = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. Dann rechnen Sie nach, dass A, B invertierbar sind, aber $A \cdot B \neq B \cdot A$.

Sei K ein Körper. Wir versuchen nun zum Schluss, möglichst einfache invertierbare Matrizen in $GL_n(K)$ zu finden; dies wird sich im nächsten Abschnitt als nützlich erweisen. Sei $n \in \mathbb{N}$. Für $1 \leqslant i, j \leqslant n$ sei $E_{ij} \in M_n(K)$ die (i,j)-Standard-Matrix $E_{ij}^{(n,n)}$; siehe Beispiel 11.7.

Für $1 \leqslant i \leqslant n$ und $0 \neq c \in K$ sei $M_i(c) := I_n + (c-1)E_{ii} = \begin{bmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & c & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{bmatrix}$.

(Diagonalmatrix mit c an der i-ten Position und 1 sonst auf der Diagonalen.)

Für $c \in K$ und $1 \leqslant i, j \leqslant n$ mit $i \neq j$ sei $I_{ij}(c) := I_n + cE_{ij} =$ $\begin{bmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 1 & & c & \\ & & & \ddots & & \\ & & & & 1 & \\ & & & & & \ddots \\ & & & & & & 1 \end{bmatrix}$.

(Man nimmt die Einheitsmatrix und setzt noch das c an die Stelle (i, j).)

Für $1 \leqslant i, j \leqslant n$ mit $i \neq j$ sei $V_{ij} := I_n + E_{ij} + E_{ji} - E_{ii} - E_{jj} =$ $\begin{bmatrix} 1 & & & & & \\ & \ddots & & & & \\ & & 0 & \dots & 1 & \\ & & \vdots & & \vdots & \\ & & i & \dots & 0 & \\ & & & & & \ddots \\ & & & & & & 1 \end{bmatrix}$.

(Vertausche in der Einheitsmatrix die i-te und j-te Zeile.)

Diese Matrizen $M_i(c)$, $I_{ij}(c)$, V_{ij} heißen ***Elementarmatrizen***.

Lemma 11.12. *Die oben definierten Elementarmatrizen sind invertierbar, also in* $\mathrm{GL}_n(K)$ *enthalten. Es gilt* $M_i(c)^{-1} = M_i(c^{-1})$, $I_{ij}(c)^{-1} = I_{ij}(-c)$ *und* $V_{ij}^{-1} = V_{ij}$. *Insbesondere ist das Inverse einer Elementarmatrix auch wieder eine Elementarmatrix.*

Beweis. Einfaches Nachrechnen, mit Hilfe der Formeln in Beispiel 11.7. □

Wir werden späten sehen (siehe Satz 13.3), dass sich jede invertierbare Matrix in $\mathrm{GL}_n(K)$ als Produkt von Elementar-Matrizen schreiben lässt.

12. *Elementare Umformungen und das Gauß–Verfahren*

Sei K ein Körper. Ein ***lineares Gleichungssystem*** (LGS) ist ein Gleichungssystem der Form

$$\left.\begin{array}{ccccccccc} a_{11}x_1 & + & \dots & + & a_{1n}x_n & = & b_1 \\ a_{21}x_1 & + & \dots & + & a_{2n}x_n & = & b_2 \\ \vdots & & & & \vdots & & \vdots \\ a_{m1}x_1 & + & \dots & + & a_{mn}x_n & = & b_m \end{array}\right\} \quad (*)$$

wobei $m, n \in \mathbb{N}$, die Koeffizienten $a_{ij} \in K$ und $b_i \in K$ vorgegeben und die $x_i \in K$ gesucht sind. (Wir haben m Gleichungen und n Unbekannte $x_1, \dots, x_n$.) Das LGS heißt ***homogen***, wenn $b_i = 0$ für alle i gilt; sonst heißt das LGS ***inhomogen***. Die ***Lösungsmenge*** eines LGS (egal ob homogen oder inhomogen) ist gegeben durch

$$L := \left\{ \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \in K^n \;\middle|\; x_1, \dots, x_n \text{ Lösung von } (*) \right\}.$$

Bemerkung 12.1. Mit obigen Bezeichnungen bilden wir die $(m \times n)$-Matrix $A = [a_{ij}] \in K^{m \times n}$ und den Spaltenvektor $b \in K^m$ mit Einträgen $b_1, \dots, b_m$. Seien $x_1, \dots, x_n \in K$. Mit der Definition des Matrixproduktes folgt dann sofort:

$$x := \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \in L \quad \text{(d.h., } x \text{ ist Lösung von } (*)) \qquad \Leftrightarrow \qquad A \cdot x = b.$$

Dann heißt $[A|b] := \left[\begin{array}{cccc|c} a_{11} & a_{12} & \dots & a_{1n} & b_1 \\ a_{21} & a_{22} & \dots & a_{2n} & b_2 \\ \vdots & \vdots & & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} & b_m \end{array}\right] \in K^{m\times(n+1)}$ ***erweiterte Matrix des LGS***.

(Ist $b_i = 0$ für alle i, so bezeichnen wir einfach A als Matrix des LGS.)

Beispiel 12.2. (a) Sei K beliebig. Die beiden Gleichungen $x_1 + x_2 = 1$, $x_1 + x_2 = 0$ bilden ein LGS mit $m = n = 2$; die erweiterte Matrix ist $\left[\begin{array}{cc|c} 1 & 1 & 1 \\ 1 & 1 & 0 \end{array}\right]$. Es gibt keine Lösung, $L = \varnothing$.

(b) Sei $K = \mathbb{Q}$. Die Gleichungen $x_1 + x_2 = 1$ und $x_2 - x_3 = 2$ bilden ein LGS mit $m = 2$, $n = 3$; die erweiterte Matrix ist $\left[\begin{array}{ccc|c} 1 & 1 & 0 & 1 \\ 0 & 1 & -1 & 2 \end{array}\right]$.
Lösung: Aus der 2. Gleichung erhalten wir $x_2 = 2 + x_3$; einsetzen in die 1. Gleichung ergibt $x_1 + (2 + x_3) = 1$, also $x_1 = -1 - x_3$. Damit

$$L = \left\{ \begin{bmatrix} -1 - x_3 \\ 2 + x_3 \\ x_3 \end{bmatrix} \;\middle|\; x_3 \in \mathbb{Q} \text{ beliebig} \right\}.$$

(c) Sei $K = \mathbb{Q}$. Die Gleichungen $x_1 + x_2 = 3$ und $3x_1 - x_2 = 1$ bilden ein LGS mit $m = n = 2$; die erweiterte Matrix ist $\left[\begin{array}{cc|c} 1 & 1 & 3 \\ 3 & -1 & 1 \end{array}\right]$.
Lösung: Addiere 1. Gleichung zur 2. Gleichung und erhalte $4x_1 = 4$, also $x_1 = 1$; einsetzen in die 1. Gleichung ergibt dann $1 + x_2 = 3$, also $x_2 = 2$. Damit $L = \left\{ \begin{bmatrix} 1 \\ 2 \end{bmatrix} \right\}$.

Wir sehen also: Ein LGS kann gar keine Lösung haben, genau eine Lösung oder unendlich viele Lösungen. Ein systematisches Lösungsverfahren ist durch die ***Gauß–Elimination*** gegeben. Dabei formt man die Gleichungen so um, dass das LGS eine einfachere Gestalt bekommt und man die Lösungen leicht ablesen kann. Grundlage dafür ist folgende Bemerkung.

Bemerkung 12.3. Gegeben sei ein LGS $(*)$, mit erweiterter Matrix $[A|b] \in K^{m\times(n+1)}$ und Lösungsmenge $L \subseteq K^n$. Sei nun $Q \in M_m(K)$; setze $A' := Q \cdot A$, $b' := Q \cdot b$. Aufgrund der Definition der Matrixmultiplikation gilt dann auch $[A'|b'] = Q \cdot [A|b]$. Wir erhalten ein neues LGS mit erweiterter Matrix $[A'|b'] \in K^{m\times(n+1)}$; sei $L' \subseteq K^n$ dessen Lösungsmenge. Dann gilt $L \subseteq L'$; ist $Q \in GL_m(K)$ invertierbar, so gilt $L = L'$.

Denn: Sei $x \in L$, also $A \cdot x = b$. Dann folgt $A' \cdot x = (Q \cdot A) \cdot x = Q \cdot (A \cdot x) = Q \cdot b = b'$, also $x \in L'$. Damit ist $L \subseteq L'$ gezeigt. Sei nun Q invertierbar. Dann folgt $A = Q^{-1} \cdot A'$ und $b = Q^{-1} \cdot b'$. Ist also $x' \in L'$, so folgt mit dem gleichen Argument wie zuvor auch $x' \in L$. $\square$

Wir bringen nun die am Ende des letzten Abschnitts definierten ***Elementarmatrizen*** ins Spiel. Im folgenden Satz sind $M_i(c)$, $I_{ij}(c)$ und V_{ij} Matrizen der Grösse $m \times m$.

Satz 12.4. *Sei $A \in K^{m\times n}$. Dann gilt:*
(a) $M_i(c) \cdot A$ *ist die Matrix, die aus A entsteht, wenn man die i-te Zeile mit c multipliziert.*
(b) $I_{ij}(c) \cdot A$ *ist die Matrix, die aus A entsteht, wenn man das c-Fache der j-ten Zeile zur i-ten Zeile addiert.*
(c) $V_{ij} \cdot A$ *ist die Matrix, die aus A entsteht, wenn man die i-te und j-te Zeile vertauscht.*

Entsprechende Aussagen gelten auch für $B \in R^{n\times m}$ und die Produkte $B \cdot M_i(c)$, $B \cdot I_{ij}(c)$, $B \cdot V_{ij}$, wobei die obigen Operationen mit den Spalten von B ausgeführt werden.

Beweis. Auch dies erfolgt durch Nachrechnen, wobei man mehrere Fälle unterscheiden muss. Es hilft, wenn man zuerst den Fall $m = 2$ betrachtet, also:

$$M_1(c) \cdot A = \begin{bmatrix} c & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \end{bmatrix} = \begin{bmatrix} ca_{11} & ca_{12} & \dots & ca_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \end{bmatrix};$$

$$M_2(c) \cdot A = \begin{bmatrix} 1 & 0 \\ 0 & c \end{bmatrix} \cdot \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ ca_{21} & ca_{22} & \dots & ca_{2n} \end{bmatrix};$$

$$I_{12}(c) \cdot A = \begin{bmatrix} 1 & c \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \end{bmatrix} = \begin{bmatrix} a_{11}+ca_{21} & a_{12}+ca_{22} & \dots & a_{1n}+ca_{2n} \\ a_{21} & a_{22} & \dots & a_{2n} \end{bmatrix};$$

$$I_{21}(c) \cdot A = \begin{bmatrix} 1 & 0 \\ c & 1 \end{bmatrix} \cdot \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21}+ca_{11} & a_{22}+ca_{12} & \dots & a_{2n}+ca_{1n} \end{bmatrix};$$

$$V_{12} \cdot A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \end{bmatrix} = \begin{bmatrix} a_{21} & a_{22} & \dots & a_{2n} \\ a_{11} & a_{12} & \dots & a_{1n} \end{bmatrix}.$$

Die weiteren Details seien Ihnen als Übung überlassen. □

Ab hier Woche 8

Seien $A, B \in K^{m\times n}$. Wir sagen, dass B aus A durch ***elementare Umformungen*** (oder genauer: ***elementare Zeilenumformungen***) entsteht (und schreiben $A \to B$), wenn man B aus A durch eine endliche Folge von Operationen wie in Satz 12.4 erhält, also:

(a) Multipliziere eine Zeile mit einem Element $0 \neq c \in K$.
(b) Addiere das c-Fache (für ein $c \in K$) einer Zeile zu einer anderen Zeile.
(c) Vertausche zwei Zeilen.

Entsprechend können auch ***elementare Spaltenumformungen*** definiert werden.

Satz 12.5 (***Gauß–Elimination***)**.** *Sei K ein Körper und $A \in K^{m\times n}$. Dann lässt sich A durch eine endliche Folge von elementaren Zeilenumformungen auf **Stufenform** bringen.*

Hier sagen wir, dass $A' = [a'_{ij}] \in K^{m\times n}$ **Stufenform** hat, wenn es ein $r \in \{0, 1, 2, \ldots, m\}$ und (Spalten-)Indizes $1 \leqslant j_1 < j_2 < \ldots < j_r \leqslant n$ gibt, so dass A' folgende Gestalt besitzt:

$$\begin{array}{c} \\ 1 \\ 2 \\ \vdots \\ \\ r \\ \hline r{+}1 \\ \vdots \\ m \end{array}
\begin{array}{c}
\begin{array}{ccccccccccccc} & & & & j_1 & & & j_2 & & j_3 & \cdots & & j_r \end{array} \\
\left[\begin{array}{ccccccccccccc}
0 & \ldots & 0 & 1 & * & \cdots & * & 0 & * & \cdots & * & 0 & * & \cdots & \\
 & & & & & & & 1 & * & \cdots & * & 0 & * & \cdots & \\
 & & & & & & & & & 1 & * & \cdots & * & \cdots & \\
 & & & & & & & & & & & \ddots & & & \\
 & & & & & & & & & & & & & 1 & * \cdots *
\end{array}\right] \\
\begin{array}{ccccccccccccc} & & & & & & & & & & & & & & \end{array} \\
\left[\begin{array}{ccccccccccccc}
 & & & & & & & & & & & & & & \\
 & & & & & & & & & & & & & & \\
 & & & & & & & & & & & & & & \\
 & & & & & & & & & & & & & & \\
 & & & & & & & & & & & & & &
\end{array}\right]
\end{array}$$

(Hier 0 vor jeder 1)

(Alles 0 hier)

Die Sterne $*$ stehen hier für beliebige Elemente aus K als Einträge; links vor sowie oberhalb und unterhalb den Einsen in den Spalten $j_1, \ldots, j_r$ stehen nur Nullen. Oder in Formeln:

$$\begin{array}{rcll} a'_{ij} & = & 0 & \text{für } i > r \text{ und alle } j = 1, \ldots, n, \\ a'_{ij} & = & 0 & \text{für } 1 \leqslant i \leqslant r \text{ und } 1 \leqslant j < j_i, \\ a'_{ij_i} & = & 1 & \text{für } 1 \leqslant i \leqslant r, \\ a'_{kj_i} & = & 0 & \text{für } 1 \leqslant k \leqslant r \text{ und } k \neq i. \end{array}$$

Die Indizes $j_1, \ldots, j_r$ werden auch ***Pivots*** genannt. (Beachten Sie, dass in manchen Texten nicht verlangt wird, dass oberhalb der Einsen in den Spalten $j_1, \ldots, j_r$ nur Nullen stehen.) Bevor wir dies allgemein beweisen, zuerst ein Beispiel (mit $K = \mathbb{Q}$).

$$\begin{aligned} A = \begin{bmatrix} 0 & 0 & 2 & 2 & 0 & 2 \\ 2 & 4 & 2 & 6 & 0 & 4 \\ 3 & 6 & 0 & 6 & 1 & 4 \end{bmatrix} &\to \begin{bmatrix} 2 & 4 & 2 & 6 & 0 & 4 \\ 0 & 0 & 2 & 2 & 0 & 2 \\ 3 & 6 & 0 & 6 & 1 & 4 \end{bmatrix} \to \begin{bmatrix} 1 & 2 & 1 & 3 & 0 & 2 \\ 0 & 0 & 2 & 2 & 0 & 2 \\ 3 & 6 & 0 & 6 & 1 & 4 \end{bmatrix} \\ &\to \begin{bmatrix} \underline{1} & 2 & 1 & 3 & 0 & 2 \\ 0 & 0 & 2 & 2 & 0 & 2 \\ 0 & 0 & -3 & -3 & 1 & -2 \end{bmatrix} \to \begin{bmatrix} \underline{1} & 2 & 1 & 3 & 0 & 2 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & -3 & -3 & 1 & -2 \end{bmatrix} \to \begin{bmatrix} \underline{1} & 2 & 1 & 3 & 0 & 2 \\ 0 & 0 & \underline{1} & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & \underline{1} & 1 \end{bmatrix} \\ &\to \begin{bmatrix} \underline{1} & 2 & 0 & 2 & 0 & 1 \\ 0 & 0 & \underline{1} & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & \underline{1} & 1 \end{bmatrix} =: A' \qquad \text{mit } r = 3 \text{ und Pivots } j_1 = 1,\ j_2 = 3,\ j_3 = 5. \end{aligned}$$

Die 6 Pfeile $\to$ entsprechen dabei (von links nach rechts) den elementaren Schritten V_{12}, $M_1(1/2)$, $I_{31}(-3)$, $M_2(1/2)$, $I_{32}(3)$, $I_{12}(-1)$. (Der letzte Schritt ist nur nötig um alle Einträge über dem Pivot $j_2 = 3$ gleich 0 zu machen.) Mit Satz 12.4 erhalten wir dann auch $A' = Q \cdot A$ mit $Q := I_{12}(-1) \cdot I_{32}(3) \cdot M_2(1/2) \cdot I_{31}(-3) \cdot M_1(1/2) \cdot V_{12}$.

Beweis von Satz 12.5. (Vollständige Induktion nach m.) Für den Startwert $m = 1$ ist $A = [a_{11} \ \ldots \ a_{1n}] \in K^{1\times n}$ eine Zeile. Sind alle Einträge gleich 0, so sind wir fertig mit $r = 0$. Andernfalls sei $j_1 := \min\{j \mid a_{1j} \neq 0\}$. Multiplizieren mit $a_{1j_1}^{-1}$ ergibt $A \to [0 \ \ldots \ 0 \ 1 \ * \ \ldots \ *]$, wobei die 1 an der Stelle j_1 steht; also haben wir Stufenform erreicht mit $r = 1$.

Sei nun $m \geqslant 2$ und die Aussage bereits für $(m-1)\times n$-Matrizen gezeigt. Ist $A = 0_{m\times n}$, so hat A Stufenform mit $r = 0$. Andernfalls sei $j_1 := \min\{j \mid j\text{-te Spalte von } A \text{ enthält Eintrag} \neq 0\}$. Sei $i \in \{1,\dots,m\}$ mit $a_{ij_1} \neq 0$. Dann multipliziere die i-te Zeile mit $a_{ij_1}^{-1}$; ist $i > 1$, so vertausche außerdem die i-te mit der 1. Zeile. Dies ergibt:

$$A \quad \to \quad B := \begin{bmatrix} 0 & \dots & 0 & 1 & * & \dots & * \\ 0 & \dots & 0 & b_{2j_1} & * & \dots & * \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & b_{mj_1} & * & \dots & * \end{bmatrix}$$

Dann addiere nacheinander:

$$\left.\begin{array}{l} \text{das } (-b_{2j_1})\text{-Fache der 1. Zeile zur 2. Zeile} \\ \text{das } (-b_{3j_1})\text{-Fache der 1. Zeile zur 3. Zeile} \\ \quad\vdots \\ \text{das } (-b_{mj_1})\text{-Fache der 1. Zeile zur m. Zeile} \end{array}\right\} \quad \to \quad \begin{bmatrix} 0 & \dots & 0 & 1 & * & \dots & * \\ 0 & \dots & 0 & 0 & * & \dots & * \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & 0 & * & \dots & * \end{bmatrix}$$

Sei nun $C \in K^{(m-1)\times n}$ die Matrix, die aus den Zeilen $2, 3, \dots, m$ der Matrix auf der rechten Seite besteht. Nach Induktion kann man C auf Stufenform bringen. Insgesamt also

$$A \to \begin{array}{c} \\ 1 \\ 2 \\ \vdots \\ \\ r \\ \hline r+1 \\ \vdots \\ m \end{array} \begin{array}{c} \begin{array}{ccccccccccccc} & & & & j_1 & & & j_2 & & & j_3 & \dots & & & j_r & & \\ \end{array} \\ \left[\begin{array}{ccccccccccccc} 0 & \dots & 0 & 1 & * & \dots & * & * & * & \dots & * & * & * & \dots & & & \\ & & & & & & & 1 & * & \dots & * & 0 & * & \dots & & & \\ & & & & & & & & & & 1 & * & \dots & * & & & \\ & & & & & & & & & & & \ddots & & & & & \\ & & & & & & & & & & & & & & 1 & * & \dots & * \\ \hline 0 & & & & & & & \dots & & & & & & & & 0 & \\ \vdots & & & & & & & & & & & & & & & \vdots & \\ 0 & & & & & & & \dots & & & & & & & & 0 & \end{array}\right] \end{array}$$

Schließlich addiere noch passende Vielfache der Zeilen $2, 3, \dots, r$ zur 1. Zeile, um die Einträge in der 1. Zeile oberhalb der Pivots $j_2, \dots, j_r$ zu Null zu machen. □

Es ist eine exzellente Übung, obiges Verfahren in einer Programmiersprache Ihrer Wahl zu programmieren. In GAP gibt es dazu bereits eine Funktion:

```
gap> TriangulizedMat([[0,0,2,2,0,2],[2,4,2,6,0,4],[3,6,0,6,1,4]]);
[ [ 1, 2, 0, 2, 0, 1 ], [ 0, 0, 1, 1, 0, 1 ], [ 0, 0, 0, 0, 1, 1 ] ]
```

Folgerung 12.6. *Sei $A \in K^{m\times n}$. Dann gibt es eine invertierbare Matrix $Q \in \mathrm{GL}_m(K)$, so dass $Q\cdot A \in K^{m\times n}$ Stufenform hat; Q ist ein Produkt von endlich vielen Elementar-Matrizen.*

Beweis. Nach Satz 12.4 werden die im Gauß–Verfahren verwendeten elementaren Umformungen durch schrittweise Multiplikationen mit Elementarmatrizen realisiert; letztere sind invertierbar nach Lemma 11.12. Ist also $A \to A'$ und A' in Stufenform, so gilt $A' = Q \cdot A$, wobei Q Produkt von Elementarmatrizen ist. □

Anwendung auf lineare Gleichungssysteme

Gegeben sei ein LGS mit erweiterter Matrix $[A|b] \in K^{m\times(n+1)}$. Gesucht ist die Lösungsmenge $L = \{x \in K^n \mid A \cdot x = b\}$. Dazu bringen wie $[A|b]$ nach obigem Verfahren auf Stufenform, also $[A|b] \to [A'|b']$ mit $A' \in K^{m\times n}$ und $b' \in K^m$. Mit Folgerung 12.6 und Bemerkung 12.3 folgt dann $L = \{x \in K^n \mid A' \cdot x = b'\}$. Nehmen wir an, dass $[A|b]$ nicht nur aus Nullen besteht; dann haben wir $r \in \{1, \dots, m\}$ Stufen in $[A'|b']$ und Pivots $1 \leqslant j_1 < \dots < j_r \leqslant n+1$.

1. Fall: $j_r = n+1$. Dann ist die r-te Zeile in $[A'|b']$ gegeben durch $[0 \ \dots \ 0 \ 1]$. Dies entspricht der Gleichung $0 \cdot x_1 + \dots + 0 \cdot x_n = 1$. Also gibt es in diesem Fall keine Lösung, $L = \varnothing$.

2. Fall: $j_r \leqslant n$. Setzen wir $I := \{1, \dots, n\} \setminus \{j_1, \dots, j_r\}$, so besteht das durch $[A'|b']$ gegebene LGS aufgrund der Bedingungen in der Stufenform aus den folgenden Gleichungen:

$$\begin{array}{rcl}
x_{j_1} + \sum_{j\in I} a'_{1j}x_j &=& b'_1 \\
x_{j_2} + \sum_{j\in I} a'_{2j}x_j &=& b'_2 \\
\vdots \qquad\quad \vdots &&\ \vdots \\
x_{j_r} + \sum_{j\in I} a'_{rj}x_j &=& b'_r
\end{array}
\quad\rightsquigarrow\quad
\begin{array}{rcl}
x_{j_1} &=& b'_1 - \sum_{j\in I} a'_{1j}x_j \\
x_{j_2} &=& b'_2 - \sum_{j\in I} a'_{2j}x_j \\
\vdots \quad\ \vdots &&\ \vdots \\
x_{j_r} &=& b'_r - \sum_{j\in I} a'_{rj}x_j
\end{array}$$

Hier sind alle x_j mit $j \in I$ (d.h., alle x_j außer $\{x_{j_1}, \dots, x_{j_r}\}$) frei wählbar, und $x_{j_1}, \dots, x_{j_r}$ sind dann durch die obigen Gleichungen bestimmt. Daher heißen $x_{j_1}, \dots, x_{j_r}$ auch "Pivot-Variablen" und die restlichen $n - r$ Unbekannten $\{x_j \mid j \in I\}$ heißen "freie Variablen".

Beispiel 12.7. (a) Betrachte das LGS mit $[A|b] = \left[\begin{array}{cc|c} 1 & 1 & 1 \\ 1 & 1 & 0 \end{array}\right]$, wie in Beispiel 12.2(a). Dann ist $[A|b] \to \left[\begin{array}{cc|c} 1 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right]$, also $r = 2$, $j_1 = 1$, $j_2 = 3$. Wir sind im 1. Fall, also $L = \varnothing$.

(b) Sei $[A|b] = \left[\begin{array}{ccc|c} 1 & 1 & 0 & 1 \\ 0 & 1 & -1 & 2 \end{array}\right]$, wie in Beispiel 12.2(b). Dann ist $[A|b] \to \left[\begin{array}{ccc|c} 1 & 0 & 1 & -1 \\ 0 & 1 & -1 & 2 \end{array}\right]$. Wir sind im 2. Fall, mit Pivot-Variablen x_1, x_2 und einer freien Variablen x_3. Wir schreiben die neuen Gleichungen hin und lösen dann nach den Pivot-Variablen auf:

$$\begin{array}{rcl}
\underline{x_1} + x_3 &=& -1 \\
\underline{x_2} - x_3 &=& 2
\end{array}
\quad\rightsquigarrow\quad
\begin{array}{rcl}
x_1 &=& -1 - x_3 \\
x_2 &=& 2 + x_3
\end{array}.$$

Also erhalten wir als Lösungsmenge $L = \left\{ \begin{bmatrix} -1 - x_3 \\ 2 + x_3 \\ x_3 \end{bmatrix} \;\middle|\; x_3 \in \mathbb{Q} \right\} = \left\{ \begin{bmatrix} -1 - t \\ 2 + t \\ t \end{bmatrix} \;\middle|\; t \in \mathbb{Q} \right\}$.

(c) Sei $[A|b] = \left[\begin{array}{cc|c} 1 & 1 & 3 \\ 3 & -1 & 1 \end{array}\right]$, wie in Beispiel 12.2(c). Dann ist $[A|b] \to \left[\begin{array}{cc|c} 1 & 0 & 1 \\ 0 & 1 & 2 \end{array}\right]$, also 2. Fall mit Pivot-Variablen x_1, x_2 und keiner freien Variablen. Die neuen Gleichungen sind jetzt einfach gegeben durch $x_1 = 1$ und $x_2 = 2$. Also erhalten wir $L = \left\{ \begin{bmatrix} 1 \\ 2 \end{bmatrix} \right\}$.

Betrachten wir schließlich auch noch das LGS mit erweiterter Matrix

$$[A|b] = \left[\begin{array}{ccccc|c} 0 & 0 & 2 & 2 & 0 & 2 \\ 2 & 4 & 2 & 6 & 0 & 4 \\ 3 & 6 & 0 & 6 & 1 & 4 \end{array}\right] \quad \to \quad \left[\begin{array}{ccccc|c} \underline{1} & 2 & 0 & 2 & 0 & 1 \\ 0 & 0 & \underline{1} & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & \underline{1} & 1 \end{array}\right] \qquad \text{(siehe oben).}$$

Wir sind im 2. Fall mit Pivot-Variablen x_1, x_3, x_5 und freien Variablen x_2, x_4. Wir schreiben wieder die neuen Gleichungen hin und lösen dann nach den Pivot-Variablen auf:

$$\begin{array}{rcl} \underline{x_1} + 2x_2 + 2x_4 &=& 1 \\ \underline{x_3} + x_4 &=& 1 \\ \underline{x_5} &=& 1 \end{array} \quad \rightsquigarrow \quad \begin{array}{rcl} x_1 &=& 1 - 2x_2 - 2x_4 \\ x_3 &=& 1 - x_4 \\ x_5 &=& 1 \end{array} \quad \rightsquigarrow \quad L = \left\{ \left[\begin{array}{c} 1-2s-2t \\ s \\ 1-t \\ t \\ 1 \end{array}\right] \;\middle|\; s,t \in \mathbb{Q} \right\}.$$

Bemerkung 12.8. Ist $r = n \leqslant m$ und $j_r \leqslant n$, so gibt es keine freien Variablen und die Pivot-Variablen sind $x_1, \ldots, x_n$. In diesem Fall gibt es eine eindeutige Lösung:

$$[A|b] \quad \to \quad [A'|b'] = \left[\begin{array}{ccc|c} 1 & & 0 & b'_1 \\ & \ddots & & \vdots \\ 0 & & 1 & b'_n \\ \hline & & & \\ 0 & \ldots & 0 & 0 \end{array}\right] \quad \rightsquigarrow \quad L = \left\{ \left[\begin{array}{c} b'_1 \\ \vdots \\ b'_n \end{array}\right] \right\}.$$

(Unterhalb des Querstrichs sind die Zeilen $n+1, n+2, \ldots, m$, mit allen Einträgen gleich 0.)

13. *Ergänzungen, Beispiele und Anwendungen*

Die im letzten Abschnitt behandelten Themen, also lineare Gleichungssysteme, elementare Umformungen und Gauß–Elimination, sind zentral nicht nur für diese Vorlesung, sondern für viele Anwendungen in der Mathematik selbst und in den Natur- und Ingenieurwissenschaften. Wir diskutieren nun noch eine Reihe von Ergänzungen und Beispielen. Sei K stets ein Körper.

Betrachten wir zuerst ein homogenes LGS mit Matrix $A \in K^{m\times n}$; die Lösungsmenge ist gegeben durch $L = \{x \in K^n \mid A \cdot x = 0_m\}$, wobei 0_m den Null-Spaltenvektor in K^m bezeichne. Es ist klar, dass $x = 0_n \in K^n$ stets eine Lösung ist (daher auch "triviale" Lösung genannt). Die Frage ist, wann es auch noch nicht-triviale Lösungen gibt.

Satz 13.1. *Sei $A \in K^{m\times n}$ mit $m < n$ (also mehr Unbekannte als Gleichungen). Dann gibt es ein $x \in K^n$ mit $A \cdot x = 0_m$ und $x \neq 0_n$ (also eine nicht-triviale Lösung).*

Beweis. Die erweiterte Matrix des LGS ist gegeben durch $[A|b]$ mit $b = 0_m$. Mit Gauß–Elimination erhalten wir $[A|b] \to [A'|b']$ wobei $[A'|b']$ Stufenform hat, mit $0 \leqslant r \leqslant m$ und Pivots $1 \leqslant j_1 < \ldots < j_r \leqslant n+1$. Wegen $b = 0_m$ ist offenbar auch $b' = 0_m$ und damit $j_r \leqslant n$. Wie im letzten Abschnitt besprochen, ist damit $L \neq \varnothing$ (wir sind im 2. Fall auf S. 55).
Es gibt r Pivot-Variablen und $n - r$ freie Variablen. Nach Voraussetzung ist $n > m \geqslant r$

und damit $n - r > 0$. Es gibt also sicher freie Variablen. Diese können wir zum Beispiel alle gleich 1 setzen und erhalten damit auf jeden Fall ein $x \in K^n$ mit $A \cdot x = 0_m$ und $x \neq 0_n$. □

Beispiel 13.2. Gegeben seien Matrizen $A_1, \ldots, A_N \in K^{m \times n}$, wobei $N \geqslant 1$. Ist $N > nm$, so gibt es eine nicht-triviale lineare Relation zwischen $A_1, \ldots, A_N$, d.h., es gibt Koeffizienten $c_1, \ldots, c_N \in K$, die nicht alle gleich 0 sind, mit $c_1 A_1 + \ldots + c_N A_N = 0_{m \times n}$.

Dazu: Wir schreiben $A_k = [a_{ij}^{(k)}]_{1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n}$ für $k = 1, \ldots, N$. Dann betrachten wir das homogene LGS, dessen Gleichungen gegegen sind durch

$$a_{ij}^{(1)} x_1 + a_{ij}^{(2)} x_2 + \ldots + a_{ij}^{(N)} x_N = 0 \qquad \text{für } 1 \leqslant i \leqslant m \text{ und } 1 \leqslant j \leqslant n.$$

Es gibt also insgesamt nm Gleichungen, mit N Unbekannten $x_1, \ldots, x_N$. Ist $N > nm$, so gibt es nach Satz 13.1 eine nicht-triviale Lösung $x_1, \ldots, x_N$; damit gilt $x_1 A_1 + \ldots + x_N A_N = 0_{m \times n}$.

Als nächstes klären wir einige noch offene Fragen zu invertierbaren Matrizen.

Satz 13.3 (Charakterisierung invertierbarer Matrizen)**.** *Sei $A \in M_n(K)$. Dann sind folgende Aussagen äquivalent.*

(a) $A \to I_n$ *(d.h., Gauß–Elimination liefert als Ergebnis die Einheitsmatrix I_n).*

(b) A *ist ein Produkt von Elementarmatrizen.*

(c) A *ist invertierbar (siehe Definition 11.9).*

(d) *Das homogene* LGS *mit Matrix A hat nur die triviale Lösung.*

Beweis. Wir müssen bei einer solchen Aussage nicht alle möglichen Äquivalenzen einzeln zeigen (in diesem Fall wären dies $\binom{4}{2} = 6$ Einzel-Beweise), sondern drehen einmal eine Runde.
"(a) ⇒ (b)" Nach Folgerung 12.6 gibt es endlich viele Elementarmatrizen $E_1, \ldots, E_k \in M_n(K)$, so dass $E_1 \cdot E_2 \cdot \ldots \cdot E_k \cdot A$ Stufenform hat, nach Voraussetzung (a) das Ergebnis also gleich I_n ist, d.h., $E_1 \cdot E_2 \cdot \ldots \cdot E_k \cdot A = I_n$. Nach Lemma 11.12 sind alle E_i invertierbar. Sukzessives Multiplizieren mit den E_i^{-1} ergibt dann $A = E_k^{-1} \cdot \ldots \cdot E_2^{-1} \cdot E_1^{-1}$. Ebenfalls nach Lemma 11.12 ist jedes E_i^{-1} wiederum eine Elementarmatrix, also folgt (b).

"(b) ⇒ (c)" Sei $A = E_1 \cdot E_2 \cdot \ldots \cdot E_k$ mit Elementarmatrizen E_i. Nach Lemma 11.12 ist jedes E_i invertierbar; setze dann $B := E_k^{-1} \cdot \ldots \cdot E_2^{-1} \cdot E_1^{-1}$. Es folgt $A \cdot B = B \cdot A = I_n$, also (c).
"(c) ⇒ (d)" Sei $x \in K^n$ mit $A \cdot x = 0_n$. Nach Voraussetzung (c) gibt es $B \in M_n(K)$ mit $A \cdot B = B \cdot A = I_n$. Also folgt $x = I_n \cdot x = (B \cdot A) \cdot x = B \cdot (A \cdot x) = B \cdot 0_n = 0_n$, d.h., (d).
"(d) ⇒ (a)" Sei $A \to A'$ wobei A' Stufenform hat mit $0 \leqslant r \leqslant n$ und Pivots $1 \leqslant j_1 < \ldots < j_r \leqslant n$. Nun ist $L = \{x \in K^n \mid A \cdot x = 0_n\} = \{x \in K^n \mid A' \cdot x = 0_n\}$, und nach Voraussetzung (d) besteht dies nur aus $x = 0_n$. Also kann es keine freien Variablen geben, d.h., es muss $r = n$ gelten. Wegen $1 \leqslant j_1 < \ldots < j_r \leqslant n$ folgt dann $j_1 = 1$, $j_2 = 2$, …, $j_n = n$ und damit $A' = I_n$ (siehe auch Bemerkung 12.8; wir sind dort im Fall $n = m$). □

Bemerkung 13.4. Sei $A \in M_n(K)$. Ist $B \in M_n(K)$ Matrix mit $A \cdot B = I_n$, so folgt $B \cdot A = I_n$; also ist A invertierbar. (Analog: Aus $B \cdot A = I_n$ folgt $A \cdot B = I_n$.)

Dazu: Betrachte das homogene LGS mit Matrix B. Ist $x \in K^n$ eine Lösung, so folgt $x = I_n \cdot x = (A \cdot B) \cdot x = A \cdot (B \cdot x) = A \cdot 0_n = 0_n$, also gibt es nur die triviale Lösung. Nach Satz 13.3 ist B invertierbar, also gibt es $C \in M_n(K)$ mit $B \cdot C = C \cdot B = I_n$. Aber dann ist $A = A \cdot I_n = A \cdot (B \cdot C) = (A \cdot B) \cdot C = I_n \cdot C = C$, also A invertierbar. □

Folgerung 13.5 (Berechnen von A^{-1})**.** *Sei $A \in M_n(K)$ und bilde die Matrix $[A|I_n] \in K^{n \times 2n}$. Bringe diese Matrix auf Stufenform, also $[A|I_n] \to [A'|B]$ mit $A', B \in M_n(K)$ und Pivots $1 \leqslant j_1 < \ldots < j_r \leqslant 2n$, wobei $0 \leqslant r \leqslant n$. Dann gilt $r = n$ und es gibt zwei Fälle:*

(1) *Ist $j_r > n$, so ist A nicht invertierbar.*

(2) *Andernfalls ist $j_r = n$, $A' = I_n$ und A invertierbar, mit $A^{-1} = B$.*

Beweis. Nach Folgerung 12.6 gibt es ein $Q \in GL_n(K)$ mit $Q \cdot [A|I_n] = [A'|B]$. Aufgrund der Definition der Matrixmultiplikation gilt dann $Q \cdot A = A'$ und $Q = Q \cdot I_n = B$. Annahme, es wäre $r < n$. Dann ist die letzte Zeile von A' und von B gleich 0, Widerspruch dazu, dass $B = Q$ invertierbar ist. Also war die Annahme falsch, d.h., es ist $r = n$.

Sei nun $j_r > n$ und betrachte $[A'|B]$. Wegen $j_r > n$ ist die letzte Zeile von A' gleich 0, also ist A' nicht invertierbar. Wäre A invertierbar, so auch $Q \cdot A = A'$, Widerspruch. Also ist A in diesem Fall nicht invertierbar.

Sei schließlich $j_r \leqslant n$. Wegen $r = n$ und $1 \leqslant j_1 < \ldots < j_r \leqslant n$ folgt dann $j_1 = 1$, $j_2 = 2$, …, $j_n = n$ und damit $A' = I_n$ (siehe wiederum Bemerkung 12.8). Also ist $Q \cdot A = I_n$ und damit nach Bemerkung 13.4 auch A invertierbar, mit $A^{-1} = Q = B$. □

Sei zum Beispiel $K = \mathbb{F}_2 = \{0, 1\}$ mit $1 + 1 = 0$ (wir lassen den Querstrich über $0, 1$ der Einfachheit halber weg) und $A = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix} \in M_3(K)$. Dann erhalten wir

$$[A|I_3] = \left[\begin{array}{ccc|ccc} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{array}\right] \quad \to \quad \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{array}\right] \quad \rightsquigarrow \quad A^{-1} = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}.$$

Beispiel 13.6. Gegeben seien paarweise verschiedene Elemente $x_1, \ldots, x_n \in K$. Dann heißt

$$V(x_1, \ldots, x_n) := \begin{bmatrix} 1 & x_1 & x_1^2 & \ldots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \ldots & x_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & x_n & x_n^2 & \ldots & x_n^{n-1} \end{bmatrix} \in M_n(K)$$

die zugehörige ***Vandermonde-Matrix***. Behauptung: $V(x_1, \ldots, x_n)$ ist invertierbar.
Dazu: Wir zeigen, dass das homogene LGS mit Matrix $V := V(x_1, \ldots, x_n) \in M_n(K)$ nur die

Lösung 0_n hat. Sei also $c \in K^n$ mit Komponenten $c_0, c_1, \ldots, c_{n-1} \in K$ und so dass $V \cdot c = 0_n$ gilt. Dann ist für $1 \leqslant i \leqslant n$ die i-te Komponente von $V \cdot c = 0_n$ gegeben durch:

$$c_0 + c_1 x_i + c_2 x_i^2 + \ldots + c_{n-1} x_i^{n-1} = 0.$$

Definieren wir also $f \in P_{n-1}(K)$ durch $f(x) := c_0 + c_1 x + c_2 x^2 + \ldots + c_{n-1} x^{n-1}$ für alle $x \in K$, so hat f die n Nullstellen $x_1, \ldots, x_n$. Nehmen wir an, nicht alle c_i sind gleich 0. Setzen wir $m := \max\{i \mid c_i \neq 0\}$, so ist also $f \in \hat{P}_m(K)$. Nach Folgerung 9.2 kann dann f aber höchstens $m \leqslant n-1$ Nullstellen haben, Widerspruch. □

Lemma 13.7. *Sei $A \in M_n(K)$ eine spalten-stochastische Matrix. Dann gibt es einen "stationären" Vektor $x \in K^n$, d.h., es gilt $x \neq 0_n$ und $A \cdot x = x$.*

Hier heißt eine Matrix $A = [a_{ij}] \in M_n(K)$ ***spalten-stochastisch***, wenn die Summe der Einträge in jeder Spalte gleich 1 ist. (Analog kann man auch ***zeilen-stochastisch*** definieren.)

Beweis. Wir zeigen zuerst, dass $A - I_n \in M_n(K)$ nicht invertierbar ist. Annahme, doch! Dann gibt es $B \in M_n(K)$ mit $(A - I_n) \cdot B = B \cdot (A - I_n) = I_n$. Nun betrachte $v := [1 \ \ldots \ 1] \in K^{1 \times n}$. Wegen $\sum_{i=1}^{n} a_{ij} = 1$ für $1 \leqslant j \leqslant n$ folgt $v \cdot A = v$ und damit $0_{1 \times n} = v \cdot (A - I_n)$. Aber dann erhalten wir $0_{1 \times n} = 0_{1 \times n} \cdot B = \big(v \cdot (A - I_n)\big) \cdot B = v \cdot \big((A - I_n) \cdot B\big) = v \cdot I_n = v$, Widerspruch. Also war die Annahme falsch, d.h., $A - I_n$ ist nicht invertierbar. Nach Satz 13.3 gibt es daher ein $x \in K^n$ mit $x \neq 0_n$ und $(A - I_n) \cdot x = 0_n$, d.h., $A \cdot x = x$. □

Solche "stationären" Vektoren und stochastische Matrizen kommen in vielen Anwendungen vor; siehe zum Beispiel §3.4 im Buch von Huppert und Willems.

Ab hier Woche 9

Beispiel 13.8 (Gewichtung von Webseiten)**.** Tippt man einen Suchbegriff in Google (oder einer anderen Internet-Suchmaschine) ein, so wird nach allen Webseiten gesucht, die diesen Begriff enthalten: Dies können mehrere Millionen sein, meistens viel zu viele für eine sinnvolle Anzeige. Das Problem ist also: Wie kann man automatisch die gefundenen Seiten so sortieren, dass nach Möglichkeit zuerst die interessanteren auf dem Bildschirm erscheinen?

Die Idee zur Lösung dieses Problems ist, ein Maß $I(P)$ für die Wichtigkeit einer Webseite P einzuführen, so dass Webseiten, die auf den Suchbegriff passen, nach Wichtigkeit geordnet werden können. Das Ganze muss dabei sehr flexibel sein; es kommen ja ständig neue Webseiten und Links hinzu oder werden gelöscht. Außerdem sollen ein paar Prinzipien gelten, etwa: $I(P)$ steigt, je mehr andere (wichtige) Seiten auf P verweisen; oder: Verweist eine andere Webseite P' auf P, so ergibt sich ein Beitrag von $I(P')$ zu $I(P)$, der allerdings umso kleiner werden sollte, je mehr Verweise es überhaupt von P' auf andere Seiten gibt.

Modellierung. Seien $P_1, \dots, P_N$ die insgesamt verfügbaren Webseiten. Dann schreibe $P_j \to P_i$, wenn P_j einen Verweis auf P_i enthält; außerdem sei ℓ_j die Anzahl aller Verweise von P_j auf andere Webseiten. Dann verlangen wir folgende Regel für die Wichtigkeiten der Webseiten:

$$I(P_i) = \sum_{1 \leqslant j \leqslant N \,:\, P_j \to P_i} \frac{I(P_j)}{\ell_j}$$

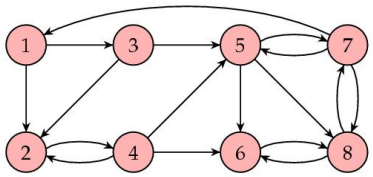
(Verweist also P_j auf P_i, so gibt P_j den ℓ_j-ten Bruchteil seiner eigenen Wichtigkeit an P_i weiter. Gibt es keinen Verweis auf P_i, so ist die Summe leer und $I(P_i) = 0$.)

Beachte: Dies ist keine Formel, um die Wichtigkeiten $I(P_i)$ einzeln zu berechnen, sondern ein Gleichungssystem, durch das sich die $I(P_i)$ gegenseitig bestimmen. Schauen wir uns dieses Gleichungssystem etwas genauer an.

Definiere dazu die "Internet–Matrix" $A = [a_{ij}]$ durch $\quad a_{ij} = \begin{cases} 1/\ell_j & \text{wenn } P_j \to P_i, \\ 0 & \text{sonst.} \end{cases}$

Ist $j \in \{1, \dots, N\}$ und $\ell_j > 0$, so gilt $\sum_{i=1}^{N} a_{ij} = \sum_{1 \leqslant i \leqslant N \,:\, P_j \to P_i} 1/\ell_j = 1$, d.h., außer wenn es eine Webseite P_j gibt, die gar keine Verweise auf andere Seiten enthält, ist A spaltenstochastisch. Es gilt $A \cdot \nu = \nu$ wobei $\nu \in \mathbb{Q}^N$ der Spaltenvektor mit den Komponenten $I(P_1), \dots, I(P_N)$ ist. Dieses ν ist also ein "stationärer" Vektor für A und wir können ν berechnen, indem wir das homogene LGS mit Matrix $A - I_N$ lösen.

Konkretes Beispiel: Unser Modell-Internet habe 8 Webseiten mit Verweisen wie folgt:



$$A = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1/3 & 0 \\ 1/2 & 0 & 1/2 & 1/3 & 0 & 0 & 0 & 0 \\ 1/2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1/2 & 1/3 & 0 & 0 & 1/3 & 0 \\ 0 & 0 & 0 & 1/3 & 1/3 & 0 & 0 & 1/2 \\ 0 & 0 & 0 & 0 & 1/3 & 0 & 0 & 1/2 \\ 0 & 0 & 0 & 0 & 1/3 & 1 & 1/3 & 0 \end{bmatrix} \quad \rightsquigarrow \quad \nu \approx \begin{bmatrix} 0.0600 \\ 0.0675 \\ 0.0300 \\ 0.0675 \\ 0.0975 \\ 0.2025 \\ 0.1800 \\ 0.2950 \end{bmatrix}$$

Also ist hier P_8 die wichtigste Seite! (Danach P_6, P_7, P_5, P_4, P_2, P_1, P_3) In diesem Fall gibt es (bis auf skalare Vielfache) nur einen stationären Vektor; ob so etwas immer gilt (bzw. wie man das erreichen kann) muss natürlich noch weiter untersucht werden. Für mehr dazu siehe

`http://www.ams.org/samplings/feature-column/fcarc-pagerank`

14. *Eigenwerte und das Minimalpolynom*

Sei K ein Körper und $A \in M_n(K)$. Wir betrachten die folgende leichte Verallgemeinerung des Begriffs des "stationären" Vektors (wie in Lemma 13.7 definiert). Ein Spaltenvektor $\nu \in K^n$

heißt ***Eigenvektor*** von A, wenn $v \neq 0_n$ gilt und es ein $\lambda \in K$ gibt mit $A \cdot v = \lambda v$; in diesem Fall heißt λ der zugehörige ***Eigenwert***. Ein stationärer Vektor ist dann also ein Eigenvektor zum Eigenwert $\lambda = 1$. — Die Theorie der Eigenwerte und Eigenvektoren ist der entscheidende Schlüssel für die Lösung von zahlreichen Problemen!

Bemerkung 14.1. Sei $A \in M_n(K)$ und $\lambda \in K$.
Für $v \in K^n$ gilt dann $A \cdot v = \lambda v \Leftrightarrow (A - \lambda I_n) \cdot v = A \cdot v - \lambda v = 0_n$. Also:

$$v \text{ Eigenvektor} \quad \Leftrightarrow \quad v \neq 0_n \text{ und } A \cdot v = \lambda v \quad \Leftrightarrow \quad v \neq 0_n \text{ und } (A - \lambda I_n) \cdot v = 0_n.$$

Insbesondere: Wenn man weiss, dass λ ein Eigenwert ist, so kann man die zugehörigen Eigenvektoren leicht bestimmen als Lösungen des homogenen LGS mit Matrix $A - \lambda I_n$.
Außerdem folgt mit Satz 13.3: λ Eigenwert $\Leftrightarrow$ $A - \lambda I_n$ nicht invertierbar.

Beispiel 14.2. (a) Sei $A = \begin{bmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_n \end{bmatrix} \in M_n(K)$ eine Diagonalmatrix mit Einträgen $a_1, \ldots, a_n \in K$ auf der Diagonalen. Ist $e_i \in K^n$ der Standard-Spaltenvektor wie in Beispiel 11.7 (also 1 an der i-ten Position und 0 sonst), so gilt $A \cdot e_i = a_i e_i$, d.h., e_i ist ein Eigenvektor mit Eigenwert a_i. Umgekehrt: Ist $\lambda \in K$ ein Eigenwert, so ist $A - \lambda I_n$ nicht invertierbar, also muss einer der Diagonaleinträge von $A - \lambda I_n$ gleich 0 sein, d.h., $\lambda = a_i$ für ein i. Die Eigenwerte von A sind also $a_1, \ldots, a_n$.

(b) Sei $A = \begin{bmatrix} a_1 & & * \\ & \ddots & \\ 0 & & a_n \end{bmatrix} \in M_n(K)$ eine obere Dreiecksmatrix mit Einträgen $a_1, \ldots, a_n \in K$ auf der Diagonalen. Dann kann man auch zeigen, dass $a_1, \ldots, a_n$ die Eigenwerte von A sind. (Wende Gauß–Elimination auf $A - \lambda I_n$ an und prüfe, wann $A - \lambda I_n$ invertierbar ist.)

(c) Sei $A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \in M_2(K)$, wobei $K \subseteq \mathbb{R}$. Sei $v = \begin{bmatrix} a \\ b \end{bmatrix} \in K^2$ und $\lambda \in K$. Ansatz:

$$\begin{bmatrix} \lambda a \\ \lambda b \end{bmatrix} = \lambda v = A \cdot v = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} b \\ a + b \end{bmatrix}.$$

Wir suchen also Lösungen für die Gleichungen $\lambda a = b$ und $\lambda b = a + b$, wobei $a \neq 0$ oder $b \neq 0$. Einsetzen der 1. Gleichung in die 2. Gleichung ergibt $a + \lambda a = \lambda b = \lambda^2 a$, also $(\lambda^2 - \lambda - 1)a = 0$. Ist $a = 0$, so auch $b = \lambda a = 0$, also erhalten wir keine Lösung. Sei nun $a \neq 0$. Dann muss $\lambda^2 - \lambda - 1 = 0$ gelten. Ist $K = \mathbb{R}$, so gibt es zwei Lösungen $\lambda_{1,2} = \frac{1}{2}(1 \pm \sqrt{5})$. Ist $K = \mathbb{Q}$, so gibt es keine Lösung. Das Problem hängt also auch vom Körper ab.

Im Allgemeinen sind die Eigenwerte und Eigenvektoren von $A = [a_{ij}] \in M_n(K)$ durch die folgenden Gleichungen bestimmt: $\sum_{j=1}^{n} a_{ij} v_j = \lambda v_i$ für $1 \leqslant i \leqslant n$, mit Unbekannten $\lambda, v_1, \ldots, v_n \in K$. Beachte, dass dies kein LGS mehr ist: Auf der rechten Seite kommen die Produkte λv_i vor! Wie können wir also systematisch vorgehen? Um das Problem mit dem

nicht-linearen Gleichungssystem zu umgehen, bringen wir die "abstrakten" Polynome aus §9 ins Spiel und verwenden nun, dass wir auch Matrizen in diese Polynome einsetzen können.

Definition 14.3. Sei $A \in M_n(K)$ und $f = a_d X^d + a_{d-1}X^{d-1} + \ldots + a_1 X + a_0 \in K[X]$ beliebig. Dann definiere

$$f(A) := a_d A^d + a_{d-1}A^{d-1} + \ldots + a_1 A + a_0 I_n \in M_n(K).$$

Ist zum Beispiel $f = 2X^3 - X + 5 \in \mathbb{Q}[X]$ und $A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$, so erhalten wir

$$f(A) = 2\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}^3 - \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} + 5\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \ldots = \begin{bmatrix} 7 & 3 \\ 3 & 10 \end{bmatrix}.$$

Wie in Bemerkung 9.9 sieht man mit einer leichten Rechnung, dass folgende Regeln gelten:

$$(f+g)(A) = f(A) + g(A) \quad \text{und} \quad (f * g)(A) = f(A) \cdot g(A) \qquad \text{für alle } f, g \in K[X].$$

Hier ist eine erste Verbindung zwischen Eigenwerten und Nullstellen von Polynomen.

Lemma 14.4. *Sei $A \in M_n(K)$ und $\lambda \in K$ ein Eigenwert von A. Dann gilt:*

(a) *Für jedes $i \in \mathbb{N}$ ist λ^i ein Eigenwert von A^i.*

(b) *Ist $f \in K[X]$ beliebig mit $f(A) = 0_{n\times n}$, so gilt auch $f(\lambda) = 0$.*

(c) *Es gibt ein Polynom $f \in K[X]$ mit $f \neq \underline{0}$ und $f(A) = 0_{n\times n}$.*

Beweis. Sei $v \in K^n$ ein Eigenvektor zu λ, also $v \neq 0_n$ und $A \cdot v = \lambda v$.

(a) Es gilt $A^2 \cdot v = A \cdot (A \cdot v) = A \cdot (\lambda v) = \lambda(A \cdot v) = \lambda(\lambda v) = \lambda^2 v$ (wobei wir Bemerkung 11.5(c) benutzt haben). Genauso erhält man $A^3 \cdot v = \lambda^3 v$. Mit einer Induktion nach i folgt allgemein $A^i \cdot v = \lambda^i v$ für alle $i \in \mathbb{N}$. Also ist v auch ein Eigenvektor von A^i, zum Eigenwert λ^i.

(b) Sei $f = a_0 + a_1 X + a_2 X^2 + \ldots + a_d X^d \in K[X]$ mit $f(A) = 0_{n\times n}$. Dann folgt $0_n = f(A) \cdot v = (a_0 I_n + a_1 A + a_2 A^2 + \ldots + a_d A^d) \cdot v = a_0 v + a_1(A \cdot v) + a_2(A^2 \cdot v) + \ldots + a_d(A^d \cdot v)$. Mit der obigen Rechnung zum Beweis von (a) folgt $0_n = a_0 v + a_1 \lambda v + a_2 \lambda^2 v + \ldots + a_d \lambda^d v = (a_0 + a_1\lambda + a_2\lambda^2 + \ldots + a_d\lambda^d)v = f(\lambda)v$. Wegen $v \neq 0_n$ muss dann $f(\lambda) = 0$ gelten.

(c) Betrachte die $N := n^2 + 1$ Matrizen $I_n, A, A^2, \ldots, A^{n^2} \in M_n(K)$. Nach Beispiel 13.2 gibt es $c_0, c_1, \ldots, c_{n^2} \in K$, die nicht alle gleich 0 sind, mit $c_0 I_n + c_1 A + c_2 A^2 + \ldots + c_{n^2} A^{n^2} = 0_{n\times n}$. Setzen wir also $f := c_0 + c_1 X + c_2 X^2 + \ldots + c_{n^2} X^{n^2} \in K[X]$, so ist $f \neq \underline{0}$ und $f(A) = 0_{n\times n}$. □

Satz 14.5. *Sei $A \in M_n(K)$. Dann gibt es ein eindeutiges normiertes Polynom $\underline{0} \neq f_0 \in K[X]$ kleinsten Grades mit $f_0(A) = 0_{n\times n}$. Dieses Polynom wird auch mit $\mu_A = f_0$ bezeichnet und heißt **Minimalpolynom** von A.*

Beweis. Sei $A := \{d \in \mathbb{N} \mid \exists\, \underline{0} \neq f \in K[X] : \text{Grad}(f) = d \text{ und } f(A) = 0_{n\times n}\}$. Nach Lemma 14.4(c) ist $A \neq \varnothing$, also gibt es ein kleinstes Element, sei dieses d_0. Sei $\underline{0} \neq f_0 \in A$ mit $\text{Grad}(f_0) = d_0$; dann ist $f_0(A) = 0_{n\times n}$. Indem wir f_0 mit dem Inversen des Leitkoeffizienten multiplizieren, können wir erreichen, dass f_0 normiert ist. Sei nun auch $\underline{0} \neq g_0 \in K[X]$

normiert mit $\mathrm{Grad}(g_0) = d_0$ und $g_0(A) = 0_{n\times n}$. Annahme, es wäre $f_0 \neq g_0$. Dann ist $h := f_0 - g_0 \neq \underline{0}$ und $\mathrm{Grad}(h) < d_0$ (denn die höchsten Terme X^{d_0} heben sich in $f_0 - g_0$ weg). Aber nach den obigen Regeln ist $h(A) = (f_0 - g_0)(A) = f_0(A) - g_0(A) = 0_{n\times n}$, Widerspruch zur Minimalität von d_0. □

Um μ_A konkret zu bestimmen, berechnet man so lange Potenzen $A, A^2, A^3, \ldots$ bis man ein $d \geqslant 1$ findet, so dass es $c_0, c_1, \ldots, c_{d-1} \in K$ gibt mit $A^d = c_0 I_n + c_1 A + c_2 A^2 + \ldots + c_{d-1} A^{d-1}$. Dann ist $\mu_A = X^d - c_{d-1}X^{d-1} - \ldots - c_1 X - c_0 \in K[X]$ das Minimalpolynom.

Beispiel 14.6. (a) Sei $A = cI_n \in M_n(K)$ mit $c \in K$. Dann ist $\mu_A = X - c$. Insbesondere erhalten wir $\mu_{0_{n\times n}} = X$ (für $c = 0$) und $\mu_{I_n} = X - 1$ (für $c = 1$).

(b) Sei $A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \in M_2(K)$. Weil A kein Vielfaches von I_2 ist, berechnen wir A^2 und prüfen, ob es $c_0, c_1 \in K$ gibt mit $A^2 = c_0 I_2 + c_1 A$:

$$\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} = A^2 = c_0 I_2 + c_1 A = \begin{bmatrix} c_0 & c_1 \\ c_1 & c_0 + c_1 \end{bmatrix}.$$

Hier sehen wir sofort die eindeutige Lösung $c_0 = c_1 = 1$. Also ist $\mu_A = X^2 - X - 1$.
Bestimmen Sie als Übung das Minimalpolynom einer beliebigen 2×2-Matrix.

(c) Sei $A = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \in M_3(\mathbb{Q})$. Weil A kein Vielfaches von I_3 ist, berechnen wir A^2 und prüfen, ob es $c_0, c_1 \in K$ gibt mit $A^2 = c_0 I_3 + c_1 A$:

$$\begin{bmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{bmatrix} = A^2 = c_0 I_3 + c_1 A = \begin{bmatrix} c_0 + c_1 & c_1 & 0 \\ c_1 & c_0 & c_1 \\ 0 & c_1 & c_0 + c_1 \end{bmatrix}.$$

Wir erhalten ein LGS für c_0, c_1. Beim Betrachten des $(1,3)$-Eintrags der obigen Matrizen sehen wir sofort, dass es keine Lösung gibt. Also müssen wir fortfahren, A^3 berechnen und prüfen, ob es $c_0, c_1, c_2 \in K$ gibt mit $A^3 = c_0 I_3 + c_1 A + c_2 A^2$. Wir erhalten folgendes LGS:

$$\begin{bmatrix} 3 & 3 & 2 \\ 3 & 2 & 3 \\ 2 & 3 & 3 \end{bmatrix} = A^3 = c_0 I_3 + c_1 A + c_2 A^2 = \begin{bmatrix} c_0 + c_1 + 2c_2 & c_1 + c_2 & c_2 \\ c_1 + c_2 & c_0 + 2c_2 & c_1 + c_2 \\ c_2 & c_1 + c_2 & c_0 + c_1 + 2c_2 \end{bmatrix}.$$

Mit dem Gauß–Verfahren finden wir die eindeutige Lösung $c_0 = -2$, $c_1 = 1$ und $c_2 = 2$. Also ist $\mu_A(x) = X^3 - 2X^2 - X + 2 = (X - 2)(X - 1)(X + 1)$.

Obiges Verfahren lässt sich auf dem Computer implementieren, sobald die Gauß–Elimination und das Lösen von LGSen programmiert sind. In GAP gibt es zum Beispiel die Funktion **`MinimalPolynomial`**.

Wenn Sie mehr dazu lesen möchten, wie man dies möglichst e zient organisiert, so siehe den Fachartikel

M. NEUNHÖFFER AND C. E. PRAEGER, Computing minimal polynomials of matrices,

LMS J. Comput. Math. 11 (2008), 252–279; **`https://doi.org/10.1112/S1461157000000590`**.

Satz 14.7. *Sei* $A \in M_n(K)$ *und* $\lambda \in K$. *Genau dann ist* λ *ein Eigenwert von* A, *wenn* $\mu_A(\lambda) = 0$ *gilt, also* λ *eine Nullstelle des Minimalpolynoms von* A *ist.*

Beweis. Sei zuerst λ ein Eigenwert von A. Wegen $\mu_A(A) = 0_{n\times n}$ ist dann auch $\mu_A(\lambda) = 0$; siehe Lemma 14.4(b). Sei nun umgekehrt $\mu_A(\lambda) = 0$. Nach Bemerkung 9.10 gilt dann $\mu_A = (X-\lambda) * g$ mit $\underline{0} \neq g \in K[X]$ und $\mathrm{Grad}(g) = \mathrm{Grad}(\mu_A) - 1$. Einsetzen von A und beachten der obigen Regeln ergibt $0_{n\times n} = \mu_A(A) = \big((X-\lambda)*g\big)(A) = (A-\lambda I_n)\cdot g(A)$. Nun ist $g \neq \underline{0}$ und $\mathrm{Grad}(g) < \mathrm{Grad}(\mu_A)$, also $B := g(A) \neq 0_{n\times n}$ nach Definition von μ_A. Sei $j \in \{1,\dots,n\}$ so, dass die j-te Spalte von B einen Eintrag $\neq 0$ enthält. Bezeichnen wir diese j-te Spalte mit $v \in K^n$, so gilt also $v = B\cdot e_j \neq 0_n$ (siehe Beispiel 11.7). Aus $(A-\lambda I_n)\cdot B = 0_{n\times n}$ folgt nun $(A-\lambda I_n)\cdot v = (A-\lambda I_n)\cdot(B\cdot e_j) = \big((A-\lambda I_n)\cdot B\big)\cdot e_j = 0_{n\times n}\cdot e_j = 0_n$ und damit $A\cdot v = \lambda v$. Also ist λ ein Eigenwert von A mit Eigenvektor v, wie gewünscht. □

Damit ist die Bestimmung der Eigenwerte einer Matrix $A \in M_n(K)$ zurückgeführt auf

(1) die Bestimmung des Minimalpolynoms μ_A und

(2) die Bestimmung der Nullstellen von μ_A.

Für (1) werden Potenzen von A berechnet und LGSe gelöst; für (2) gibt es je nach K verschiedene Verfahren (z.B. Näherungsverfahren für $K = \mathbb{R}$; endliches Probieren für $|K| < \infty$). Im Allgemeinen ist das Finden von Nullstellen von Polynomen, und damit die Bestimmung von Eigenwerten einer Matrix, ein schwieriges Problem.

Wir können noch eine leichte Verschärfung von Satz 14.5 zeigen. Dazu benötigen wir die folgenden Konstruktionen mit Polynomen, die sich auch sonst als nützlich erweisen.
Seien $f, g \in K[X]$. Wie für ganze Zahlen schreiben wir $f \mid g$ (und sagen "f teilt g"), wenn es ein $h \in K[X]$ gibt mit $g = f * h$. Es gelten dann analoge Regeln wie in §2.

Lemma 14.8 (***Teilen mit Rest für Polynome***, vgl. Satz 2.7)**.** *Seien* $f, g \in K[X]$ *gegeben mit* $g \neq \underline{0}$. *Dann gibt es* $h, r \in K[X]$ *mit* $f = g * h + r$, *wobei entweder* $r = \underline{0}$, *oder* $r \neq \underline{0}$ *und* $\mathrm{Grad}(r) < \mathrm{Grad}(g)$ *gilt. Hier sind* h, r *eindeutig bestimmt.*

Beweis. Wir beschreiben ein Verfahren zur Bestimmung von h und r. Sei $m := \mathrm{Grad}(g) \geqslant 0$ und $0 \neq b_m \in K$ der Leitkoeffizient von g. Zuerst einige triviale Fälle. Für $f = \underline{0}$ ist $f = g*\underline{0}+\underline{0}$ und die Aussage gilt mit $h := \underline{0}$ und $r := \underline{0}$. Sei nun $f \neq \underline{0}$ und $n := \mathrm{Grad}(f) \geqslant 0$. Ist $n < m$, so ist $f = g\cdot\underline{0} + f$ und die Aussage gilt mit $h := \underline{0}$ und $r := f$.

Sei nun $n \geqslant m$. Dann setze $f' := f - a_n b_m^{-1} X^{n-m} * g \in K[X]$, wobei $0 \neq a_n \in K$ der Leitkoeffizient von f ist. Ist $f' = \underline{0}$, so gilt die Aussage mit $h := a_n b_m^{-1} X^{n-m}$ und $r := \underline{0}$. Ist $f' \neq \underline{0}$, so erhalten wir

$$f' = f - a_n b_m^{-1} X^{n-m} * g = \big(a_n X^n + \ldots + a_1 X + a_0\big) - a_n b_m^{-1} X^{n-m}\big(b_m X^m + \ldots + b_1 X + b_0\big)$$
$$= \big(a_n X^n + a_{n-1} X^{n-1} + \ldots + a_0\big) - \big(a_n X^n + a_n b_m^{-1} b_{m-1} X^{n-1} + \ldots + a_n b_m^{-1} b_0 X^{n-m}\big),$$

wobei der Term $a_n X^n$ wegfällt. Also folgt $\mathrm{Grad}(f') < n$. Nehmen wir an, wir haben nun schon eine Darstellung der gewünschten Form für f', also $f' = g * h' + r$ mit $h', r \in K[X]$, wobei $r = \underline{0}$, oder $r \neq \underline{0}$ und $\mathrm{Grad}(r) < m$. Dann folgt

$$f = f' + a_n b_m^{-1} X^{n-m} * g = g * (h' + a_n b_m^{-1} X^{n-m}) + r,$$

also gilt die Aussage auch für f mit $h := h' + a_n b_m^{-1} X^{n-m}$ und r.

Eindeutigkeit: Ist auch $f = g * h' + r'$ (wobei h', r' analoge Bedingungen wie h, r erfüllen), so gilt $g * (h - h') = r' - r$. Wäre $r' \neq r$, dann $g \mid r' - r$, was wegen $\mathrm{Grad}(r' - r) < \mathrm{Grad}(g)$ unmöglich ist. Also gilt $r = r'$. Dann ist aber $g * (h - h') = \underline{0}$. Wäre $h \neq h'$, so $h - h' \neq \underline{0}$ und dann $g * (h - h') \neq \underline{0}$ (siehe Lemma 9.5(c)), Widerspruch. □

Bei größeren Beispielen ist es sinnvoll, die erforderlichen Rechnungen in einem Schema wie folgt zu arrangieren. Sei etwa $f = X^6 + X + 1$ und $g = X^2 - X + 2$:

$$\begin{array}{rl}
X^6 + X + 1 & = (X^2 - X + 2) * \underbrace{(X^4 + X^3 - X^2 - 3X - 1)}_{=h} + \underbrace{(6X + 3)}_{=r} \\
\underline{-(X^6 - X^5 + 2X^4)} & \\
X^5 - 2X^4 + X + 1 & \\
\underline{-(X^5 - X^4 + 2X^3)} & \\
-X^4 - 2X^3 + X + 1 & \\
\underline{-(-X^4 + X^3 - 2X^2)} & \\
-3X^3 + 2X^2 + X + 1 & \\
\underline{-(-3X^3 + 3X^2 - 6X)} & \\
-X^2 + 7X + 1 & \\
\underline{-(-X^2 + X - 2)} & \\
6X + 3 &
\end{array}$$

Bemerkung 14.9. Sobald "Teilen mit Rest" für Polynome definiert ist, gibt es auch einen erweiterten ***Euklidischen Algorithmus*** (so wie im Lemma von Bézout). Sind $f, g \in K[X]$ gegeben mit $f \neq \underline{0}$ oder $g \neq \underline{0}$, so liefert dieser Algorithmus Polynome $d, r, s \in K[X]$ mit:

$$d \neq \underline{0} \text{ ist ein gemeinsamer Teiler von } f, g \text{ und es gilt } d = r * f + s * g.$$

Beachte: Ist auch $0 \neq d' \in K[X]$ ein gemeinsamer Teiler von f und g, so folgt $d' \mid (r*f+s*g) = d$, insbesondere $\mathrm{Grad}(d') \leqslant \mathrm{Grad}(d)$. Also ist d ein Grad-mäßig ***größter gemeinsamer Teiler*** von f und g. Verlangt man, dass d normiert ist, so sieht man leicht, dass d eindeutig bestimmt ist und wird wieder mit $d = \mathrm{ggT}(f, g)$ bezeichnet.
Teilen mit Rest für Polynome läßt sich leicht programmieren — versuchen Sie es selbst! Für obiges Beispiel erhält man mit GAP:

```
gap> t:=Indeterminate(Rationals,"t");;
gap> f:=t^6+t+1;; g:=t^2-t+2;;
```

```
gap> d:=Gcd(f,g);                          # Gcd = ggT
1
gap> GcdRepresentation(f,g);               # Koeffs r,s mit d=r*f+s*g
[ -2/33*t+1/11, 2/33*t^5-1/33*t^4-5/33*t^3-1/11*t^2+7/33*t+5/11 ]
gap> last[1]*f+last[2]*g;                  # Probe
1
```

Folgerung 14.10. *Sei* $A \in M_n(K)$ *und* $f \in K[X]$ *beliebig mit* $f(A) = 0_{n\times n}$. *Dann gilt* $\mu_A \mid f$.

Beweis. Teilen mit Rest ergibt $f = \mu_A * h + r$ wobei $h, r \in K[X]$ mit $r = \underline{0}$, oder $r \neq \underline{0}$ und $\mathrm{Grad}(r) < \mathrm{Grad}(\mu_A)$. Angenommen, es wäre $r \neq \underline{0}$. Einsetzen von A und beachten der obigen Regeln ergibt $0_{n\times n} = f(A) = (\mu_A * h + r)(A) = \mu(A) \cdot h(A) + r(A) = 0_{n\times n} \cdot h(A) = r(A)$, Widerspruch zu $\mathrm{Grad}(r) < \mathrm{Grad}(\mu_A)$. Also ist $r = \underline{0}$ und damit $\mu_A \mid f$. □

Ab hier Woche 10

15. *Ausblick: Determinanten*

Determinanten von Matrizen sind in einer einführenden Vorlesung zur Matrix-Theorie (oder zur Linearen Algebra) meist ein etwas kniffliges Thema. Dies liegt einerseits daran, dass die Definition von $\det(A)$ "vom Himmel zu fallen scheint". (Es wird erst im Laufe der Zeit klarer, warum die etwas künstlich aussehende Definition die einzig mögliche ist, damit $\det(A)$ bestimmte Eigenschaften hat.) Andererseits ist es auch so, dass Beweise zu Aussagen über Determinanten meist technisch anspruchsvoller sind als das, was man bis dahin gesehen hat. Wir geben hier eine erste Einführung; Fortsetzung folgt im 2. Semester.

Vermutlich ist die Formel für 2×2-Matrizen bekannt: $\det\left(\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}\right) = a_{11}a_{22} - a_{12}a_{21}$.

Vielleicht haben Sie auch die ***Regel von Sarrus*** für 3×3-Matrizen schon einmal gesehen:

$$\det\left(\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}\right) = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33}.$$

Versuchen wir, ein allgemeines Muster in der obigen Formel zu finden. Die Terme, die aufsummiert werden, haben alle die Form $\pm a_{1i_1}a_{2i_2}a_{3i_3}$ wobei i_1, i_2, i_3 eine Umordnung der Ziffern $1, 2, 3$ ist. Eine solche Umordung ist nichts Anderes als eine bijektive Abbildung $\sigma\colon \{1,2,3\} \to \{1,2,3\}$, wobei $i_1 = \sigma(1)$, $i_2 = \sigma(2)$, $i_3 = \sigma(3)$. Nach Lemma 5.16 gibt es genau $3! = 6$ solche bijektiven Abbildungen; das passt also genau zu den obigen 6 Summanden.

Für $n \in \mathbb{N}$ beliebig definieren wir nun S_n als die Menge aller bijektiven Abbildungen $\sigma\colon \{1,\dots,n\} \to \{1,\dots,n\}$. Die Elemente von S_n heißen auch ***Permutationen***. Nach Lemma 5.16 ist S_n eine endliche Menge mit $|S_n| = n!$. Der erste Ansatz für eine allgemeine Definition von $\det(A)$ wäre dann

$$\det(A) = \sum_{\sigma\in S_n} \pm a_{1\sigma(1)}\, a_{2\sigma(2)} \cdots a_{n\sigma(n)} \qquad \text{wobei} \qquad A = [a_{ij}]_{1\leqslant i,j\leqslant n}.$$

Es ist nun nicht ganz leicht, die "richtige" allgemeine Formel für die Vorzeichen zu raten. Dazu: Sei $n \in \mathbb{N}$ und $\sigma \in S_n$. Sei $N(\sigma)$ die Menge aller Indexpaare (i,j) mit $1 \leqslant i < j \leqslant n$ aber $\sigma(i) > \sigma(j)$ gilt; diese Indexpaare heißen ***Fehlstände*** von σ. Dann wird das ***Signum*** von σ definiert als

$$\operatorname{sgn}(\sigma) := \begin{cases} +1 & \text{falls } |N(\sigma)| \text{ gerade ist,} \\ -1 & \text{falls } |N(\sigma)| \text{ ungerade ist.} \end{cases}$$

Überzeugen Sie sich davon, dass das so definierte Signum genau die obigen Vorzeichen in den Formeln für 2×2- und 3×3-Matrizen ergibt.

Beispiel 15.1. (a) Ist $\mathrm{id} \in S_n$ die identische Abbildung (also $\mathrm{id}(i) = i$ für $i = 1,\dots,n$), so gibt es offenbar keine Fehlstände, also gilt $N(\mathrm{id}) = \varnothing$ und $\operatorname{sgn}(\mathrm{id}) = 1$.
(b) Seien $k,l \in \{1,\dots,n\}$ fest mit $k < l$. Dann definieren wir $\tau_{kl} \in S_n$ durch $\tau_{kl}(k) := l$, $\tau_{kl}(l) := k$ und $\tau_{kl}(i) := i$ für alle $i \neq k,l$. Also vertauscht τ_{kl} die beiden Ziffern k und l, und lässt alle anderen Ziffern fest. Eine solche Permutation heißt auch ***Transposition***. Es gilt $\tau_{ij} \circ \tau_{ij} = \mathrm{id}$, also $\tau_{ij}^{-1} = \tau_{ij}$. Wie man leicht sieht, gilt:

$$N(\tau_{kl}) = \big\{(k,l),\ (k+1,l),\ \dots,\ (l-1,l),\ (k,k+1),\ (k,k+2),\ \dots,\ (k,l-1)\big\}.$$

Dann ist $|N(\tau_{kl})| = 2(l-k)-1$ ungerade, also $\operatorname{sgn}(\tau_{kl}) = -1$.

(c) Es gilt $\operatorname{sgn}(\sigma) = \operatorname{sgn}(\sigma^{-1})$ für alle $\sigma \in S_n$. Dazu: Ist $(i,j) \in N(\sigma)$, so setze $i' := \sigma(i)$ und $j' := \sigma(j)$; dann ist $(j',i') \in N(\sigma^{-1})$, denn $j' < i'$ aber $\sigma^{-1}(j') = j > i = \sigma^{-1}(i')$. Also erhalten wir eine Abbildung $f\colon N(\sigma) \to N(\sigma^{-1})$, $(i,j) \mapsto \big(\sigma(j),\sigma(i)\big)$. Analog erhalten wir $g\colon N(\sigma^{-1}) \to N(\sigma)$, $(i,j) \mapsto \big(\sigma^{-1}(j),\sigma^{-1}(i)\big)$. Nun ist $f\circ g = \mathrm{id}_{N(\sigma^{-1})}$ und $g\circ f = \mathrm{id}_{N(\sigma)}$. Also sind f,g bijektiv und damit $|N(\sigma)| = |N(\sigma^{-1})|$, also auch $\operatorname{sgn}(\sigma) = \operatorname{sgn}(\sigma^{-1})$.

Definition 15.2 (***Leibniz–Formel***)**.** Sei R ein kommutativer Ring mit 1. Dann ist die ***Determinante*** einer Matrix $A = [a_{ij}]_{1\leqslant i,j\leqslant n} \in M_n(R)$ definiert als

$$\det(A) = \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma)\, a_{1\sigma(1)}\, a_{2\sigma(2)} \cdots a_{n\sigma(n)} \in R.$$

Beachte, dass diese Formel für große Werte von n praktisch völlig unbrauchbar ist. Immerhin kann man die Formel aber für Matrizen mit bestimmten Eigenschaften auswerten. Beispiele:

Lemma 15.3. *Sei $A = [a_{ij}]_{1\leqslant i,j\leqslant n} \in M_n(R)$ so, dass alle Einträge in einer Zeile gleich 0 sind. Dann ist $\det(A) = 0$.*

Beweis. Sei $k \in \{1,\dots,n\}$ so, dass $a_{kj} = 0$ für alle j gilt. Ist $\sigma \in S_n$, so ist also $a_{k\sigma(k)} = 0$ und damit der entsprechende Term $\operatorname{sgn}(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)}$ in der Formel für $\det(A)$ ebenfalls gleich 0. Also ist insgesamt $\det(A) = 0$. □

Lemma 15.4. *Sei* $A = [a_{ij}]_{1\leqslant i,j\leqslant n} \in M_n(R)$ *eine obere Dreiecksmatrix, d.h.,* $a_{ij} = 0$ *für* $1 \leqslant j < i \leqslant n$. *Dann gilt* $\det(A) = a_{11}a_{22}\cdots a_{nn}$. *Eine analoge Aussage gilt auch für untere Dreiecksmatrizen. Inbesondere ist* $\det(I_n) = 1$.

Beweis. Sei $\sigma \in S_n$ so, dass der entsprechende Term $\operatorname{sgn}(\sigma)a_{1\sigma(1)}a_{2\sigma(2)}\cdots a_{n\sigma(n)}$ in der Formel für $\det(A)$ ungleich 0 ist. Dann ist $a_{k\sigma(k)} \neq 0$ für alle k, also $\sigma(k) \geqslant k$, d.h.,

$$\sigma(n) \geqslant n, \qquad \sigma(n-1) \geqslant n-1, \qquad \ldots, \qquad \sigma(1) \geqslant 1.$$

Aus der ersten Bedingung folgt $\sigma(n) = n$, dann aus der zweiten $\sigma(n-1) = n-1$ und so weiter bis $\sigma(1) = 1$. Damit liefert nur der Term für $\sigma = \mathrm{id}$ einen Beitrag ungleich 0 zu $\det(A)$, also gilt die genannte Formel. Angewandt auf $A = I_n$ erhalten wir $\det(I_n) = 1$. Der Beweis für untere Dreiecksmatrizen ist völlig analog. □

Für $\tau \in S_n$ definieren wir eine Matrix

$$A^\tau = (a^\tau_{ij})_{1\leqslant i,j\leqslant n} \in M_n(R) \qquad \text{wobei} \qquad a^\tau_{ij} := \begin{cases} 1 & \text{falls } i = \tau(j), \\ 0 & \text{sonst.} \end{cases}$$

Die Matrix A^τ heißt die zu τ gehörige ***Permutationsmatrix***. Einige Beispiele für $n = 3$:

$$A^{(2,1,3)} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \qquad A^{(3,1,2)} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \qquad A^{(3,2,1)} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}.$$

(Hier wird jeweils τ einfach durch die Liste $(\tau(1), \tau(2), \tau(3))$ bezeichnet; wir erhalten A^τ durch Permutieren der Zeilen der Einheitsmatrix gemäß τ.) Es gilt $A^\tau \cdot e_i = e_{\tau(i)}$ für $1 \leqslant i \leqslant n$.

Lemma 15.5. *Es gilt* $\det(A^\tau) = \operatorname{sgn}(\tau^{-1}) = \operatorname{sgn}(\tau)$ *für alle* $\tau \in S_n$.

Beweis. Sei $\sigma \in S_n$ so, dass der entsprechende Term $\operatorname{sgn}(\sigma)a^\tau_{1\sigma(1)}a^\tau_{2\sigma(2)}\cdots a^\tau_{n\sigma(n)}$ in der Formel für $\det(A^\tau)$ ungleich 0 ist. Dann folgt aus der Definition von A^τ, dass $i = \tau(\sigma(i))$ für alle i gelten muss. Also ist $\tau \circ \sigma = \mathrm{id}$ und damit $\sigma = \tau^{-1}$. Die Summe in der Definition von $\det(A^\tau)$ hat also nur einen Term und es gilt $\det(A^\tau) = \operatorname{sgn}(\tau^{-1})a^\tau_{1\tau^{-1}(1)}a^\tau_{2\tau^{-1}(2)}\cdots a^\tau_{n\tau^{-1}(n)} = \operatorname{sgn}(\tau^{-1}) = \operatorname{sgn}(\tau)$; die letzte Gleichheit gilt nach Beispiel 15.1(c). □

Satz 15.6 (Zeilen/Spalten-Symmetrie)**.** *Es gilt* $\det(A) = \det(A^{\mathrm{tr}})$ *für alle* $A \in M_n(R)$.

Beweis. Sei $A = [a_{ij}]_{1\leqslant i,j\leqslant n}$; dann ist $A^{\mathrm{tr}} = [a_{ji}]_{1\leqslant i,j\leqslant n}$, also gilt

$$\det(A^{\mathrm{tr}}) = \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma)a_{\sigma(1)1}a_{\sigma(2)2}\cdots a_{\sigma(n)n} = \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma)\prod_{k=1}^{n} a_{\sigma(k)k}.$$

Sei $\sigma \in S_n$ fest und setze $l := \sigma(k)$ für $1 \leqslant k \leqslant n$. Mit k durchläuft auch l alle Ziffern von 1 bis n, nur in einer anderen Reihenfolge. Mit $k := \sigma^{-1}(l)$ erhalten wir also

$$\prod_{k=1}^{n} a_{\sigma(k)k} = \prod_{l=1}^{n} a_{l\sigma^{-1}(l)}$$

und damit $\det(A^{tr}) = \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) a_{1\sigma^{-1}(1)} a_{2\sigma^{-1}(2)} \cdots a_{n\sigma^{-1}(n)}$.

Schließlich sieht man sofort, dass die Abbildung $S_n \to S_n$, $\sigma \mapsto \sigma^{-1}$, bijektiv ist. Also können wir in der letzteren Formel für $\det(A^{tr})$ auch überall σ^{-1} durch σ ersetzen. Wegen $\operatorname{sgn}(\sigma^{-1}) = \operatorname{sgn}(\sigma)$ (siehe Beispiel 15.1(c)) folgt dann $\det(A^{tr}) = \det(A)$. □

Ohne Beweis geben wir noch den folgenden Satz an und diskutieren anschließend einige Anwendungen. (Der Beweis wird im 2. Semester nachgeholt.)

Satz 15.7 (Produktregel)**.** *Es gilt* $\det(A \cdot B) = \det(A)\det(B)$ *für alle* $A, B \in M_n(R)$.

Bemerkung 15.8. Sei K ein Körper und $A \in M_n(K)$.
(a) Ist A invertierbar, so sei $A^{-1} \in M_n(K)$ die inverse Matrix. Mit der Produktregel und Lemma 15.4 erhalten wir $1 = \det(I_n) = \det(A)\det(A^{-1})$. Damit folgt $\det(A) \neq 0$ und $\det(A^{-1}) = \det(A)^{-1}$. Die Determinante einer invertierbaren Matrix ist also stets ungleich 0.

(b) Betrachten wir nun die $n \times n$-Elementarmatrizen $M_i(c)$, $I_{ij}(c)$, V_{ij} (definiert am Ende von §12). Hier sind $M_i(c)$ und $I_{ij}(c)$ Dreiecksmatrizen; V_{ij} ist die Permutationsmatrix zur Transposition τ_{ij}. Also folgt mit Lemma 15.4 und Lemma 15.5:

$$\det(M_i(c)) = c, \qquad \det(I_{ij}(c)) = 1, \qquad \det(V_{ij}) = -1.$$

Sei nun $A \in M_n(K)$ beliebig; dann gibt es ein $Q \in GL_n(K)$ so dass $Q \cdot A = A'$ Stufenform hat; sei $r \in \{0, 1, \ldots, n\}$ die Anzahl der Stufen. Dann ist $A = Q^{-1} \cdot A'$, also folgt mit (a) und der Produktregel $\det(A) = \det(Q)^{-1}\det(A')$. Jetzt gibt es 2 Fälle:

1) Ist $r < n$, so sind alle Einträge in der letzten Zeile von A' gleich 0. Also ist $\det(A') = 0$ nach Lemma 15.3 und damit auch $\det(A) = 0$.
2) Ist $r = n$, so ist $A' = I_n$ (siehe Bemerkung 12.8), also $\det(A) = \det(Q)^{-1} \neq 0$.

Nach Satz 13.3 ist Q ein Produkt von Elementarmatrizen (die sich aus dem Gauß–Verfahren für $Q \to I_n$ ergeben). Also ist $\det(Q)$ das Produkt der Determinanten dieser Elementarmatrizen. Mit den obigen Formeln für diese Determinanten erhalten wir im Fall 2) eine Methode, um $\det(A) = \det(Q)^{-1}$ zu berechnen, die in den meisten Fällen effizienter ist als die Leibniz-Formel.

Folgerung 15.9. *Sei* K *ein Körper und* $A \in M_n(K)$*. Genau dann ist* A *invertierbar, wenn* $\det(A) \neq 0$ *gilt.*

Beweis. Wir haben bereits gesehen, dass $\det(A) \neq 0$ gilt, wenn A invertierbar ist. Sei nun umgekehrt $\det(A) \neq 0$. Sei $Q \in M_n(K)$ invertierbar so dass $A' = Q \cdot A$ Stufenform hat, mit $r \in \{0, 1, \ldots, n\}$ Stufen. Wegen $\det(A) \neq 0$ sind wir in Fall 2) von Bemerkung 15.8(b), also $r = n$ und $I_n = A' = Q \cdot A$. Also ist A invertierbar, mit $A^{-1} = Q$. □

Bemerkung 15.10. Sei $A \in M_n(K)$ und $\lambda \in K$. Mit Bemerkung 14.1 und Folgerung 15.9 erhalten wir: λ Eigenwert von $A \Leftrightarrow A - \lambda I_n$ nicht invertierbar $\Leftrightarrow \det(A - \lambda I_n) = 0$. Damit haben wir eine neue Charakterisierung von Eigenwerten! Wir können in $\det(A - \lambda I_n)$ das $\lambda \in K$ durch eine Unbestimmte X über K ersetzen und definieren das ***charakteristische Polynom*** von A als $\chi_A := \det(A - XI_n)$. Die Leibniz–Formel zeigt, dass $\det(A - XI_n)$ in der Tat ein Polynom in $K[X]$ ist; schaut man etwas genauer auf die Koeffizienten, so sieht man

$$\chi_A = \det(A - XI_n) = (-1)^n X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0 \in K[X]$$

mit $a_0 = \det(A)$ und $a_{n-1} = (-1)^{n-1}\mathrm{Spur}(A)$, wobei $\mathrm{Spur}(A) := a_{11} + \ldots + a_{nn} \in K$ als die ***Spur*** von A bezeichnet wird. (Es gibt auch Formeln für die anderen Koeffizienten, aber die sind komplizierter.) Also folgt:

λ Eigenwert von $A \quad \Leftrightarrow \quad \lambda$ ist Nullstelle des charakteristischen Polynoms χ_A.

Der folgende Satz ist eine berühmte Aussage der Matrix-Theorie. (Beweis im 2. Semester.)

Satz 15.11 (***Cayley–Hamilton***)**.** *Sei $A \in M_n(K)$ und $\chi_A \in K[X]$ das charakteristische Polynom von A. Dann gilt $\chi_A(A) = 0_{n\times n}$ und damit auch $\mu_A \mid \chi_A$ (siehe Folgerung 14.10).*

Beispiel 15.12. Sei $K = \mathbb{Q}$ und $A = \begin{bmatrix} -1 & 0 & 1 \\ 3 & 0 & -3 \\ 1 & 0 & -1 \end{bmatrix} \in M_3(\mathbb{Q})$.

Mit der Regel von Sarrus erhalten wir

$$\begin{aligned}\chi_A = \det\left(\begin{bmatrix} -1-X & 0 & 1 \\ 3 & -X & -3 \\ 1 & 0 & -1-X \end{bmatrix}\right) &= (-1-X) * (-X) * (-1-X) - 1 * (-X) * 1 \\ &= -X^3 - 2X^2 - X + X = -X^2 * (X+2).\end{aligned}$$

Andererseits können wir mit den Methoden wie in Beispiel 14.6 das Minimalpolynom von A bestimmen; wir erhalten $\mu_A = X * (X+2)$. Das charakteristische Polynom ist also "fast" gleich dem Minimalpolynom; es gilt aber auf jeden Fall $\mu_A \mid \chi_A$.

Kapitel IV: Vektorräume und lineare Abbildungen

In der Physik und anderen Naturwissenschaften kommen zum Beispiel "vektorielle" Größen (Geschwindigkeit, Kraft, ...) vor, die nicht nur einen Betrag, sondern auch eine Richtung haben. Durch Abstraktion von den jeweiligen konkreten Gegebenheiten gelangt man zum allgemeinen Begriff des "Vektorraums", der sich als äußerst nützlich nicht nur in der Mathematik selbst sondern auch in diversen Anwendungen erwiesen hat.

16. *Definition, Teilräume, Basis und Dimension*

Um einen Vektorraum zu definieren, braucht man zunächst einen Körper. Sei also K ein Körper, der im Folgenden meist fest vorgegeben ist. Ein ***Vektorraum*** über K (oder auch einfach K-Vektorraum) ist dann eine abelsche Gruppe $(V,+)$, auf der zusätzlich noch eine ***skalare Multiplikation*** mit Elementen aus K definiert ist. Dies bedeutet, dass es eine Abbildung $K \times V \to V$, $(s,v) \mapsto s.v$, mit folgenden Eigenschaften gibt:

$$(s_1+s_2).v = s_1.v + s_2.v, \quad s.(v_1+v_2) = s.v_1 + s.v_2, \quad s_1.(s_2.v) = (s_1s_2).v, \quad 1_K.v = v$$

für alle $s, s_1, s_2 \in K$ und $v, v_1, v_2 \in V$ (wobei 1_K das Eins-Element in K bezeichnet).

Wir haben bereits Beispiele gesehen: Die Menge der $m \times n$-Matrizen $V = K^{m\times n}$ ist ein K-Vektorraum, wobei Addition und skalare Multiplikation wie in Definition 11.2 definiert sind. Insbesondere sind $K^m = K^{m\times 1}$ (alle Spaltenvektoren mit m Einträgen in K) und $K^{1\times n}$ (alle Zeilenvektoren mit n Einträgen in K) Vektorräume über K.

Außerdem: Sei $K[X]$ die Menge der Polynome in einer Unbestimmten X mit Koeffizienten in K. Mit der üblichen Addition und skalaren Multiplikation für Polynome (siehe §9, S. 38) ist dann $K[X]$ ein K-Vektorraum. Weitere Beispiele:

Beispiel 16.1. (a) Sei X eine beliebige, nicht-leere Menge und $V := \mathrm{Abb}(X,K)$ die Menge aller Funktionen $f\colon X \to K$. Für $f, g \in V$ und $s \in K$ definieren wir $f+g \in V$ und $s.f \in V$ durch $(f+g)(x) := f(x)+g(x)$ und $(s.f)(x) := sf(x)$ für alle $x \in X$. Dann prüft man leicht nach, dass V ein K-Vektorraum ist. Das neutrale Element bezüglich der Addition ist die Null-Funktion $\underline{0}\colon X \to K$ mit $\underline{0}(x) := 0$ für alle $x \in X$. Für $f \in V$ ist $-f \in V$ gegeben durch $(-f)(x) := -f(x)$ für alle $x \in X$. Wichtiger Spezialfall: $X = \mathbb{N}_0$. Eine Funktion $f\colon \mathbb{N}_0 \to K$ ist nichts Anderes als eine Folge $(a_n)_{n\in\mathbb{N}_0}$ wobei $a_n = f(n)$ für alle $n \in \mathbb{N}_0$.

(b) Sei K in einem größeren Körper L enthalten, so dass die Operationen in K durch die Einschränkungen der entsprechenden Operationen in L gegeben sind. Typische Beispiele sind $K = \mathbb{Q} \subseteq L = \mathbb{R}$ oder $K = \mathbb{R} \subseteq L = \mathbb{C}$. Dann ist L ein K-Vektorraum, wobei die skalare Multiplikation $K \times L \to L$ einfach die Multiplikation von $s \in K$ mit $v \in L$ in L ist.

(c) (Ein exotisches Beispiel) Sei A beliebige, nicht-leere Menge und $V := \mathcal{P}(A)$ die Potenzmenge von A. Für $S, T \in V$ (also Teilmengen $S, T \subseteq A$) definieren wir $S+T := (S \cup T) \setminus (S \cap T)$ als die ***symmetrische Differenz***. Nach Ü1A6 ist "+" assoziativ und kommutativ. Außerdem ist $S + S = (S \cup S) \setminus (S \cap S) = S \setminus S = \varnothing$; es folgt, dass $\varnothing$ neutrales Element bezüglich "+" ist und $-S = S$. Damit ist $(V, +)$ eine abelsche Gruppe. Sei nun $\mathbb{F}_2 = \{\bar{0}, \bar{1}\}$ Körper mit 2 Elementen. Setzen wir $\bar{0}.S := \varnothing$ und $\bar{1}.S := S$ für alle $S \in V$, so prüft man leicht nach, dass obige Regeln für diese skalare Multiplikation gelten. Also ist V ein $\mathbb{F}_2$-Vektorraum.

Bemerkung 16.2. Sei V ein K-Vektorraum. Dann gilt:

(a) $s.0_V = 0_V$ für alle $s \in K$ (wobei 0_V = neutrales Element in V bezüglich "+").

(b) $0_K.v = 0_V$ für alle $v \in V$ (wobei 0_K = neutrales Element in K bezüiglich "+").

Denn: $0_V = s.0_V - s.0_V = s.(0_V + 0_V) - s.0_V = s.0_V + s.0_V - s.0_V = s.0_V$, also gilt (a). Der Beweis von (b) geht analog.

(c) Gilt $s.v = 0_V$ (wobei $s \in K$), so ist $s = 0_K$ oder $v = 0_V$.

Denn: Angenommen, es wäre $s \neq 0_K$. Dann gibt es $s^{-1} \in K$ und es folgt $v = 1_K.v = (s^{-1}s).v = s^{-1}.(s.v) = s^{-1}.0_V = 0_V$ nach (a).

(d) $-(s.v) = (-s).v = s.(-v)$ für alle $s \in K$ und $v \in V$.

Denn: $s.v + (-s).v = (s + (-s)).v = 0_K.v = 0_V$ nach (b). Also ist $(-s).v = -(s.v)$. Außerdem $s.v + s.(-v) = s.(v + (-v)) = s.0_V = 0_V$ nach (a). Also ist auch $s.(-v) = -(s.v)$.

Die folgende Definition ist eine wichtige Quelle, um neue Vektorräume zu erhalten.

Definition 16.3. Sei V ein K-Vektorraum und $U \subseteq V$ eine Teilmenge. Dann heißt U ein ***Teilraum*** (oder auch Untervektorraum) von V, in Zeichen manchmal $U \leqslant V$, wenn gilt:

$0_V \in U$ (insbesondere, U ist nicht-leer);

$u + u' \in U$ für alle $u, u' \in U$;

$s.u \in U$ für alle $s \in K$ und $u \in U$.

Also ist U abgeschlossen bezüglich Addition und skalarer Multiplikation. Dann ist U mit den Einschränkungen der Verknüpfungen aus V auch selbst wieder ein K-Vektorraum.

Beispiel 16.4. (a) Sei V ein K-Vektorraum. Dann sind $\{0_V\}$ und V Teilräume. Sei $v \in V$ fest und $U := K.v = \{s.v \mid s \in K\} \subseteq V$. Dann sieht man sofort, dass U ein Teilraum ist.

(b) Seien $U_1, U_2 \subseteq V$ Teilräume. Dann ist $U_1 \cap U_2 \subseteq V$ ein Teilraum (Übung, selbst), aber $U_1 \cup U_2$ ist im Allgemeinen kein Teilraum. Schließlich ist auch $U_1 + U_2 := \{u_1 + u_2 \mid u_1 \in U_1, u_2 \in U_2\} \subseteq V$ ein Teilraum. Etwas allgemeiner: Sind $U_1, \ldots, U_n \subseteq V$ Teilräume, so erhalten wir Teilräume $U_1 \cap U_2 \cap \ldots \cap U_n \subseteq V$ und $U_1 + U_2 + \ldots + U_n \subseteq V$.

(c) Sei $V = \mathrm{Abb}(K, K)$ der Vektorraum aller Funktionen $f\colon K \to K$. Wir betrachten

$U_1 := \{f \in V \mid f(t + 1) = f(t) \text{ für alle } t \in K\}$,

$U_2 := \{f \in V \mid f(1) = f(0)\}$,
$U_3 := \{f \in V \mid f(0) = 1\}$.
Behauptung: U_1 und U_2 sind Teilräume, U_3 ist kein Teilraum.
Zu U_1: Die Null-Funktion erfüllt die Bedingung, ist also in U_1 enthalten. Für $f, g \in U_1$ folgt $(f+g)(t+1) = f(t+1) + g(t+1) = f(t) + g(t) = (f+g)(t)$ für alle $t \in K$; für $s \in K$ gilt $(s.f)(t+1) = sf(t+1) = sf(t) = (s.f)(t)$ für alle $t \in K$. Also ist $f + g \in U_1$ und $s.f \in U_1$.
Zu U_2: Dies geht völlig analog (selbst). Zu U_3: Die Null-Funktion ist nicht in U_3.

Beispiel 16.5. Sei $A \in K^{m\times n}$ und $b \in K^m$. Sei $L := \{x \in K^n \mid A \cdot x = b\} \subseteq K^n$ die Lösungsmenge des zugehörigen LGS. Ist $b \neq 0_m$, so ist L kein Teilraum (weil $0_n \notin L$). Sei $N(A) := \{x \in K^n \mid A \cdot x = 0_m\} \subseteq K^n$ die Lösungsmenge des zugehörgen homogenen LGS. Dann ist $N(A)$ ein Teilraum. Dazu: Zunächst gilt $0_n \in N(A)$. Sind $x, y \in N(A)$ und $s \in K$, so folgt $A \cdot (x+y) = A \cdot x + A \cdot y = 0_m + 0_m = 0_m$ und $A \cdot (s.x) = s.(A \cdot x) = s.0_m = 0_m$, wobei wir die Regeln in Bemerkung 11.3 benutzt haben. Also ist $N(A)$ ein Teilraum.
Nehmen wir nun an, es sei $L \neq \varnothing$; sei $x_0 \in L$ eine feste Lösung. Dann gilt

$$L = x_0 + N(A) := \{x_0 + x \mid x \in N(A)\}.$$

Denn: Ist $x \in N(A)$ beliebig, so gilt $A \cdot (x_0 + x) = A \cdot x_0 + A \cdot x = b + 0_m = b$, also $x_0 + x \in L$. Sei umgekehrt $y \in L$ beliebig. Dann ist $A \cdot (y - x_0) = A \cdot y - A \cdot x_0 = b - b = 0_m$, also $x := y - x_0 \in N(A)$ und damit $y = x_0 + x \in x_0 + N(A)$.

Beispiel 16.6. (Beispiel aus der Analysis.) Sei $X = [a, b] \subseteq \mathbb{R}$ ein abgeschlossenes Intervall, wobei $a, b \in \mathbb{R}$ mit $a < b$. Dann ist $\mathcal{C}([a, b]) := \{f\colon [a, b] \to \mathbb{R} \mid f \text{ stetig}\}$ ein Teilraum von $\mathrm{Abb}([a, b], \mathbb{R})$. (Dazu benötigt man die Aussage, dass Summen und skalare Vielfache von stetigen Funktionen wieder stetig sind; siehe Analysis-Vorlesung.) Analog ist $\mathcal{D}((a, b)) := \{f\colon (a, b) \to \mathbb{R} \mid f \text{ differenzierbar für alle } x \in (a, b)\}$ ein Teilraum von $\mathrm{Abb}((a, b), \mathbb{R})$.

Ab hier Woche 11

Definition 16.7. Sei V ein K-Vektorraum und $B = \{v_1, \ldots, v_n\} \subseteq V$ eine Teilmenge (wobei $n \geqslant 1$). Um die Betrachtung von Sonderfällen zu vermeiden, nehmen wir $V \neq \{0_V\}$ an.
(a) Sind $s_1, \ldots, s_n \in K$ gegeben, so heißt $s_1v_1 + \ldots + s_nv_n \in V$ eine ***Linearkombination*** von $v_1, \ldots, v_n$ mit Koeffizienten $s_1, \ldots, s_n$.
(b) Die Teilmenge B heißt ***Erzeugendensystem*** von V, wenn sich jedes $v \in V$ schreiben lässt als Linearkombination $v = s_1.v_1 + \ldots + s_n.v_n$ mit $s_1, \ldots, s_n \in K$.
(c) Die Teilmenge B heißt ***Basis*** von V, wenn sich jedes $v \in V$ auf eindeutige Weise schreiben lässt als Linearkombination $v = s_1.v_1 + \ldots + s_n.v_n$ mit $s_1, \ldots, s_n \in K$.
(Eine Basis ist also ein spezielles Erzeugendensystem.)

Beispiel 16.8. Sei $V := K^{m\times n}$ und $B := \{E_{ij}^{(m,n)} \mid 1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n\} \subseteq V$ die Menge der Standardmatrizen; siehe Beispiel 11.7. Für $A = [a_{ij}] \in V$ beliebig gilt dann die Gleichung $A = \sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}E_{ij}^{(m,n)}$; also ist B ein Erzeugendensystem von V. Dies ist sogar eine Basis, denn für beliebige Koeffizienten $b_{ij} \in K$ ergibt die Linearkombination $\sum_{i=1}^{m}\sum_{j=1}^{n} b_{ij}E_{ij}^{(m,n)}$ die Matrix $B = [b_{ij}] \in V$; also ist $A = B$ genau dann, wenn $a_{ij} = b_{ij}$ für alle i, j gilt. Wir bezeichnen obiges B auch als ***Standardbasis*** von $K^{m\times n}$.

Betrachte konkret $K^2 = \left\{ \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \;\middle|\; x_1, x_2 \in K \right\}$. Dann ist $B = \left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\}$ die Standardbasis. Es gibt aber auch noch andere Basen; sei zum Beispiel $C = \left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right\}$. Dann haben wir eine eindeutige Darstellung $\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = (x_1 - x_2)\begin{bmatrix} 1 \\ 0 \end{bmatrix} + x_2 \begin{bmatrix} 1 \\ 1 \end{bmatrix}$ für $x_1, x_2 \in K$. Also ist C eine Basis. Die damit einhergehende Frage von "Basiswechseln" werden wir in §19 näher untersuchen.

Beispiel 16.9. Sei $P(K)$ die Menge aller Polynomfunktionen $f\colon K \to K$. Dann ist $P(K) \subseteq \mathrm{Abb}(K, K)$ und man sieht sofort, dass $P(K)$ ein Teilraum ist, also selbst ein K-Vektorraum. Sei weiterhin $n \in \mathbb{N}_0$ und $P_n(K) \subseteq P(K)$ die Teilmenge aller Polynomfunktionen f, so dass es Koeffizietnen $a_0, a_1, \ldots, a_n \in K$ gibt mit $f(x) = a_0 + a_1x + \ldots + a_nx^n$ für alle $x \in K$ (wie auch schon zu Beginn von §9 definiert). Dann sieht man wiederum sofort, dass $P_n(K)$ ein Teilraum ist, also selbst ein K-Vektorraum. Für $i \in \mathbb{N}_0$ sei nun $p_i \in P(K)$ definiert durch $p_i(x) := x^i$ für alle $x \in K$ (wobei $0^0 = 1$). Sei $B := \{p_0, p_1, \ldots, p_n\} \subseteq P_n(K)$. Aufgrund der Definition von $P_n(K)$ ist dann klar, dass B ein Erzeugendensystem von $P_n(K)$ ist. Ist $|K| > n$, so besagt Folgerung 9.3, dass B sogar eine Basis von $P_n(K)$ ist. (Und das Beispiel unmittelbar nach Folgerung 9.3 zeigt, dass B im Allgemeinen keine Basis von $P_n(K)$ ist, wenn K zu klein ist.) Ist $|K| > n$, so ist wiederum eine weitere Basis von $P_n(K)$ gegeben durch die Lagrange–Polynomfunktionen $\{L_1, L_2, \ldots, L_{n+1}\}$; siehe Beweis von Folgerung 9.4.

Man sieht, dass es im Allgemeinen keine ausgezeichnete oder irgendwie bevorzugte Basis gibt; für manche Zwecke mag die eine Basis nützlicher sein als die andere.

Im weiteren Verlauf werden wir noch viele Beispiele für Basen und Erzeugendensysteme sehen. Zentral sind nun die folgende Aussage und die anschließende Definition.

Satz 16.10. *Sei $V \neq \{0_V\}$ ein K-Vektorraum. Seien $B = \{v_1, \ldots, v_n\}$ und $C = \{w_1, \ldots, w_m\}$ Basen (mit $m, n \geqslant 1$). Dann gilt $n = m$; d.h., je zwei Basen enthalten gleich viele Elemente.*

Beweis. Angenommen, es wäre $n > m$. Da C ein Erzeugendensystem ist, ist jedes v_j eine Linearkombination der w_i. Für $1 \leqslant j \leqslant n$ gibt es also Koeffizienten $a_{ij} \in K$ mit $v_j =$

$\sum_{i=1}^{m} a_{ij}.w_i$. Wir betrachten das homogene LGS mit Matrix $A := [a_{ij}]_{1\leqslant i\leqslant m, 1\leqslant j\leqslant n} \in K^{m\times n}$. Wegen $n > m$ hat dies mehr Unbekannte als Gleichungen; nach Satz 13.1 gibt es also ein $x \in K^n$ mit $A \cdot x = 0_m$ und $x \neq 0_n$. Seien $x_1, \ldots, x_n \in K$ die Komponenten von x. Dann folgt

$$x_1.v_1 + \ldots + x_n.v_n = \sum_{j=1}^{n} x_j.v_j = \sum_{j=1}^{n} x_j.\Big(\sum_{i=1}^{m} a_{ij}.w_i\Big) = \sum_{j=1}^{n}\sum_{i=1}^{m} (x_j a_{ij}).w_i$$
$$= \sum_{i=1}^{m}\sum_{j=1}^{n} (a_{ij}x_j).w_i = \sum_{i=1}^{m} \underbrace{\Big(\sum_{j=1}^{n} a_{ij}x_j\Big)}_{=0 \text{ da } A\cdot x=0_m}.w_i = 0_V.$$

Andererseits ist auch $0.v_1 + \ldots + 0.v_n = 0_V$. Nun haben wir 0_V auf zwei verschiedene Weisen als Linearkombination von $v_1, \ldots, v_n$ geschrieben (die beiden sind verschieden, weil nicht alle x_j gleich 0 sind), Widerspruch dazu, dass B eine Basis ist. Also war die Annahme falsch, d.h., es ist $n \leqslant m$. Völlig analog führt man die Annahme $n < m$ zum Widerspruch. □

Definition 16.11. Sei V ein K-Vektorraum, $V \neq \{0_V\}$. Ist $B = \{v_1, \ldots, v_n\}$ eine Basis (mit $n \geqslant 1$), so heißt $\dim V = n$ die ***Dimension*** von V. Nach Satz 16.10 hängt dies nicht davon ab, welche Basis B wir nehmen. Ist $V = \{0_V\}$, so setzen wir $\dim V = 0$.
Wir werden im nächsten Abschnitt zeigen (Satz 17.6), dass ein Vektorraum, für den es ein Erzeugendensystem mit endlich vielen Elementen gibt, auch tatsächlich eine Basis besitzt. Gibt es kein endliches Erzeugendensystem von V, so setzen wir $\dim V = \infty$.

In Beispiel 16.8 ist $\dim K^{m\times n} = mn$; insbesondere haben wir die Spezialfälle

$$\dim K^{1\times n} = n \text{ (Zeilenvektoren)} \qquad \text{und} \qquad \dim K^{m\times 1} = m \text{ (Spaltenvektoren).}$$

In Beispiel 16.9 ist $\dim P_n(K) = n + 1$, jedenfalls wenn $|K| > n$.

Betrachten wir noch den $\mathbb{F}_2$-Vektorraum $V = \mathcal{P}(A)$ wie im "exotischen" Beispiel 16.1(c), wobei A eine nicht-leere, endliche Menge sei; also $A = \{a_1, \ldots, a_n\}$ mit $n \geqslant 1$. Sei $v_i := \{a_i\}$ für $i = 1, \ldots, n$. Dann überzeugen Sie sich leicht, dass $B = \{v_1, \ldots, v_n\}$ eine Basis ist, und damit $\mathcal{P}(A) = \{s_1.v_1 + \ldots + s_n.v_n \mid s_i \in \mathbb{F}_2\}$. Weil wir für jedes s_i genau 2 Mglichkeiten haben, folgt $|\mathcal{P}(A)| = 2^n$; wir haben hier also einen neuen Beweis für die Aussage in Beispiel 7.7.

Als weiteres (wichtigeres) Beispiel betrachten wir die Lösungsmenge $N(A) \subseteq K^n$ eines homogenen LGS mit Matrix $A \in K^{m\times n}$. Nach Beispiel 16.5 ist $N(A)$ ein Teilraum, also selbst ein K-Vektorraum. Mit dem Gauß-Verfahren in §12 erhalten wir nun auch eine Basis von $N(A)$, wie folgt. Sei $A \to A'$ wobei $A' = [a'_{ij}] \in K^{m\times n}$ Stufenform hat mit $r \in \{0, 1, \ldots, m\}$ Stufen und Pivots $1 \leqslant j_1 < \ldots < j_r \leqslant n$.

Satz 16.12 (Basis von $\mathsf{N}(A)$)**.** *Mit den obigen Bezeichnungen sei* $I := \{1,\dots,n\}\backslash\{j_1,\dots,j_r\}$. *Wir setzen* $v_j := e_j - \sum_{i=1}^{r} a'_{ij} e_{j_i} \in K^n$ *für alle* $j \in I$, *wobei* $e_1,\dots,e_n$ *die Standardvektoren in* K^n *sind. Dann ist* $\{v_j \mid j \in I\}$ *eine Basis von* $\mathsf{N}(A)$, *also* $\dim \mathsf{N}(A) = n - r$.

Beweis. Nach Bemerkung 12.3 ist $\mathsf{N}(A) = \mathsf{N}(A')$. Sei $j \in I$ und $w_j := A' \cdot v_j \in K^m$. Für $k \in \{1,\dots,m\}$ sei $w_j^{(k)} \in K$ die k-te Komponente von w_j. Da $A' \cdot e_j$ die j-te Spalte von A' und $A' \cdot e_{j_i}$ die j_i-te Spalte von A' ist, folgt $w_j^{(k)} = a'_{kj} - \sum_{i=1}^{r} a'_{ij} a'_{kj_i}$. Ist $k > r$ so ist $a'_{kl} = 0$ für alle $l = 1,\dots,n$, also auch $w_j^{(k)} = 0$. Sei nun $1 \leqslant k \leqslant r$. Nun ist die j_i-te Spalte von A' gleich dem i-ten Standardvektor in K^m, also gilt $a'_{kj_i} = \delta_{ik}$ (Kronecker–Delta) und damit $w_j^{(k)} = a'_{kj} - \sum_{i=1}^{r} a'_{ij}\delta_{ik} = a'_{kj} - a'_{kj} = 0$. Also sind alle Komponenten von $w_j = A' \cdot v_j$ gleich 0 und damit $v_j \in \mathsf{N}(A') = \mathsf{N}(A)$. Wir müssen noch zeigen, dass jedes $v \in \mathsf{N}(A)$ sich auf eindeutige Weise als Linearkombination der v_j mit $j \in I$ schreiben lässt.

Sei $x \in \mathsf{N}(A)$ beliebig, mit Komponenten $x_1,\dots,x_n \in K$. Wie in §12 (S. 55) gilt dann $x_{j_i} = -\sum_{j\in I} a'_{ij} x_j$ für $i = 1,\dots,r$. Damit folgt $\sum_{j\in I} x_j v_j = \sum_{j\in I} x_j\big(e_j - \sum_{i=1}^{r} a'_{ij} e_{j_i}\big) = \sum_{j\in I} x_j e_j - \sum_{i=1}^{r}\Big(\sum_{j\in I} a'_{ij} x_j\Big) e_{j_i} = \sum_{j\in I} x_j e_j + \sum_{i=1}^{r} x_{j_i} e_{j_i} = x$, also ist $\{v_j \mid j \in I\}$ ein Erzeugendensystem für $\mathsf{N}(A)$. Zur Eindeutigkeit: Sind auch $y_j \in K$ für $j \in I$ gegeben mit $x = \sum_{j\in I} y_j v_j$, so zeigt eine analoge Rechnung, das für $k \in I$ die k-te Komponente von $\sum_{j\in I} y_j v_j$ gegeben ist durch y_k. Also muss $y_k = x_k$ gelten für alle $k \in I$. □

Beispiel ($K = \mathbb{Q}$): $A = \begin{bmatrix} 0 & 0 & 2 & 2 \\ 2 & 4 & 2 & 6 \\ 3 & 6 & 0 & 6 \end{bmatrix} \rightarrow A' = \begin{bmatrix} \underline{1} & 2 & 0 & 2 \\ 0 & 0 & \underline{1} & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$ $\quad r = 2,\ j_1 = 1,\ j_2 = 3,\ I = \{2,4\}$

Allgemeine Lösung: $\begin{bmatrix} -2x_2 - 2x_4 \\ x_2 \\ -x_4 \\ x_4 \end{bmatrix} = x_2 v_2 + x_4 v_4$ mit $v_2 = \begin{bmatrix} -2 \\ 1 \\ 0 \\ 0 \end{bmatrix}$, $v_4 = \begin{bmatrix} -2 \\ 0 \\ -1 \\ 1 \end{bmatrix}$.

(In GAP erhält man die Vektoren v_2, v_4 mit der Funktion `NullspaceMat`.)

Bemerkung 16.13. Betrachten wir $\mathbb{C}$ als $\mathbb{R}$-Vektorraum (wie in Beispiel 16.1(b)), so gilt $\dim \mathbb{C} = 2$, denn jedes $z \in \mathbb{C}$ lässt sich eindeutig schreiben als Linearkombination $z = a + bi$ mit $a, b \in \mathbb{R}$. Hier ist also $B = \{1, i\}$ eine $\mathbb{R}$-Basis von $\mathbb{C}$. Betrachten wir dagegen $\mathbb{R}$ als $\mathbb{Q}$-Vektorraum, so gilt $\dim \mathbb{R} = \infty$. Denn sonst gäbe es eine $\mathbb{Q}$-Basis $B = \{v_1,\dots,v_n\}$ von $\mathbb{R}$, wobei $n \in \mathbb{N}$. Wir erhielten dann eine bijektive Abbildung

$$\mathbb{Q}^n \to \mathbb{R}, \qquad (s_1,\dots,s_n) \mapsto s_1 v_1 + \ldots + s_n v_n,$$

was bedeuten würde, dass $\mathbb{R}$ und $\mathbb{Q}^n$ gleichmächtig sind. Aber mit $\mathbb{Q}$ ist auch $\mathbb{Q}^n$ abzählbar unendlich, Widerspruch dazu dass $\mathbb{R}$ überabzählbar ist.

Man kann auch den Begriff einer "Basis" definieren, wenn $\dim V = \infty$ gilt; siehe dazu Bemerkung 17.8 im nächsten Abschnitt.

17. *Erzeugnis und lineare Unabhängigkeit*

Um effizient mit Basen und $\dim V$ umgehen zu können, benötigen wir noch einige weitere Begriffe, die zum Grundwerkzeug der Linearen Algebra gehören. Die einzelnen Beweise in diesem Abschnitt werden nicht sehr schwierig sein, aber am Ende erhält man doch einige wichtige Ergebnisse, die im Folgenden ständig und fast automatisch benutzt werden.

Sei V ein Vektorraum über einem Körper K. Sind $v_1, \ldots, v_n \in V$ mit $n \geqslant 1$ gegeben, so definieren wir $\langle v_1, \ldots, v_n \rangle_K \subseteq V$ als die Menge aller Linearkombinationen $s_1.v_1 + \ldots + s_n.v_n$ mit $s_1, \ldots, s_n \in K$. Man sieht dann sofort, dass $\langle v_1, \ldots, v_n \rangle_K$ ein Teilraum von V ist, der als ***Erzeugnis*** (englisch: "span") von $v_1, \ldots, v_n$ bezeichnet wird. Ist $S \subseteq V$ eine beliebige nichtleere Teilmenge, so definieren wir das Erzeugnis $\langle S \rangle_K$ als die Menge aller Linearkombinationen $s_1.v_1 + \ldots + s_n.v_n$ wobei $n \in \mathbb{N}$ sowie $v_1, \ldots, v_n \in S$ und $s_1, \ldots, s_n \in K$ beliebig sind. Wiederum ist dann klar, dass $\langle S \rangle_K$ ein Teilraum von V ist. Ist $S = \varnothing$, so setzen wir $\langle \varnothing \rangle_K = \{0_V\}$. (Damit ist $\{\}$ eine Basis des Vektorraums $V = \{0_V\}$.)

Beachte: Ist $U \subseteq V$ ein Teilraum mit $S \subseteq U$, so gilt offenbar $\langle S \rangle_K \subseteq U$ (aufgrund der Definition eines Teilraums); also ist $\langle S \rangle_K$ der kleinste Teilraum, der S enthält. Wir sagen, dass V ***endlich erzeugt*** ist, wenn es eine endliche Teilmenge $S \subseteq V$ gibt mit $V = \langle S \rangle_K$.

Beispiel 17.1. Sei $K[X]$ der Vektorraum der Polynome in der Unbestimmten X über K.
(a) Für $n \in \mathbb{N}_0$ definieren wir $K[X]_{\leqslant n} := \langle 1, X, X^2, \ldots, X^n \rangle_K \subseteq K[X]$. Dann besteht $K[X]_{\leqslant n}$ genau aus allen Polynomen der Form $f = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0$ mit $a_i \in K$ für alle i. Hier ist $B := \{1, X, X^2, \ldots, X^n\}$ sogar eine Basis von $K[X]_{\leqslant n}$, also $\dim K[X]_{\leqslant n} = n + 1$.
(b) Für $K[X]$ selbst ist $S = \{X^n \mid n \in \mathbb{N}_0\}$ ein Erzeugendensystem, weil jedes $f \in K[X]$ eine Linearkombination von endlich vielen der Potenzen X^n ist. Dieses Erzeugendensystem ist sicherlich minimal, denn ist $S' \subsetneqq S$ und $n \in \mathbb{N}_0$ mit $X^n \in S \setminus S'$, so ist $f = X^n$ nicht als Linearkombination von Potenzen X^m mit $m \neq n$ schreibbar, also $\langle S' \rangle_K \subsetneqq K[X]$.
(c) Behauptung: $K[X]$ ist nicht endlich erzeugt. Annahme, doch! Dann gäbe es $f_1, \ldots, f_m \in K[X]$ mit $K[X] = \langle f_1, \ldots, f_m \rangle_K$; hier können wir $f_i \neq \underline{0}$ für alle i annehmen. Sei $N := \max\{\mathrm{Grad}(f_i) \mid 1 \leqslant i \leqslant m\}$. Dann ist jedes f_i eine Linearkombination von $1, X, X^2, \ldots, X^N$, also $f_i \in K[X]_{\leqslant N}$. Weil $K[X]_{\leqslant N}$ ein Teilraum ist, gilt dann für beliebige $s_1, \ldots, s_N \in K$ auch $s_1 f_1 + \ldots + s_N f_N \in K[X]_{\leqslant N}$. Also folgt $K[X] = \langle f_1, \ldots, f_m \rangle_K \subseteq K[X]_{\leqslant N}$, Widerspruch dazu, dass zum Beispiel $X^{N+1} \notin K[X]_{\leqslant N}$. Also ist $K[X]$ nicht endlich erzeugt.

Definition 17.2. Gegeben seien $v_1, \ldots, v_n \in V$ (mit $n \geqslant 1$). Das Tupel $(v_1, \ldots, v_n)$ heißt ***linear abhängig*** (kurz l.a.), wenn es Koeffizienten $s_1, \ldots, s_n \in K$ gibt, die nicht alle gleich 0 sind, so dass $s_1.v_1 + \ldots + s_n.v_n = 0_V$ gilt. Andernfalls heißt das Tupel ***linear unabhängig*** (kurz l.u.). Die Bedingung, dass $(v_1, \ldots, v_n)$ l.u. ist, bedeutet also:

Wenn $s_1.v_1 + \ldots + s_n.v_n = 0_V$ gilt mit $s_i \in K$, so folgt $s_1 = \ldots = s_n = 0$.

Als Konvention verabreden wir, dass das leere Tupel () ebenfalls l.u. ist.

Folgerung 17.3. *Gegeben seien* $v_1, \ldots, v_n \in V$ *mit* $n \geqslant 1$. *Dann gilt:*

$B = \{v_1, \ldots, v_n\}$ *Basis von* $V \quad \Leftrightarrow \quad (v_1, \ldots, v_n)$ *ist l.u. und* $V = \langle v_1, \ldots, v_n \rangle_K$.

Beweis. "$\Rightarrow$" Ist B eine Basis, so ist B ein Erzeugendensystem von V. Außerdem ist jedes $v \in V$ auf eindeutige Weise eine Linearkombination von $v_1, \ldots, v_n$. Nehmen wir $v = 0_V$, so bedeutet dies speziell, dass $0_V = 0.v_1 + \ldots + 0.v_n$ die einzige Darstellung von 0_V als Linearkombination von $v_1, \ldots, v_n$ ist, d.h., das Tupel $(v_1, \ldots, v_n)$ ist l.u.

"$\Leftarrow$" Da B ein Erzeugendensystem ist, müssen wir noch zeigen, dass jedes $v \in V$ auf eindeutige Weise eine Linearkombination von $v_1, \ldots, v_n$ ist. Seien also $s_i, t_j \in K$ gegeben mit $s_1.v_1 + \ldots + s_n.v_n = t_1.v_1 + \ldots + t_n.v_n$. Dann folgt $(s_1 - t_1).v_1 + \ldots + (s_n - t_n).v_n = 0_V$, also $s_i - t_i = 0$ für alle i, weil $(v_1, \ldots, v_n)$ als l.u. angenommen ist. Damit auch $s_i = t_i$ für alle i. □

Beispiel 17.4. Sei $A = [a_{ij}] \in K^{m \times n}$. Für $j = 1, \ldots, n$ sei $v_j \in K^m$ die j-te Spalte von A, also $v_j = \begin{bmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{bmatrix} = A \cdot e_j$ wobei $e_j \in K^n$ der j-te Standardvektor ist (siehe Beispiel 11.7). Frage: Wann ist das Tupel $(v_1, \ldots, v_n)$ l.u.? Dazu seien $s_1, \ldots, s_n \in K$. Dann ist

$$0_m = s_1.v_1 + \ldots + s_n.v_n = s_1(A \cdot e_1) + \ldots + s_n(A \cdot e_n) = A \cdot (s_1 e_1) + \ldots + A \cdot (s_n e_n) = A \cdot \begin{bmatrix} s_1 \\ \vdots \\ s_n \end{bmatrix}.$$

Also ist $(v_1, \ldots, v_n)$ genau dann l.u., wenn das homogene LGS mit Matrix A nur die triviale Lösung hat. Damit ist das Problem zurückgeführt auf das Lösen eines homogenen LGS.

Sei zum Beispiel $A = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \in M_3(K)$, also $v_1 = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}, v_2 = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix}, v_3 = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$.

Mit Gauß–Elimination erhalten wir $A \to \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & -1 \\ 0 & 0 & 2 \end{bmatrix}$.

Ist $2 = 1 + 1 \neq 0$ in K, so können wir die 3. Zeile mit 2^{-1} multiplizieren und die Einträge in der letzten Spalte ausräumen, d.h., $A \to I_3$. Also ist in diesem Fall (v_1, v_2, v_3) l.u.

Ist $1 + 1 = 0$, so sind alle Einträge in der 3. Zeile gleich 0, also haben wir Stufenform mit $r = 2$. Damit gibt es eine freie Variable, also eine nicht-triviale Lösung, d.h., (v_1, v_2, v_3) l.a.

Weiteres Beispiel: $A = \begin{bmatrix} 0 & 1 \\ 1 & 2 \\ 2 & 4 \\ -1 & -2 \end{bmatrix} \in \mathbb{Q}^{4 \times 2}$, also $v_1 = \begin{bmatrix} 0 \\ 1 \\ 2 \\ -1 \end{bmatrix}, v_2 = \begin{bmatrix} 1 \\ 2 \\ 4 \\ -2 \end{bmatrix}$, mit $A \to \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}$.

Also ist (v_1, v_2) l.u.

Lemma 17.5. *Gegeben seien* $v_1, \ldots, v_n \in V$ *mit* $n \geqslant 1$. *Ist das Tupel* $(v_1, \ldots, v_n)$ *l.a., so gibt es ein* $j \in \{1, \ldots, n\}$ *mit* $v_j \in \langle v_1, \ldots, v_{j-1}\rangle_K$ *und* $\langle v_1, \ldots, v_n\rangle_K = \langle v_1, \ldots, v_{j-1}, v_{j+1}, \ldots, v_n\rangle_K$, *d.h.,* v_j *kann im Erzeugnis weggelassen werden.*

Beweis. Nach Voraussetzung gibt es $s_1, \ldots, s_n \in K$, die nicht alle gleich 0 sind, mit $s_1.v_1 + \ldots + s_n.v_n = 0_V$. Sei $j := \max\{1 \leqslant i \leqslant n \mid s_i \neq 0\}$. Dann ist $0_V = s_1.v_1 + \ldots + s_{j-1}.v_{j-1} + s_j.v_j$ wobei $s_j \neq 0$. Also erhalten wir auch $0_V = (s_j^{-1}s_1).v_1 + \ldots + (s_j^{-1}s_{j-1}).v_{j-1} + v_j$ und damit $v_j = -(s_j^{-1}s_1).v_1 - \ldots - (s_j^{-1}s_{j-1}).v_{j-1} \in \langle v_1, \ldots, v_{j-1}\rangle_K$. Seien nun $U := \langle v_1, \ldots, v_n\rangle_K$ und $U' := \langle v_1, \ldots, v_{j-1}, v_{j+1}, \ldots, v_n\rangle_K$. Es ist klar, dass $U' \subseteq U$ gilt. Andererseits ist auch $v_j \in \langle v_1, \ldots, v_{j-1}\rangle_K \subseteq U'$. Insgesamt also $v_i \in U'$ für alle i und damit auch $U \subseteq U'$. □

Satz 17.6 (Existenz von Basen)**.** *Sei* V *ein endlich erzeugter Vektorraum; sei* $S \subseteq V$ *eine endliche Menge mit* $V = \langle S\rangle_K$. *Dann gibt es eine Teilmenge* $B \subseteq S$, *so dass* B *eine Basis ist. Insbesondere ist* $\dim V = |B| \leqslant |S| < \infty$.

Beweis. Ist $V = \{0_V\}$, so ist $B := \{\}$ eine Basis. Sei nun $V \neq \{0_V\}$. Wähle eine Teilmenge $B \subseteq S$, so dass $|B|$ minimal ist und immer noch $V = \langle B\rangle_K$ gilt. (Dann ist $B \neq \varnothing$; der Fall $B = S$ ist hier natürlich erlaubt und möglich.) Behauptung: B ist eine Basis. Dazu: Sei $d := |B| \geqslant 1$ und schreibe $B := \{v_1, \ldots, v_d\}$. Da bereits $V = \langle B\rangle_K$ gilt, müssen wir noch zeigen, dass das Tupel $(v_1, \ldots, v_d)$ l.u. ist (siehe Folgerung 17.3). Wäre $(v_1, \ldots, v_d)$ l.a., so gibt es nach Lemma 17.5 ein $j \in \{1, \ldots, d\}$ mit $\langle B\rangle_K = \langle v_1, \ldots, v_{j-1}, v_{j+1}, \ldots, v_d\rangle_K$, d.h., die echt kleinere Teilmenge $\{v_1, \ldots, v_{j-1}, v_{j+1}, \ldots, v_d\} \subsetneqq B \subseteq S$ wäre ebenfalls ein Erzeugendensystem, Widerspruch. □

Folgerung 17.7. *Sei* V *ein endlich erzeugter Vektorraum und* $B \subseteq V$ *eine endliche Teilmenge. Genau dann ist* B *eine Basis von* V, *wenn* $V = \langle B\rangle_K$ *gilt und* $V \neq \langle B'\rangle_K$ *für jede echte Teilmenge* $B' \subsetneqq B$.

Beweis. Sei zuerst $B \subseteq V$ endlich mit $V = \langle B\rangle_K$ und $V \neq \langle B'\rangle_K$ für jede echte Teilmenge $B' \subsetneqq B$. Mit im Wesentlichen dem gleichen Beweis wie oben folgt, dass B eine Basis ist. Sei nun umgekehrt B eine Basis; dann ist jedenfalls $V = \langle B\rangle_K$. Sei $B' \subsetneqq B$ und $v_0 \in B \setminus B'$. Angenommen, es gilt $V = \langle B'\rangle_K$. Dann gibt es $v_1, \ldots, v_n \in B'$ und $s_i \in K$ mit $v_0 = s_1.v_1 + \ldots + s_n.v_n$. Aber dies sind zwei verschiedene Weisen, um v_0 als Linearkombinationen von Elementen in B zu schreiben, einmal als $1.v_0$ und einmal als $s_1.v_1 + \ldots + s_n.v_n$ (beachte $v_0 \neq v_i$ für $i = 1, \ldots, n$), Widerspruch zur Definition einer Basis. □

Bemerkung 17.8. Sei V beliebiger K-Vektorraum, also nicht unbedingt endlich erzeugt. Dann können wir die Äquivalenz in Folgerung 17.7 als *Definition* für den Begriff einer Basis von V nehmen. Also: *Eine Teilmenge* $B \subseteq V$ *heißt Basis von* V, *wenn* $V = \langle B\rangle_K$ *gilt und* $V \neq \langle B'\rangle_K$ *für jede echte Teilmenge* $B' \subsetneqq B$. Genau wie oben zeigt man, dass sich wiederum

jedes $v \in V$ auf eindeutige Weise als Linearkombination von endlich vielen Elementen von B schreiben lässt. Zum Beispiel ist $B := \{X^n \mid n \in \mathbb{N}_0\}$ eine Basis von $K[X]$ (siehe Beispiel 17.1).

Mit dem ***Auswahlaxiom*** (bzw. dem ***Lemma von Zorn***) kann man ganz allgemein zeigen, dass es stets eine Basis gibt und dass alle Basen gleichmächtig sind. Diese reinen Existenzaussagen sind zwar von prinzipiellem theoretischen Interesse; die praktischen Anwendungen halten sich aber sehr in Grenzen. Mehr dazu im 2. Semester, oder siehe auch die Diskussion in `https://en.wikipedia.org/wiki/Basis_(linear_algebra)`.

Zum Beispiel muss es damit eine Teilmenge $B \subseteq \mathbb{R}$ geben, so dass B eine Basis von $\mathbb{R}$ als $\mathbb{Q}$-Vektorraum ist; nach Bemerkung 16.13 ist sicherlich $|B| = \infty$. Aber niemanden ist es bisher gelungen, eine solche Teilmenge $B \subseteq \mathbb{R}$ explizit zu bestimmen oder hinzuschreiben!

Ab hier Woche 12

Beispiel 17.9. Seien $v_1, \ldots, v_n \in V$. Dann bilden wir den Teilraum $U := \langle v_1, \ldots, v_n \rangle_K \subseteq V$. Also ist $\{v_1, \ldots, v_n\}$ ein Erzeugendensystem von U; wie findet man eine Basis ? Dazu: Man sieht leicht, dass sich U nicht ändert, wenn man eine der 3 folgenden Operationen ausführt (analog zu elementaren Umformungen für Matrizen):

(i) Für $i \neq j$ vertausche v_i und v_j.
(ii) Für $0 \neq c \in K$ ersetze v_i durch cv_i.
(iii) Für $i \neq j$ und $c \in K$ ersetze v_i durch $v_i + cv_j$.

Betrachten wir ein konkreteres Beispiel. Sei $A = [a_{ij}] \in K^{m \times n}$. Seien $v_1, \ldots, v_n \in K^m$ die Spalten von A und $w_1, \ldots, w_m \in K^{1 \times n}$ die Zeilen von A. Wir definieren

$$SR(A) := \langle v_1, \ldots, v_n \rangle_K \subseteq K^m, \qquad \textbf{\textit{Spaltenraum}} \text{ von } A,$$
$$ZR(A) := \langle w_1, \ldots, w_m \rangle_K \subseteq K^n, \qquad \textbf{\textit{Zeilenraum}} \text{ von } A.$$

Betrachten wir zunächst $ZR(A)$. Die Operationen (i), (ii), (iii) entsprechen dann den elementaren Zeilenumformungen in §12. Also gilt $ZR(A) = ZR(A')$ wobei $A \to A' \in K^{m \times n}$ (Gauß–Elimination) und A' Stufenform hat mit $r \in \{0, 1, \ldots, m\}$ Stufen und Pivots $1 \leqslant j_1 < \ldots < j_r \leqslant n$. Seien $w'_1, \ldots, w'_r \in K^{1 \times n}$ die ersten r Zeilen von A'. (Die Einträge in den restlichen Zeilen sind alle gleich 0.)

Behauptung: $B := \{w'_1, \ldots, w'_r\}$ ist eine Basis von $ZR(A)$.

Dazu: Wegen $ZR(A) = ZR(A')$ ist B ein Erzeugendensystem. Seien nun $s_1, \ldots, s_r \in K$ gegeben mit $s_1 w'_1 + \ldots + s_r w'_r = 0_{1 \times n}$. Wegen der Bedingungen in der Definition der Stufenform sind die Spalten von A' zu den Pivots $j_1, \ldots, j_r$ gegegen durch die Standardvektoren $e_1, \ldots, e_r \in K^m$. Also sind die Komponenten des Zeilenvektors $s_1 w'_1 + \ldots + s_r w'_r \in K^{1 \times n}$ zu den Pivot-Spalten $j_1, \ldots, j_r$ gegeben durch $s_1, \ldots, s_r$. Also folgt $s_1 = \ldots = s_r = 0$. □

Dies zeigt wieder einmal die fundamentale Bedeutung des Gauß–Verfahrens. — Mit der oben beschriebenen Methode können Sie praktisch alle Fragen zu Basis und Dimension für

Vektorräume lösen, die aus Zeilenvektoren bestehen. (Mit Hilfe von elementaren Spaltenumformungen erhält man eine analoge Aussage für $\mathrm{SR}(A)$.)

Lemma 17.10. *Gegeben seien $v, v_1, \ldots, v_n \in V$ mit $n \geqslant 0$. Wenn das Tupel $(v_1, \ldots, v_n)$ l.u. ist und $v \notin \langle v_1, \ldots, v_n \rangle_K$ gilt, dann ist das Tupel $(v_1, \ldots, v_n, v)$ auch l.u.*

Beweis. Die Aussage gilt für $n = 0$, denn dann ist $v \notin \langle\{\}\rangle_K = \{0_V\}$, d.h., $v \neq 0_V$; also ist das Tupel (v) l.u. Sei nun $n \geqslant 1$ und setze $v_{n+1} := v$. Angenommen, $(v_1, \ldots, v_n, v_{n+1})$ wäre l.a. Nach Lemma 17.5 gibt es dann ein $j \in \{1, \ldots, n+1\}$ und $s_1, \ldots, s_{j-1} \in K$ mit $v_j = s_1.v_1 + \ldots + s_{j-1}.v_{j-1}$. Wäre $j \leqslant n$, so erhielten wir $s_1.v_1 + \ldots + s_{j-1}.v_{j-1} + (-1).s_j + 0.v_{j+1} + \ldots + 0.v_n = 0_V$, Widerspruch zur ersten Voraussetzung (dass $(v_1, \ldots, v_n)$ l.u. ist). Also muss $j = n+1$ gelten, d.h., $v = v_{n+1} \in \langle v_1, \ldots, v_n \rangle_K$, Widerspruch zur zweiten Voraussetzung. □

Satz 17.11. *Sei V endlich erzeugt und $m := \dim V < \infty$. Sei $B := \{v_1, \ldots, v_n\} \subseteq V$ so dass das Tupel $(v_1, \ldots, v_n)$ l.u. ist. Dann gilt $n \leqslant m$. Ist $n = m$, so ist B eine Basis von V.*

Beweis. Sei $C = \{w_1, \ldots, w_m\}$ eine Basis von V. Annahme, es wäre $n > m$. Mit wörtlich dem gleichen Beweis wie zu Satz 16.10 erhalten wir $x_1, \ldots, x_n \in K$, die nicht alle gleich 0 sind, mit $x_1.v_1 + \ldots + x_n.v_n = 0_V$, Widerspruch zur Voraussetzung, dass $(v_1, \ldots, v_n)$ l.u. ist. Also war die Annahme falsch, d.h., es gilt $n \leqslant m$, wie behauptet.
Sei nun $n = m$. Dann müssen wir noch zeigen, dass $V = \langle v_1, \ldots, v_n \rangle_K$ gilt. Sei $v \in V$ beliebig. Wäre $v \notin \langle v_1, \ldots, v_n \rangle_K$, so wäre nach Lemma 17.10 auch das $(n+1)$-Tupel $(v_1, \ldots, v_n, v)$ l.u., also auch $n + 1 \leqslant m = n$, Widerspruch. □

Beispiel 17.12. Sei $A = [a_{ij}] \in M_n(K)$. Für $j = 1, \ldots, n$ sei $v_j \in K^n$ die j-te Spalte von A, wie in Beispiel 17.9 (aber nun mit $m = n$). Mit Satz 17.11, sowie Satz 13.3 und Folgerung 15.9, erhalten wir die Äquivalenzen:

$$\begin{array}{lcllcl} \{v_1, \ldots, v_n\} \text{ Basis von } K^n & \Leftrightarrow & (v_1, \ldots, v_n) \text{ l.u.} & \Leftrightarrow & A \to I_n \\ & \Leftrightarrow & A \text{ invertierbar} & \Leftrightarrow & \det(A) \neq 0. \end{array}$$

Man erhält also alle Basen von $V = K^n$, indem man alle n-Tupel betrachtet, die durch die Spalten von invertierbaren Matrizen gegeben sind.

Die folgende Aussage sieht sehr plausibel aus — aber die präzise Begründung ist keineswegs offensichtlich. Der Beweis ist eine gute Illustration dafür, wie die obigen Sätze ineinandergreifen. Es wird praktisch alles benutzt, was wir in diesem Abschnitt gemacht haben!

Satz 17.13. *Sei V endlich erzeugt und $U \subseteq V$ ein Teilraum. Dann ist auch U endlich erzeugt. Ist $U \subsetneqq V$, so gilt $\dim U < \dim V$.*

Beweis. Da V endlich erzeugt ist, gilt $n := \dim V < \infty$; siehe Satz 17.6. Annahme, U wäre nicht endlich erzeugt. Dann ist zunächst $U \neq \{0_V\}$; sei $0 \neq v_1 \in U$. Nach Definition ist (v_1) l.u. Da U nicht endlich erzeugt ist, gilt $\langle v_1\rangle_K \subsetneqq U$ und es gibt ein $v_2 \in U$ mit $v_2 \notin \langle v_1\rangle_K$. Nach Lemma 17.10 ist (v_1, v_2) l.u. Wiederum weil U nicht endlich erzeugt ist, gilt $\langle v_1, v_2\rangle_K \subsetneqq U$ und es gibt ein $v_3 \in U$ mit $v_3 \notin \langle v_1, v_2\rangle_K$. Nach Lemma 17.10 ist (v_1, v_2, v_3) l.u. Wir wiederholen dieses Argument insgesamt $(n+1)$-mal und erhalten ein $(n+1)$-Tupel $(v_1, v_2, \ldots, v_{n+1})$, das l.u. in V ist, Widerspruch zu Satz 17.11. Also war die Annahme falsch, d.h., U ist in der Tat endlich erzeugt und damit $d := \dim U < \infty$. Sei $\{u_1, \ldots, u_d\}$ eine Basis von U. Da $(u_1, \ldots, u_d)$ l.u. in V ist, folgt wieder $d \leqslant n$ nach Satz 17.11. Und wäre $d = n$, so wäre $\{u_1, \ldots, u_d\}$ schon eine Basis von V und damit $U = V$, Widerspruch. □

Satz 17.14 (Basisergänzungssatz)**.** *Sei V endlich erzeugt und $S \subseteq V$ eine endliche Teilmenge mit $V = \langle S\rangle_K$. Gegeben seien $v_1, \ldots, v_d \in V$, so dass das Tupel $(v_1, \ldots, v_d)$ l.u. ist (mit $d \geqslant 0$). Nach Satz 17.11 ist $d \leqslant n := \dim V$. Dann gibt es $v_{d+1}, \ldots, v_n \in S$, so dass $B := \{v_1, \ldots, v_d, v_{d+1}, \ldots, v_n\}$ eine Basis von V ist.*

Beweis. Ist $d = n$, so ist $\{v_1, \ldots, v_d\}$ bereits eine Basis von V; siehe Satz 17.11. Sei nun $d < n$. Dann ist $\langle v_1, \ldots, v_d\rangle_K \subsetneqq V$, also gibt es ein $v \in S$ mit $v \notin \langle v_1, \ldots, v_d\}$. (Wäre $S \subseteq \langle v_1, \ldots, v_d\rangle_K$, so auch $V = \langle S\rangle_K \subseteq \langle v_1, \ldots, v_d\rangle_K \subsetneqq V$, Widerspruch.) Setze $v_{d+1} := v$. Nach Lemma 17.10 ist $\{v_1, \ldots, v_d, v_{d+1}\}$ ebenfalls l.u. Ist $d + 1 = n$, so sind wir fertig (wieder nach Satz 17.11). Ist $d + 1 < n$, so wiederholen wir das Argument. Nach insgesamt $n - d$ Wiederholungen finden wir $v_{d+1}, \ldots, v_n \in S$ so dass $(v_1, \ldots, v_d, v_{d+1}, \ldots, v_n)$ l.u. ist. Nochmalige Anwenung von Satz 17.11 zeigt, dass $\{v_1, \ldots, v_d, v_{d+1}, \ldots, v_n\}$ eine Basis ist. □

18. *Der Euklidische Raum* $\mathbb{R}^n$

In diesem Abschnitt betrachten wir den Standard-Vektorraum $V = \mathbb{R}^n$. Wegen der besonderen Eigenschaften von $\mathbb{R}$ ergibt sich hier die Möglichkeit, Abstände zu messen oder die "Norm" eines $x \in \mathbb{R}^n$ zu bestimmen. Damit werden wir auch einige sehr konkrete Anwendungen betrachten können. Ist zum Beispiel ein Punkt $(a, b) \in \mathbb{R} \times \mathbb{R}$ in der reellen Ebene gegeben, so ist der Abstand von (a, b) zum Ursprung $(0, 0)$ nach dem Satz von Pythagoras gegeben durch $\sqrt{a^2 + b^2}$. Für $n \geqslant 1$ beliebig definieren wir eine Abbildung

$$\langle\ ,\ \rangle \colon \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}, \qquad (x, y) \mapsto x_1y_1 + \ldots + x_ny_n,$$

wobei $x_1, \ldots, x_n \in \mathbb{R}$ die Komponenten des Spaltenvektors $x \in \mathbb{R}^n$ sind und $y_1, \ldots, y_n \in \mathbb{R}$ die Komponenten des Spaltenvektors $y \in \mathbb{R}^n$. Wir bezeichnen $\langle\ ,\ \rangle$ als ***Standard-Skalarprodukt*** auf $\mathbb{R}^n$. Es gilt $\langle x, y\rangle = \langle y, x\rangle$ für alle $x, y \in \mathbb{R}^n$. Für $x = y$ gilt

$$\langle x, x\rangle = x_1^2 + \ldots + x_n^2 \geqslant 0,$$

also können wir $\|x\| := \sqrt{\langle x, x\rangle}$ als die Norm von x definieren, auch als ***Euklidische Norm*** bezeichnet. Beachte: Hier gilt $\|x\| = 0$ nur für $x = 0_n$; man bezeichnet diese Eigenschaft auch als ***Positiv-Definitheit*** von $\langle\ ,\ \rangle$. Für $x, y \in \mathbb{R}^n$ heißt $\|x-y\|$ der ***Abstand*** zwischen x und y. Mit Hilfe der Definition des Matrixprodukts können wir $\langle\ ,\ \rangle$ auch schreiben als

$$\langle x, y\rangle = [x_1\ \ldots\ x_n] \cdot \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} = x^{tr} \cdot y \qquad \text{für alle } x, y \in \mathbb{R}^n,$$

wobei das Ergebnis eine 1×1-Matrix der Form $[a]$ mit $a \in \mathbb{R}$ ist, wofür wir nach unseren Konventionen einfach nur $a \in \mathbb{R}$ schreiben. Aus den Eigenschaften der Matrixmultiplikation folgt dann zum Beispiel die Regel:

$$\begin{aligned}\langle sx + ty, y'\rangle &= (sx + ty)^{tr} \cdot y' = (sx^{tr} + ty^{tr}) \cdot y' \\ &= s(x^{tr} \cdot y') + t(y^{tr} \cdot y') = s\langle x, y'\rangle + t\langle y, y'\rangle\end{aligned}$$

für alle $x, y, y' \in \mathbb{R}^n$ und $s, t \in \mathbb{R}$. Man darf also Skalarpodukte "ausmultiplizieren". Zum Beispiel erhält man auch folgende Formel, die oft benutzt werden wird:

$$\begin{aligned}\|sx + ty\|^2 &= \langle sx + ty, sx + ty\rangle = s\langle x, sx + ty\rangle + t\langle y, sx + ty\rangle \\ &= s^2\langle x, x\rangle + st\langle x, y\rangle + st\langle y, x\rangle + t^2\langle y, y\rangle \\ &= s^2\|x\|^2 + 2st\langle x, y\rangle + t^2\|y\|^2.\end{aligned}$$

Beispiel 18.1. (Beispiel aus der Analysis) Man kann "Skalarprodukte" auch für allgemeinere $\mathbb{R}$-Vektoräume definieren. Sei zum Beispiel $\mathcal{C}([a, b], \mathbb{R})$ der Vektorraum der stetigen Funktionen auf dem Intervall $[a, b]$ wobei $a, b \in \mathbb{R}$ und $a < b$. Wir definieren

$$\langle f, g\rangle := \int_a^b f(x)g(x)dx \qquad \text{für alle } f, g \in \mathcal{C}([a, b], \mathbb{R}).$$

Dann hat $\langle\ ,\ \rangle$ analoge Eigenschaften wie das obige Standard-Skalarprodukt auf $\mathbb{R}^n$ (was aus bekannten Aussagen über Integrale folgt; ist zum Beispiel $\langle f, f\rangle = \int_a^b f(x)^2dx = 0$, so folgt in der Tat, dass f die Null-Funktion ist; also gilt auch hier "Positiv-Definitheit".)
Solche allgemeineren Skalarprodukte werden im 2. Semester weiter studiert.

Satz 18.2 (***Cauchy–Schwarz–Ungleichung***)**.** *Sei* $\langle\ ,\ \rangle\colon \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ *wie oben definiert. Dann gilt* $\langle x, y\rangle \leqslant \sqrt{\langle x, x\rangle}\sqrt{\langle y, y\rangle} = \|x\| \cdot \|y\|$ *für alle* $x, y \in \mathbb{R}^n$*. Sind* $x, y \neq 0_n$ *und ist* y *kein Vielfaches von* x*, so ist die Ungleichung echt. Insbesondere folgt die* ***Dreiecksungleichung*** $\|x + y\| \leqslant \|x\| + \|y\|$ *für alle* $x, y \in \mathbb{R}^n$*.*

Ausgeschrieben mit den Komponenten von x und y ergibt sich also die Ungleichung

$$x_1y_1 + \ldots + x_ny_n \leqslant \sqrt{x_1^2 + \ldots + x_n^2} \cdot \sqrt{y_1^2 + \ldots + y_n^2} \qquad \text{für alle } x_i, y_j \in \mathbb{R}.$$

Beweis. Ist $x = 0_n$ oder $y = 0_n$, so gilt die Ungleichung. Sei nun $x \neq 0_n$ und $y \neq 0_n$. Ist $y = sx$ mit einem $s \in \mathbb{R}$, so gilt $\langle x, y\rangle = \langle x, sx\rangle = s\langle x, x\rangle$ und $\langle y, y\rangle = \langle sx, sx\rangle = s^2\langle x, x\rangle$;

also folgt $\langle x,y\rangle^2 = s^2\langle x,x\rangle^2 = \langle x,x\rangle\langle y,y\rangle$. Sei nun y kein Vielfaches von x; dann ist auch x kein Vielfaches von y. Mit $a := -\langle x,y\rangle/\langle y,y\rangle$ folgt also $x + ay \neq 0_n$ und dann

$$\begin{aligned}0 &< \langle y,y\rangle\langle x+ay, x+ay\rangle = \langle y,y\rangle\big(\langle x,x\rangle + 2a\langle x,y\rangle + a^2\langle y,y\rangle\big)\\ &= \langle y,y\rangle\Big(\langle x,x\rangle - 2\frac{\langle x,y\rangle}{\langle y,y\rangle}\langle x,y\rangle + \frac{\langle x,y\rangle^2}{\langle y,y\rangle^2}\langle y,y\rangle\Big)\\ &= \langle y,y\rangle\langle x,x\rangle - 2\langle x,y\rangle\langle x,y\rangle + \langle x,y\rangle^2 = \langle y,y\rangle\langle x,x\rangle - \langle x,y\rangle^2.\end{aligned}$$

Also folgt $\langle x,y\rangle < \|x\|\cdot\|y\|$. Nun zur Dreiecksungleichung. Mit der obigen Ungleichung folgt $\|x+y\|^2 = \langle x+y, x+y\rangle = \langle x,x\rangle + 2\langle x,y\rangle + \langle y,y\rangle \leqslant \|x\|^2 + 2\|x\|\cdot\|y\| + \|y\|^2 \leqslant (\|x\|+\|y\|)^2$ und damit $\|x+y\| \leqslant \|x\| + \|y\|$. □

Satz 18.3 (***Gram–Schmidt–Orthogonalisierung***)**.** *Sei $U \subseteq \mathbb{R}^n$ ein Teilraum mit $m := \dim U \geqslant 1$ und $\{v_1,\ldots,v_m\}$ eine Basis von U. Dann gibt es eine Basis $C = \{w_1,\ldots,w_m\}$ von U mit folgenden Eigenschaften:*

(a) $d_i := \|w_i\|^2 > 0$ *und* $\langle w_i, w_j\rangle = 0$ *für alle* $1 \leqslant i,j \leqslant m$ *mit* $i \neq j$*;*

(b) $w_1 = v_1$ *und* $w_k = v_k - \sum_{j=1}^{k-1} d_j^{-1}\langle v_k, w_j\rangle.w_j$ *für* $k = 2,3,\ldots,m$.

Es gilt $\langle v_1,\ldots,v_k\rangle_{\mathbb{R}} = \langle w_1,\ldots,w_k\rangle_{\mathbb{R}}$ für $1 \leqslant k \leqslant m$. Jedes $u \in U$ lässt sich auf eindeutige Weise schreiben als Linearkombination

$$u = d_1^{-1}\langle u, w_1\rangle.w_1 + d_2^{-1}\langle u, w_2\rangle.w_2 + \ldots + d_m^{-1}\langle u, w_m\rangle.w_m.$$

Beweis. (Vollständige Induktion nach m.) Für $m = 1$ gilt die Aussage mit $w_1 := v_1$. Sei nun $m > 1$ und die Aussage bereits bewiesen für Teilräume der Dimension $\leqslant m-1$. Sei $U' := \langle v_1,\ldots,v_{m-1}\rangle_{\mathbb{R}} \subseteq V$. Dann ist $\dim U' = m-1$ und nach Induktion erhalten wir eine neue Basis $\{w_1,\ldots,w_{m-1}\}$ von U', so dass (a) und (b) gelten. Außerdem ist dann $\langle v_1,\ldots,v_k\rangle_K = \langle w_1,\ldots,w_k\rangle_K$ für $1 \leqslant k \leqslant m-1$. Gemäß der Vorgabe in (b) sei

$$w_m := v_m - \sum_{j=1}^{m-1} d_j^{-1}\langle v_m, w_j\rangle.w_j \in \mathbb{R}^n.$$

Wegen $w_1,\ldots,w_{m-1} \in U' \subseteq U$ und $v_m \in U$ ist auch $w_m \in U$. Für $i \in \{1,\ldots,m-1\}$ gilt

$$\begin{aligned}\langle w_m, w_i\rangle &= \langle v_k - \sum_{j=1}^{m-1} d_j^{-1}\langle v_m, w_j\rangle.w_j, w_i\rangle = \langle v_m, w_i\rangle - \sum_{j=1}^{m-1} d_j^{-1}\langle v_m, w_j\rangle\langle w_j, w_i\rangle\\ &= \langle v_m, w_i\rangle - d_i^{-1}\langle v_m, w_i\rangle\langle w_i, w_i\rangle = \langle v_m, w_i\rangle - \langle v_m, w_i\rangle = 0.\end{aligned}$$

Wäre $w_m = 0_n$, so $0_n = v_m - \sum_{j=1}^{m-1} d_j^{-1}\langle v_m, w_j\rangle.w_j$ und damit $v_m \in \langle w_1,\ldots,w_{m-1}\rangle_{\mathbb{R}} = U' = \langle v_1,\ldots,v_{m-1}\rangle_{\mathbb{R}}$. Also gibt es $s_1,\ldots,s_{m-1} \in \mathbb{R}$ mit $s_1.v_1 + \ldots + s_{m-1}.v_{m-1} + (-1).v_m = 0_n$, Widerspruch dazu, dass $(v_1,\ldots,v_n)$ l.u. ist. Also ist $w_m \neq 0_n$ und damit auch $d_m := \langle w_m, w_m\rangle > 0$, d.h., es gilt (a).

Sei nun $u \in U$ beliebig. Es gilt $v_1 = w_1$ und $v_k = w_k + \sum_{j=1}^{k-1} d_j^{-1}\langle v_k, w_j\rangle . w_j$ für $k = 2, 3, \ldots, m$, d.h., jedes v_k ist eine Linearkombination von $w_1, \ldots, w_k$. Schreiben wir also zuerst u als Linearkombination von $v_1, \ldots, v_m$ und danach jedes v_k als Linearkombination von $w_1, \ldots, w_k$, so erhalten wir insgesamt eine Darstellung von u als Linearkombination von $w_1, \ldots, w_m$. Also ist $\{w_1, \ldots, w_m\}$ ein Erzeugendensystem von U. Seien $t_1, \ldots, t_n \in \mathbb{R}$ mit $u = t_1.w_1 + \ldots + t_n.w_n$. Wir müssen noch zeigen, dass die t_i eindeutig bestimmt und durch die obigen Formeln gegeben sind. Dazu sei $k \in \{1, 2, \ldots, n\}$ und betrachte

$$\langle u, w_k\rangle = \langle t_1.w_1 + \ldots + t_n.w_n, w_k\rangle = t_1\langle w_1, w_k\rangle + \ldots + t_n\langle w_n, w_k\rangle.$$

Auf der rechten Seite bleibt nur der Term $t_k\langle w_k, w_k\rangle$ übrig, also folgt $t_k = d_k^{-1}\langle u, w_k\rangle$. □

Definition 18.4. Sind $x, y \in \mathbb{R}^n$ und gilt $\langle x, y\rangle = 0$, so heißen x, y ***orthogonal***. Sei $U \subseteq \mathbb{R}^n$ ein Teilraum mit $1 \leqslant m := \dim U \leqslant n$ und $B = \{v_1, \ldots, v_m\}$ eine Basis von U. Dann heißt B eine ***Orthogonalbasis***, wenn $\langle v_i, v_j\rangle = 0$ für alle $i \neq j$ gilt. Ist zusätzlich noch $\|v_i\| = \sqrt{\langle v_i, v_i\rangle} = 1$ für alle i, so heißt B eine ***Orthonormalbasis*** von U.
Mit dem Gram–Schmidt–Verfahren kann man dann jede Basis $B = \{v_1, \ldots, v_m\}$ von U in eine Orthogonalbasis $C = \{w_1, \ldots, w_m\}$ überführen. Setzen wir schließlich noch $w_i' := \|w_i\|^{-1} w_i$, so gilt $\|w_i'\| = 1$ für alle i, also ist $C' = \{w_1', \ldots, w_m'\}$ eine Orthonormalbasis. Damit hat jedes $u \in U$ eine eindeutige Darstellung als $u = \langle u, w_1'\rangle.w_1' + \ldots + \langle u, w_m'\rangle.w_m'$.

Beispiel 18.5. Sei $A := \begin{bmatrix} 1 & 2 & -1 & 3 \end{bmatrix} \in \mathbb{R}^{1\times 4}$ und $U = N(A) \subseteq \mathbb{R}^4$ der Lösungsraum des homogenen LGS mit Matrix A. Die allgemeine Lösung ist

$$\begin{bmatrix} -2x_2+x_3-3x_4 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = x_2v_1 + x_3v_2 + x_4v_3 \quad \text{mit} \quad v_1 := \begin{bmatrix} -2 \\ 1 \\ 0 \\ 0 \end{bmatrix}, v_2 := \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}, v_3 := \begin{bmatrix} -3 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

und $x_2, x_3, x_4 \in \mathbb{R}$. Dann ist $U := \langle v_1, v_2, v_3\rangle_{\mathbb{R}}$ und $\dim U = 3$. Es gilt $\langle v_1, v_2\rangle = -2$, $\langle v_2, v_3\rangle = -3$, $\langle v_1, v_3\rangle = 6$, also ist $B = \{v_1, v_2, v_3\}$ noch keine Orthogonalbasis von U. Mit dem Gram–Schmidt–Verfahren erhalten wir nun in 3 Schritten:

- $w_1 := v_1 = \begin{bmatrix} -2 \\ 1 \\ 0 \\ 0 \end{bmatrix}$ und $d_1 := \|w_1\|^2 = 5$;
- $w_2 := v_2 - d_1^{-1}\langle v_2, w_1\rangle w_1 = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} - (-2)\cdot 5^{-1} \begin{bmatrix} -2 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1/5 \\ 2/5 \\ 1 \\ 0 \end{bmatrix}$ und $d_2 := \|w_2\|^2 = 6/5$;
- $w_3 := v_3 - d_1^{-1}\langle v_3, w_1\rangle w_1 - d_2^{-1}\langle v_3, w_2\rangle w_2 = \ldots = \begin{bmatrix} -1/2 \\ -1 \\ 1/2 \\ 1 \end{bmatrix}$ und $d_3 := \|w_3\|^2 = 5/2$.

Nun ist $C = \{w_1, w_2, w_3\}$ eine Orthogonalbasis von U.
Beachte auch: Um kompliziertere Nenner in den Formeln für die w_k zu vermeiden, kann man

auch in jedem Schritt des Algorithmus gleich w_k durch ein geeignetes Vielfaches ersetzen und damit weiterrechnen.

Der folgende Hilfssatz ist das entscheidende Hilfsmittel für die anschließenden Anwendungen.

Lemma 18.6. *Sei $U \subseteq \mathbb{R}^n$ ein Teilraum. Zu jedem $v \in \mathbb{R}^n$ gibt es dann $u_0 \in U$ und $v' \in \mathbb{R}^n$, so dass $v = u_0 + v'$ und $\langle u, v' \rangle = 0$ für alle $u \in U$ gilt.*

Beweis. Ist $U = \{0_n\}$, so gilt die Aussage mit $u_0 := 0_n$ und $v' := v$. Sei also nun $U \neq \{0_n\}$ und $1 \leqslant m := \dim U \leqslant n$. Sei $B = \{u_1, \ldots, u_m\}$ eine Basis von U. Mit dem Gram–Schmidt–Verfahren erhalten wir also eine Orthogonalbasis $C = \{w_1, \ldots, w_m\}$ von U. Setze nun

$$u_0 := \sum_{j=1}^{m} \frac{\langle w_j, v \rangle}{\langle w_j, w_j \rangle}.w_j \in U \qquad \text{und} \qquad v' := v - u_0 \in V.$$

Dann ist jedenfalls $v = u_0 + v'$. Sei nun $u \in U$ beliebig. Wir müssen noch zeigen, dass $\langle u, v' \rangle = 0$ gilt. Dazu: Zunächst gilt $\langle u, v' \rangle = \langle u, v - u_0 \rangle = \langle u, v \rangle - \langle u, u_0 \rangle$. Wir schreiben $u = x_1.w_1 + \ldots + x_m.w_m$ mit $x_i \in \mathbb{R}$. Dann folgt

$$\langle u, u_0 \rangle = \sum_{i=1}^{m} x_i \langle w_i, u_0 \rangle = \sum_{i=1}^{m} x_i \Big\langle w_i, \sum_{j=1}^{m} \frac{\langle w_j, v \rangle}{\langle w_j, w_j \rangle}.w_j \Big\rangle = \sum_{i=1}^{m} \sum_{j=1}^{m} x_i \langle w_j, v \rangle \frac{\langle w_i, w_j \rangle}{\langle w_j, w_j \rangle}.$$

Da $C = \{w_1, \ldots, w_m\}$ eine Orthogonalbasis ist, fallen auf der rechten Seite alle Terme mit $i \neq j$ weg. Dies ergibt $\langle u, u_0 \rangle = \sum_{i=1}^{m} x_i \langle w_i, v \rangle = \Big\langle \sum_{i=1}^{m} x_i.w_i, v \Big\rangle = \langle u, v \rangle$. Damit erhalten wir schließlich $\langle u, v' \rangle = \langle u, v \rangle - \langle u, u_0 \rangle = \langle u, v \rangle - \langle u, v \rangle = 0$, wie gewünscht. □

Beachte, dass der obige Beweis konstruktiv ist: Es wird ein konkretes Verfahren angegeben, wie man u_0 und v' bestimmt. Dies ist natürlich für die folgenden Anwendungen sehr nützlich.

Ab hier Woche 13

Beispiel 18.7 (***Gaußsche Methode der kleinsten Quadrate***)**.** Gegeben seien Messwerte (t_i, y_i) mit $t_i, y_i \in \mathbb{R}$ für $1 \leqslant i \leqslant N$, wobei zum Beispiel jedes t_i einen Zeitpunkt angibt und y_i den zur Zeit t_i erhobenen Messwert. (Um Sonderfälle zu vermeiden, nehmen wir an, dass die t_i alle verschieden sind.) Gesucht ist eine Gerade mit Gleichung $y = at + b$ (in der reellen (t, y)-Ebene), die möglichst nahe an den Punkten (t_i, y_i) vorbeiläuft. Also suche $a, b \in \mathbb{R}$ so dass der Fehler $F(a, b) := \sum_{i=1}^{N} \big(y_i - (at_i + b)\big)^2$ möglichst klein wird; dann heißt die Gerade $y = at + b$ auch ***Ausgleichsgerade***.

Lösung: Wir betrachten das Standard-Skalarprodukt $\langle\ ,\ \rangle$ auf $\mathbb{R}^N$. Setze:

$$y := \begin{bmatrix} y_1 \\ \vdots \\ y_N \end{bmatrix} \in \mathbb{R}^N \qquad \text{und} \qquad u(a, b) := \begin{bmatrix} at_1 + b \\ \vdots \\ at_N + b \end{bmatrix} \in \mathbb{R}^N \qquad \text{für } a, b \in \mathbb{R}.$$

Dann prüft man sofort nach, dass $U := \{u(a, b) \mid a, b \in \mathbb{R}\} \subseteq \mathbb{R}^N$ ein Teilraum ist, mit Basis $\{u(1, 0), u(0, 1)\}$, also $\dim U = 2$. Für $a, b \in \mathbb{R}$ ist dann $F(a, b) = \|y - u(a, b)\|^2$. Nach

Lemma 18.6 gibt es $u_0 \in U$ und $v' \in \mathbb{R}^N$ mit $y = u_0 + v'$ und $\langle u, v' \rangle = 0$ für alle $u \in U$. Seien $a_0, b_0 \in \mathbb{R}$ mit $u_0 = u(a_0, b_0)$. Für beliebige $a, b \in \mathbb{R}$ gilt dann:

$$\begin{aligned} F(a,b) &= \|y - u(a,b)\|^2 = \|y - u_0 + u_0 - u(a,b)\|^2 = \|v' + \big(u_0 - u(a,b)\big)\|^2 \\ &= \langle v' + \big(u_0 - u(a,b)\big), v' + \big(u_0 - u(a,b)\big)\rangle \\ &= \langle v', v'\rangle + 2\underbrace{\big\langle v', u_0 - u(a,b)\big\rangle}_{=0} + \underbrace{\big\langle u_0 - u(a,b), u_0 - u(a,b)\big\rangle}_{\geqslant 0} \\ &\geqslant \|v'\|^2 = \|y - u_0\|^2 = \|y - u(a_0,b_0)\|^2 = F(a_0,b_0). \end{aligned}$$

Also ist die durch $y = a_0 t + b_0$ gegebene Gerade die gesuchte Lösung. Beachte: Die Lösung ist eindeutig weil $F(a,b) > F(a_0,b_0)$ für $u(a,b) \neq u_0$ gilt. — Beispiele in den Übungen.

Allgemeiner kann man anstelle einer Ausgleichsgeraden $y = at + b$ auch eine ***Ausgleichs-Polynomfunktion*** der Form $y = a_0 + a_1 t + \ldots + a_d t^d$ suchen (wobei $d \geqslant 1$ vorgegeben ist). Die Lösung erfolgt völlig analog, wobei man anstelle des obigen 2-dimensionalen Teilraums $U \subseteq \mathbb{R}^N$ den folgenden $(d+1)$-dimensionalen Teilraum betrachtet:

$$U := \left\{ \begin{bmatrix} a_d t_1^d + a_{d-1} t_1^{d-1} + \ldots + a_1 t_1 + a_0 \\ \vdots \\ a_d t_N^d + a_{d-1} t_N^{d-1} + \ldots + a_1 t_N + a_0 \end{bmatrix} \;\middle|\; a_0, a_1, \ldots, a_d \in \mathbb{R} \right\} \subseteq \mathbb{R}^N.$$

(Unter Anderem mit dieser Methode gelang es Gauß 1801 auf spektakuläre Weise, die Bahn des Zwergplaneten Ceres vorauszuberechnen.)

Und schließlich eine Anwendung auf die Lösungen eines LGS. (Beispiele ebenfalls in den Übungen.) Beachte, dass es für ein LGS über einem beliebigen Körper im Allgemeinen nicht möglich ist, eine irgendwie eindeutig bestimmte Lösung zu finden.

Satz 18.8. *Gegeben seien $A \in \mathbb{R}^{m\times n}$ und $b \in \mathbb{R}^m$. Sei $L := \{x \in \mathbb{R}^n \mid A \cdot x = b\}$ die Lösungsmenge des zugehörigen* LGS. *Nehmen wir an, es ist $L \neq \varnothing$. Dann gibt es genau ein $x_0 \in L$ mit minimaler Norm, d.h., es gilt $\|x_0\| < \|x\|$ für alle $x \in L$ mit $x \neq x_0$.*

Beweis. Wir betrachten den Teilraum $U := N(A) = \{x \in \mathbb{R}^n \mid A \cdot x = 0_m\} \subseteq \mathbb{R}^n$. Nach Voraussetzung gibt es ein $v \in L$. Nach Lemma 18.6 gibt es $u_0 \in U$ und $x_0 \in \mathbb{R}^n$ mit $v = u_0 + x_0$ und $\langle u, x_0\rangle = 0$ für alle $u \in U$. Dann ist $A \cdot x_0 = A \cdot (v - u_0) = A \cdot v - A \cdot u_0 = b - 0_m = b$, also $x_0 \in L$. Sei nun $x \in L$ beliebig; nach Beispiel 16.5 gilt $x = x_0 + u$ mit $u \in U$. Wegen $\langle u, x_0\rangle = 0$ folgt $\|x\|^2 = \|x_0 + u\|^2 = \langle x_0 + u, x_0 + u\rangle = \langle x_0, x_0\rangle + 2\langle u, x_0\rangle + \langle u, u\rangle = \|x_0\|^2 + \|u\|^2$. Hier ist die rechte Seite $> \|x_0\|^2$ falls $u \neq 0_n$ (also $x \neq x_0$). Also ist x_0 eindeutig bestimmt durch die Bedingung, dass $\|x_0\|$ minimal ist. □

19. *Lineare Abbildungen und Matrizen*

Ist eine Matrix $A \in K^{m\times n}$ gegeben, so erhalten wir eine Abbildung $\varphi_A\colon K^n \to K^m$, indem wir $\varphi_A(x) := A \cdot x$ für alle $x \in K^n$ setzen. Man sieht sofort, dass dies eine "lineare Abbildung" ist im Sinne der folgenden allgemeinen Definition.

Definition 19.1. Seien V und W Vektorräume über dem gleichen Körper K. Eine Abbildung $\varphi\colon V \to W$ heißt ***lineare Abbildung***, wenn $\varphi(v+v') = \varphi(v) + \varphi(v')$ und $\varphi(s.v) = s.\varphi(v)$ für alle $v, v' \in V$ und $s \in K$ gilt. Wie üblich ist das Bild von φ definiert durch $\mathrm{Bild}(\varphi) := \{\varphi(v) \mid v \in V\} \subseteq W$; der ***Kern*** von φ ist definiert als $\mathrm{Kern}(\varphi) := \{v \in V \mid \varphi(v) = 0_W\} \subseteq V$.

Wie bereits erwähnt, definiert jede Matrix eine lineare Abbildung. Weitere Beispiele:

Beispiel 19.2. (a) Sei X eine nicht-leere Menge und $V := \mathrm{Abb}(X, K)$, wie in Beispiel 16.1(a). Sei $x_0 \in X$ fest. Dann definiere $\varphi\colon V \to K$ durch $\varphi(f) := f(x_0)$ "***Auswertung*** an x_0". Für $f, g \in V$ und $s \in K$ gilt $\varphi(f+g) = (f+g)(x_0) = f(x_0) + g(x_0) = \varphi(f) + \varphi(g)$ und $\varphi(s.f) = (s.f)(x_0) = sf(x_0) = s.\varphi(f)$. Also ist φ linear.

(b) Sei $V = K[X]$ der Vektorraum der Polynome in einer Unbestimmten X über K. Für $f = a_0 + a_1X + \ldots + a_nX^n \in K[X]$ beliebig definiere $D(f) := a_1 + a_2X + \ldots + na_nX^{n-1}$ (wobei $D(f) = \underline{0}$ falls $n = 0$.) Dann sieht man sofort, dass $D\colon K[X] \to K[X]$ linear ist; diese Abbildung heiß ***formale Ableitung***. Hier können Sie direkt zeigen (ohne Grenzwertbetrachtungen), dass $D(f * g) = f * D(g) + D(f) * g$ für alle $f, g \in K[X]$ gilt.

Beispiel 19.3. (Beispiel aus der Analysis.) Sei $X = [a, b] \subseteq \mathbb{R}$ ein abgeschlossenes Intervall, wobei $a, b \in \mathbb{R}$ mit $a < b$. Dann ist $\mathcal{C}([a, b]) := \{f\colon [a, b] \to \mathbb{R} \mid f \text{ stetig}\}$ ein Teilraum von $\mathrm{Abb}([a, b], \mathbb{R})$. (Dazu benötigt man die Aussage, dass Summen und skalare Vielfache von stetigen Funktionen wieder stetig sind.) Dann ist

$$\varphi\colon \mathcal{C}([a, b]) \to \mathbb{R}, \qquad f \mapsto \int_a^b f(x)\,dx,$$

eine lineare Abbildung (siehe Analysis-Vorlesung).

Lemma 19.4. *Seien $n, m \geqslant 1$ und $\varphi\colon K^n \to K^m$ linear. Dann gibt es genau eine Matrix $A \in K^{m\times n}$, so dass $\varphi(x) = A \cdot x$ für alle $x \in K^n$ gilt.*

Beweis. Sei dazu $B = \{e_1, \ldots, e_n\}$ die Standard-Basis von K^n. Für $1 \leqslant j \leqslant n$ sei $y_j := \varphi(e_j) \in K^m$. Sei $A \in K^{m\times n}$ die Matrix mit Spalten $y_1, \ldots, y_n$, d.h., es gilt $\varphi(e_j) = y_j = A \cdot e_j$ für $1 \leqslant j \leqslant n$. Sei nun $x \in K^n$ beliebig, mit Komponenten $x_1, \ldots, x_n$. Dann folgt:

$$\varphi(x) = \varphi\Big(\sum_{j=1}^n x_j e_j\Big) = \sum_{j=1}^n x_j \varphi(e_j) = \sum_{j=1}^n x_j (A \cdot e_j) = \sum_{j=1}^n A \cdot (x_j e_j) = A \cdot \Big(\sum_{j=1}^n v_j e_j\Big) = A \cdot x.$$

Ist auch $A' \in K^{m\times n}$ so, dass $\varphi(x) = A' \cdot x$ gilt für alle $v \in K^n$, so folgt $A \cdot e_j = \varphi(e_j) = A' \cdot e_j$ für $1 \leqslant j \leqslant n$, also sind alle Spalten von A und A' gleich. □

Lemma 19.5. *Sei* $\varphi\colon V \to W$ *eine lineare Abbildung. Dann gilt:*
(a) $\mathrm{Bild}(\varphi) \subseteq W$ *ist ein Teilraum und* $\mathrm{Kern}(\varphi) \subseteq V$ *ist ein Teilraum.*
(b) *Genau dann ist* φ *injektiv, wenn* $\mathrm{Kern}(\varphi) = \{0_V\}$ *gilt.*
(c) *Ist* φ *bijektiv, so ist die Umkehrabbildung* $\varphi^{-1}\colon W \to V$ *ebenfalls linear (und bijektiv). In diesem Fall heißt* φ *ein* ***Isomorphismus****.*

Beweis. (a) ist einfaches Nachrechnen; beachte: Wegen $0_V = 0.0_V$ ist $\varphi(0_V) = \varphi(0.0_V) = 0.\varphi(0_V) = 0_W$, also $0_V \in \mathrm{Kern}(\varphi)$ und $0_W \in \mathrm{Bild}(\varphi)$.
(b) Sei zuerst φ injektiv. Ist $v \in \mathrm{Kern}(\varphi)$, so gilt $\varphi(v) = 0_W$. Es gilt aber auch $\varphi(0_V) = 0_W$, also folgt $v = 0_V$. Sei umgekehrt $\mathrm{Kern}(\varphi) = \{0_V\}$. Seien $v_1, v_2 \in V$ mit $\varphi(v_1) = \varphi(v_2)$. Dann ist $\varphi(v_1 - v_2) = \varphi(v_1) - \varphi(v_2) = 0_W$, also $v_1 - v_2 \in \mathrm{Kern}(\varphi) = \{0_V\}$ und damit $v_1 = v_2$.
(c) Sei φ bijektiv und $\psi = \varphi^{-1}\colon W \to V$ die Umkehrabbildung. Seien $w_1, w_2 \in W$ und $v_1, v_2 \in V$ mit $w_1 = \varphi(v_1)$ und $w_2 = \varphi(v_2)$. Dann folgt $\psi(w_1 + w_2) = \psi\big(\varphi(v_1) + \varphi(v_2)\big) = \psi\big(\varphi(v_1+v_2)\big) = (\psi\circ\varphi)(v_1+v_2) = v_1+v_2 = \psi(w_1)+\psi(w_2)$. Analog $\psi(s.w_1) = \psi\big(s.\varphi(v_1)\big) = \psi\big(\varphi(s.v_1)\big) = (\psi \circ \varphi)(s.v_1) = s.v_1 = s.\psi(w_1)$ für alle $s \in K$. □

Lemma 19.6. *Seien* V *und* W *Vektorräume über* K. *Sei* V *endlich erzeugt,* $n = \dim V \geqslant 1$ *und* $B = \{v_1, \ldots, v_n\}$ *eine Basis von* V.
(a) *Es gilt* $\mathrm{Bild}(\varphi) = \langle \varphi(v_1), \ldots, \varphi(v_n)\rangle_K$*; insbesondere ist auch* $\mathrm{Bild}(\varphi)$ *endlich erzeugt.*
(b) *Sind* $\varphi, \psi\colon V \to W$ *linear mit* $\varphi(v_i) = \psi(v_i)$ *für* $1 \leqslant i \leqslant n$*, so gilt* $\varphi = \psi$.
(c) *Seien* $w_1, \ldots, w_n \in W$ *beliebig. Dann gibt es genau eine lineare Abbildung* $\varphi\colon V \to W$ *mit* $\varphi(v_i) = w_i$ *für* $1 \leqslant i \leqslant n$.

Beweis. (a) Ist $v \in V$ beliebig, so schreiben wir $v = s_1.v_1 + \ldots + s_n.v_n$ mit $s_i \in K$. Dann folgt $\varphi(v) = s_1.\varphi(v_1) + \ldots + s_n.\varphi(v_n)$. Damit ist die Inklusion $\mathrm{Bild}(\varphi) \subseteq \langle \varphi(v_1), \ldots, \varphi(v_n)\rangle_K$ gezeigt; die andere Inklusion ist klar.

(b) Sei $v \in V$ beliebig. Dann ist $v = s_1.v_1 + \ldots + s_n.v_n$ mit $s_i \in K$, also

$$\varphi(v) = \varphi\Big(\sum_{i=1}^{n} s_i.v_i\Big) = \sum_{i=1}^{n} s_i.\varphi(v_i) = \sum_{i=1}^{n} s_i.\psi(v_i) = \psi(v).$$

(c) Wir definieren $\varphi\colon V \to W$ wie folgt. Sei $v \in V$ beliebig. Dann gibt es eine eindeutige Darstellung $v = s_1.v_1 + \ldots + s_n.v_n$ mit $s_i \in K$. Wir setzen

$$\varphi(v) := \sum_{i=1}^{n} s_i.w_i \in W.$$

Seien $v, w \in V$, mit eindeutigen Darstellungen $v = s_1.v_1 + \ldots + s_n.v_n$ und $w = t_1.v_1 + \ldots + t_n.v_n$, wobei $s_i, t_i \in K$. Dann gilt also $\varphi(v) = \sum_{i=1}^n s_i.w_i$ und $\varphi(w) = \sum_{i=1}^n t_i.w_i$. Hieraus folgt sofort $\varphi(v+w) = \sum_{i=1}^n (s_i+t_i).w_i = \varphi(v)+\varphi(w)$ und $\varphi(s.v) = \sum_{i=1}^n s.(s_i.w_i) = s.\varphi(v)$

für $s \in K$. Also gibt es eine lineare Abbildung $\varphi\colon V \to W$ mit der gewünschten Eigenschaft. Die Eindeutigkeit ist dann klar nach (a). □

Hier ist nun eine zentrale Aussage über lineare Abbildungen.

Satz 19.7 (***Kern-Bild-Dimensionsformel***)**.** *Gegeben seien* K*-Vektorräume* V*,* W *und eine lineare Abbildung* $\varphi\colon V \to W$*. Ist* $\dim V < \infty$*, so gilt* $\dim V = \dim \operatorname{Kern}(\varphi) + \dim \operatorname{Bild}(\varphi)$.

Beweis. Da $\operatorname{Kern}(\varphi) \subseteq V$ ein Teilraum und V endlich erzeugt ist, folgt aus Satz 17.13, dass auch $\operatorname{Kern}(\varphi)$ endlich erzeugt ist und $d := \dim \operatorname{Kern}(\varphi) \leqslant n := \dim V < \infty$ gilt. Nach Lemma 19.6(a) ist auch $\operatorname{Bild}(\varphi)$ endlich erzeugt und damit $\dim \operatorname{Bild}(\varphi) < \infty$.

Ist $d = n$, so ist $V = \operatorname{Kern}(\varphi)$ (siehe noch einmal Satz 17.13), also $\varphi(v) = 0_W$ für alle $v \in V$. Damit folgt $\operatorname{Bild}(\varphi) = \{0_W\}$ und die gewünschte Dimensionsformel gilt. Sei nun $d < n$ und $\{v_1, \ldots, v_d\}$ eine Basis von $\operatorname{Kern}(\varphi)$. Nach dem Basisergänzungssatz 17.14 gibt es $v_{d+1}, \ldots, v_n \in V$, so dass $\{v_1, \ldots, v_d, v_{d+1}, \ldots, v_n\}$ eine Basis von V ist.
Behauptung: $\{\varphi(v_{d+1}), \ldots, \varphi(v_n)\}$ ist eine Basis von $\operatorname{Bild}(\varphi)$.
(Dann folgt $\dim \operatorname{Bild}(\varphi) = n - d = \dim V - \dim \operatorname{Kern}(\varphi)$ und wir sind fertig.)

Dazu: Weil $V = \langle v_1, \ldots, v_n\rangle_K$ gilt und $\varphi(v_1) = \ldots = \varphi(v_d) = 0_W$, folgt
$$\operatorname{Bild}(\varphi) = \langle \varphi(v_1), \ldots, \varphi(v_n)\rangle_K = \langle \varphi(v_{d+1}), \ldots, \varphi(v_n)\rangle_K.$$
Also ist $\{\varphi(v_{d+1}), \ldots, \varphi(v_n)\}$ ein Erzeugendensystem für $\operatorname{Bild}(\varphi)$. Wir müssen noch zeigen, dass das Tupel $\big(\varphi(v_{d+1}), \ldots, \varphi(v_n)\big)$ l.u. ist. Dazu seien $s_{d+1}, \ldots, s_n \in K$ mit
$$0_W = s_{d+1}.\varphi(v_{d+1}) + \ldots + s_n.\varphi(v_n) = \varphi\big(s_{d+1}.v_{d+1} + \ldots + s_n.v_n\big).$$
Dann ist $s_{d+1}.v_{d+1} + \ldots + s_n.v_n \in \operatorname{Kern}(\varphi)$, also gibt es $s_1, \ldots, s_d \in K$ mit
$$s_{d+1}.v_{d+1} + \ldots + s_n.v_n = s_1.v_1 + \ldots + s_n.v_d.$$
Damit erhalten wir eine Linearkombination $s_1.v_1 + \ldots + s_n.v_d - s_{d+1}.v_{d+1} - \ldots - s_n.v_n = 0_W$. Weil das Tupel $(v_1, \ldots, v_n)$ l.u. ist, folgt $s_1 = \ldots = s_n = 0$, also auch $s_{d+1} = \ldots = s_n = 0$. □

Beispiel 19.8. Seien V, W Vektorräume über K mit $\dim V < \infty$ und $\dim W < \infty$. Sei $\varphi\colon V \to W$ eine lineare Abbildung. Dann gelten folgende Aussagen:

(a) *Ist* φ *bijektiv, so gilt* $\dim V = \dim W$.

(Denn in diesem Fall ist $\operatorname{Bild}(\varphi) = W$ und $\operatorname{Kern}(\varphi) = \{0_V\}$, also folgt mit der Kern-Bild-Dimensionsformel $\dim V = \dim \operatorname{Kern}(\varphi) + \dim \operatorname{Bild}(\varphi) = \dim W$.) Ungekehrt gilt:

(b) *Ist* $\dim V = \dim W$ *so gilt:* φ *bijektiv* $\Leftrightarrow$ φ *injektiv* $\Leftrightarrow$ φ *surjektiv.*

(Denn: Ist φ bijektiv, so ist φ natürlich injektiv und surjektiv. Nun betrachte die Kern-Bild-Dimensionsformel $\dim W = \dim V = \dim \operatorname{Kern}(\varphi) + \dim \operatorname{Bild}(\varphi)$. Ist φ injektiv, so $\dim \operatorname{Kern}(\varphi) = 0$, also $\dim \operatorname{Bild}(\varphi) = \dim W$ und damit auch $W = \varphi(V)$ nach Satz 17.13. Ist φ surjektiv, so $\dim W = \dim \operatorname{Bild}(\varphi)$, also $\dim \operatorname{Kern}(\varphi) = 0$, d.h., φ auch injektiv.)

Bemerkung 19.9. Seien V_1, V_2 Vektorräume über K. Man prüft dann leicht nach, dass das kartesische Produkt $V_1 \times V_2 = \{(v_1, v_2) \mid v_1 \in V_1, v_2 \in V_2\}$ auch zu einem K-Vektorraum wird, mit Addition und skalarer Multiplikation gegeben durch

$$(v_1, v_2) + (v_1', v_2') := (v_1 + v_1', v_2 + v_2') \qquad \text{und} \qquad s.(v_1, v_2) := (s.v_1, s.v_2)$$

für $v_1, v_1' \in V_1$, $v_2, v_2' \in V_2$ und $s \in K$. (Das neutrale Element von $V_1 \times V_2$ ist $(0_{V_1}, 0_{V_2})$.)
Die beiden Projektionsabbildungen

$$\pi_1 \colon V_1 \times V_2 \to V_1, (v_1, v_2) \mapsto v_1, \qquad \text{und} \qquad \pi_2 \colon V_1 \times V_2 \to V_1, (v_1, v_2) \mapsto v_2,$$

sind linear und surjektiv. Seien nun $\dim V_1 < \infty$ und $\dim V_2 < \infty$. Ist B_1 eine Basis von V_1 und B_2 eine Basis von V_2, so sieht man leicht, dass $B := \{(b_1, 0_{V_2}) \mid b_1 \in B_1\} \cup \{(0_{V_1}, b_2) \mid b_2 \in B_2\}$ eine Basis von $V_1 \times V_2$ ist, also folgt $\dim(V_1 \times V_2) = \dim V_1 + \dim V_2$.

Satz 19.10. *Seien $U_1, U_2 \subseteq V$ endlich erzeugte Teilräume. Dann sind auch $U_1 + U_2 \subseteq V$ und $U_1 \cap U_2 \subseteq V$ endlich erzeugt und es gilt* $\dim U_1 + \dim U_2 = \dim(U_1 + U_2) + \dim(U_1 \cap U_2)$.

Beweis. Sei $W := \{(u_1 + u_2, u_1) \mid u_1 \in U_1, u_2 \in U_2\} \subseteq U_1 \times U_2$. Man sieht sofort, dass W ein Teilraum von $U_1 \times U_2$ ist. Durch Einschränkung von π_1 und π_2 auf W erhalten wir lineare Abbildungen $\pi_1' \colon W \to U_1$ und $\pi_2' \colon W \to U_2$. Wir berechnen deren Kerne und Bilder.
Es gilt $\operatorname{Kern}(\pi_2') = \operatorname{Kern}(\pi_2) \cap W = \{(u_1 + u_2, u_1) \mid u_1 = 0_V\} = \{(u_2, 0_V) \mid u_2 \in U_2\}$ und $\pi_2'(W) = U_1$. Die Abbildung $U_2 \to \operatorname{Kern}(\pi_2')$, $u_2 \mapsto (u_2, 0_V)$ ist linear und bijektiv, also $\dim \operatorname{Kern}(\pi_2') = \dim U_2$; siehe Beispiel 19.8(a). Mit dem Kern-Bild-Dimensionssatz folgt $\dim W = \dim U_1 + \dim U_2$. Andererseits ist $\pi_1'(W) = \{(u_1 + u_2 \mid u_1 \in U_1, u_2 \in U_2\} = U_1 + U_2$ und $\operatorname{Kern}(\pi_1') = \operatorname{Kern}(\pi_1) \cap W = \{(u_1 + u_2, u_1) \mid u_1 + u_2 = 0_V\}$. Nun ist die Abbildung $U_1 \cap U_2 \to \operatorname{Kern}(\pi_1')$, $u \mapsto (0_V, u)$, linear und bijektiv (wie man sofort nachrechnet). Damit folgt $\dim \operatorname{Kern}(\pi_1') = \dim(U_1 \cap U_2)$ und $\dim W = \dim(U_1 + U_2) + \dim(U_1 \cap U_2)$. □

Beispiel 19.11. Sei $U \leqslant K^n$ ein beliebiger Teilraum. Dann gibt es eine Matrix $A \in M_n(K)$ mit $U = N(A) = \{x \in K^n \mid A \cdot x = 0_n\}$.

Denn: Ist $U = \{0_V\}$, so setze $A := I_n$; ist $U = K^n$, so setze $A = 0_{n \times n}$. Sei nun $1 \leqslant d := \dim U < n$; sei $\{v_1, \ldots, v_d\}$ eine Basis von U. Mit dem Basisergänzungssatzr können wir diese zu einer Basis $B := \{v_1, \ldots, v_d, v_{d+1}, \ldots, v_n\}$ von K^n ergänzen. Mit Lemma 19.6(c) erhalten wir eine lineare Abbildung $\varphi \colon K^n \to K^n$ mit $\varphi(v_i) = 0_n$ für $1 \leqslant i \leqslant d$ und $\varphi(v_i) = v_i$ für $d + 1 \leqslant i \leqslant n$. Dann ist $U \subseteq \operatorname{Kern}(\varphi)$ und $\operatorname{Bild}(\varphi) = \langle v_{d+1}, \ldots v_n \rangle_K$ hat Dimension $n - d$. Mit der Kern-Bild-Dimensionsformel folgt $\dim \operatorname{Kern}(\varphi) = n - (n - d) = d = \dim U$; wegen $U \subseteq \operatorname{Kern}(\varphi)$ also $\operatorname{Kern}(\varphi) = U$. Nach Lemma 19.4 gibt es eine Matrix $A \in M_n(K)$ mit $\varphi(x) = A \cdot x$ für alle $x \in K^n$. Dann ist $U = \operatorname{Kern}(\varphi) = \{x \in K^n \mid A \cdot x = \varphi(x) = 0_n\}$. □

Die obigen Sätze haben einige sehr nützliche Anwendungen auf Matrizen und LGSe. Sei $A \in K^{m \times n}$ und $N(A) := \{x \in K^n \mid A \cdot x = 0_m\} \subseteq K^n$ die Lösungsmenge des homogenen LGS

mit Matrix A; nach Beispiel 16.5 ist dies ein Teilraum. Wie in Beispiel 17.9 betrachten wir nun auch den Zeilenraum $\mathrm{ZR}(A) \subseteq K^{1\times n}$ und den Spaltenraum $\mathrm{SR}(A) \subseteq K^m$. Sei wie oben $\varphi_A\colon K^n \to K^m$ die lineare Abbildung mit $\varphi_A(x) := A \cdot x$ für alle $x \in K^n$.

Lemma 19.12. *Es gilt* $\mathrm{Kern}(\varphi_A) = \mathrm{N}(A)$ *und* $\mathrm{Bild}(\varphi_A) = \mathrm{SR}(A)$. *Außerdem gilt*

$$\dim \mathrm{N}(A) = n - \dim \mathrm{SR}(A) \qquad \textit{und} \qquad \dim \mathrm{SR}(A) = \dim \mathrm{ZR}(A).$$

Beweis. Die Gleichheit $\mathrm{N}(A) = \mathrm{Kern}(\varphi_A)$ ist klar. Seien $v_1, \ldots, v_n \in K^m$ die Spalten von A, also $\mathrm{SR}(A) = \langle v_1, \ldots, v_n\rangle_K$. Sei $\{e_1, \ldots, e_n\}$ die Standardbasis von K^n (siehe Beispiel 11.7). Dann ist $\varphi_A(e_j) = A \cdot e_j = v_j$ für $1 \leqslant j \leqslant n$. Sei $x \in K^n$ beliebig mit Komponenten $x_1, \ldots, x_n \in K$. Dann ist $x = x_1e_1 + \ldots + x_ne_n$ und $A \cdot x = x_1(A \cdot e_1) + \ldots + x_n(A \cdot e_n) = x_1v_1 + \ldots + x_nv_n$. Also folgt $\mathrm{Bild}(\varphi_A) = \{A \cdot x \mid x \in K^n\} = \langle v_1, \ldots, v_n\rangle_K = \mathrm{SR}(A)$. Mit der Kern-Bild-Dimensionsformel erhalten wir

$$n = \dim V = \dim \mathrm{Kern}(\varphi_A) + \dim \mathrm{Bild}(\varphi_A) = \dim \mathrm{N}(A) + \dim \mathrm{SR}(A).$$

Sei $A \to A'$ (Gauß–Elimination), wobei A' Stufenform hat mit $r \in \{0, 1, \ldots, m\}$ Stufen und Pivots $1 \leqslant j_1 < \ldots < j_r \leqslant n$. Nach Satz 16.12 gilt $\dim \mathrm{N}(A) = n - r$. Also folgt $\dim \mathrm{SR}(A) = r$. Nach Beispiel 17.9 gilt auch $\dim \mathrm{ZR}(A) = \dim \mathrm{ZR}(A') = r$. □

Definition 19.13. Sei $A \in K^{m\times n}$ beliebig. Dann heißt $\mathrm{Rang}(A) := \dim \mathrm{SR}(A) = \dim \mathrm{ZR}(A)$ der ***Rang*** von A. (Wie bereits in Beispiel 17.9 erklärt, kann man $\dim \mathrm{ZR}(A)$ mit Hilfe des Gauß–Verfahrens effizient bestimmen.)

Bemerkung 19.14. Sei $A \in K^{m\times n}$ gegeben.
(a) Ist $m = n$, so gilt: $\mathrm{Rang}(A) = n \Leftrightarrow A$ invertierbar.
(b) Ist $B \in K^{n\times p}$, so gilt $\mathrm{Rang}(A \cdot B) \leqslant \min\{\mathrm{Rang}(A), \mathrm{Rang}(B)\}$.

Beweis. (a) Wegen $n = \dim \mathrm{N}(A) + \mathrm{Rang}(A)$ und mit Satz 13.3 folgt:
$n = \mathrm{Rang}(A) \Leftrightarrow \dim \mathrm{N}(A) = 0 \Leftrightarrow \{x \in K^n \mid A \cdot x = 0_n\} = \{0_n\} \Leftrightarrow A$ invertierbar.

(b) Sei $\varphi\colon K^n \to K^m$, $x \mapsto A \cdot x$. Dann ist $\mathrm{SR}(A) = \mathrm{Bild}(\varphi) = \{A \cdot x \mid x \in K^n\}$. Analog gilt $\mathrm{SR}(A \cdot B) = \{A \cdot (B \cdot y) \mid y \in K^p\}$. Nun ist $B \cdot y \in K^n$ für alle $y \in K^p$, also

$$\mathrm{SR}(A \cdot B) = \{(A \cdot B) \cdot y \mid y \in K^p\} \subseteq \{A \cdot x \mid x \in K^n\} = \mathrm{SR}(A),$$

d.h., $\mathrm{Rang}(A \cdot B) \leqslant \mathrm{Rang}(A)$. Andererseits gilt $\mathrm{N}(B) \subseteq \mathrm{N}(A \cdot B)$, denn ist $y \in \mathrm{N}(B)$, d.h., $B \cdot y = 0$, so folgt auch $(A \cdot B) \cdot y = 0_m$. Damit also $\dim \mathrm{N}(B) \leqslant \dim \mathrm{N}(A \cdot B)$. Mit

$$p = \dim \mathrm{N}(B) + \mathrm{Rang}(B) = \dim \mathrm{N}(A \cdot B) + \mathrm{Rang}(A \cdot B)$$

erhalten wir $\mathrm{Rang}(A \cdot B) = p - \dim \mathrm{N}(A \cdot B) \leqslant p - \dim \mathrm{N}(B) = \mathrm{Rang}(B)$. □

Schließlich erhalten wir ein Kriterium für die Lösbarkeit eines LGS mit Hilfe des Rangs:

Satz 19.15. *Sei* $A \in K^{m\times n}$ *und* $b \in K^m$. *Sei* $L := \{x \in K^n \mid A \cdot x = b\}$ *die Lösungsmenge des zugehörigen* LGS. *Dann gilt:* $L \neq \varnothing \quad \Leftrightarrow \quad b \in \mathrm{SR}(A) \quad \Leftrightarrow \quad \mathrm{Rang}(A) = \mathrm{Rang}([A \mid b])$.

Beweis. Sei wieder $\varphi_A\colon K^n \to K^m$ mit $\varphi_A(x) := A \cdot x$ für alle $x \in K^n$. Seien $v_1, \ldots, v_n \in K^m$ die Spalten von A. Nach Satz 19.12 ist $\mathrm{Bild}(\varphi_A) = \langle v_1, \ldots, v_n\rangle_K = \mathrm{SR}(A)$.

Sei zuerst $L \neq \varnothing$, so gibt es ein $x \in K^n$ mit $\varphi_A(x) = A \cdot x = b$, also $b \in \mathrm{Bild}(\varphi_A) = \mathrm{SR}(A)$. Sei nun $b \in \mathrm{SR}(A)$. Dann ist $b \in \langle v_1, \ldots, v_n\rangle_K$, also $\{v_1, \ldots, v_n, b\} \subseteq \mathrm{SR}(A)$ und damit auch $\mathrm{SR}([A \mid b]) = \langle v_1, \ldots, v_n, b\rangle_K \subseteq \mathrm{SR}(A)$. Die Inklusion $\mathrm{SR}(A) \subseteq \mathrm{SR}([A \mid b])$ ist klar nach Definition, also gilt $\mathrm{SR}(A) = \mathrm{SR}([A \mid b])$ und damit $\mathrm{Rang}(A) = \mathrm{Rang}([A \mid b])$.
Sei schließlich $\mathrm{Rang}(A) = \mathrm{Rang}([A \mid b])$. Wegen $\mathrm{SR}(A) \subseteq \mathrm{SR}([A \mid b])$ folgt $\mathrm{SR}([A \mid b]) = \mathrm{SR}(A)$ (siehe Satz 17.13), also auch $b \in \mathrm{SR}([A \mid b]) = \mathrm{SR}(A) = \mathrm{Bild}(\varphi_A)$, d.h., es gibt ein $x \in K^n$ mit $A \cdot x = \varphi_A(x) = b$. □

Ab hier Woche 14 Seien V und W Vektorräume über einem Körper K. Wir setzen

$$\mathrm{Hom}(V, W) := \{\varphi\colon V \to W \mid \ \varphi \text{ linear}\} \subseteq \mathrm{Abb}(V, W);$$

hier steht "Hom" für "***Homomorphismen***". Ist $V = W$, so schreiben wir auch $\mathrm{End}(V) := \mathrm{Hom}(V, V)$; hier steht "End" für "***Endomorphismen***".
Seien $\varphi, \psi \in \mathrm{Hom}(V, W)$ und $s \in K$. Dann definieren wir Abbildungen

$$\varphi + \psi\colon V \to W \qquad \text{und} \qquad s.\varphi\colon V \to W$$

durch $(\varphi + \psi)(v) := \varphi(v) + \psi(v)$ und $(s.\varphi)(v) := s.\varphi(v)$ für alle $v \in V$. Man rechnet dann sofort nach, dass $\varphi + \psi\colon V \to W$ und $s.\varphi\colon V \to W$ wieder linear sind, und dass mit diesen Verknüpfungen $\mathrm{Hom}(V, W)$ ein K-Vektorraum ist.

Sei von nun an $1 \leqslant n := \dim V < \infty$ und $1 \leqslant m := \dim W < \infty$. Dann haben wir auch den K-Vektorraum $K^{m\times n}$ der $m \times n$-Matrizen mit Einträgen in K. Als Nächstes beschreiben wir einen fundamentalen Zusammenhang zwischen $\mathrm{Hom}(V, W)$ und $K^{m\times n}$.

Sei $B = \{v_1, \ldots, v_n\}$ eine Basis von V und $C = \{w_1, \ldots, w_m\}$ von W. Jedes $v \in V$ können wir auf eindeutige Weise schreiben als $v = x_1.v_1 + \ldots + x_n.v_n$ mit $x_i \in K$. Dann heißt

$$M_B(v) := \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \in K^n \qquad \textbf{\textit{Koordinatenvektor}} \text{ von } v \text{ bezüglich } B.$$

Analog erhalten wir für jedes $w \in W$ den Koordinatenvektor $M_C(w) \in K^m$ bezüglich C. Sei $\varphi \in \mathrm{Hom}(V, w)$; sei $v \in V$ beliebig und $w := \varphi(v) \in W$. Die Frage ist nun, wie sich der Koordinatenvektor $M_C(w) \in K^m$ aus dem Koordinatenvektor $M_B(v) \in K^n$ berechnen lässt. Dazu: Für jedes $j \in \{1, \ldots, n\}$ schreiben wir $\varphi(v_j) \in W$ auf eindeutige Weise als

$$\varphi(v_j) = a_{1j}.w_1 + \ldots + a_{mj}.w_m = \sum_{i=1}^{m} a_{ij}.w_i \qquad \text{mit Koeffizienten } a_{ij} \in K.$$

Wir erhalten also eine Matrix $A = [a_{ij}]_{1\leqslant i\leqslant m, 1\leqslant j\leqslant n} \in K^{m\times n}$. Diese Matrix heißt ***darstellende Matrix*** von φ bezüglich der Basen B und C; sie wird mit $A = M_C^B(\varphi)$ bezeichnet. Die j-te Spalte von A ist der Koordinatenvektor $M_C\big(\varphi(v_j)\big)$.

Beachte: Die Reihenfolge der Vektoren in den Basen B und C ist wichtig. Ändert man die Reihenfolge, so ändert sich auch $M_C^B(\varphi)$ entsprechend.

Beispiel 19.16. Sei $A \in K^{m\times n}$; betrachte die lineare Abbildung $\varphi_A\colon K^n \to K^m$, $x \mapsto A \cdot x$. Sei $B = \{e_1, \dots, e_n\}$ die Standard-Basis von $V = K^n$, also $M_B(x) = x$ für $x \in K^n$. Sei auch C die Standard-Basis von $W = K^m$, also $M_C(y) = y$ für $y \in K^m$. Für $1 \leqslant j \leqslant n$ ist $M_C\big(\varphi_A(e_j)\big) = M_C(A \cdot e_j) = A \cdot e_j$ die j-te Spalte von A, also folgt $A = M_C^B(\varphi_A)$. (Jede Matrix ist die darstellende Matrix einer linearen Abbildung.)

Lemma 19.17. *Sei $v \in V$ beliebig. Dann gilt $M_C\big(\varphi(v)\big) = M_C^B(\varphi) \cdot M_B(v)$ (Produkt der Matrix $A = M_C^B(\varphi) \in K^{m\times n}$ mit dem Spaltenvektor $M_B(v) \in K^n$).*

Beweis. Sei $v \in V$ und $x := M_B(v) \in K^n$, mit Komponenten $x_1, \dots, x_n \in K$. Dann ist $v = x_1.v_1 + \ldots + x_n.v_n$ und damit

$$\varphi(v) = \varphi\Big(\sum_{j=1}^{n} x_j.v_j\Big) = \sum_{j=1}^{n} x_j.\varphi(v_j) = \sum_{j=1}^{n} x_j.\Big(\sum_{i=1}^{m} a_{ij}.w_i\Big) = \sum_{i=1}^{m}\Big(\sum_{j=1}^{n} a_{ij}x_j\Big).w_i.$$

Für jedes i ist also $y_i := \sum_{j=1}^{n} a_{ij}x_j$ die i-te Komponente von $M_B\big(\varphi(v)\big)$; die Summe auf der rechten Seite ist aber die i-te Komponente von $A \cdot x \in K^m$. □

Gehen wir also von den Vektorräumen V und W zu den Spaltenräumen K^n und K^m über, so wird die lineare Abbildung $\varphi\colon V \to W$ überführt in die Abbildung $\varphi_A\colon K^n \to K^m$, $x \mapsto A \cdot x$.

Beispiel 19.18. Sei $K = \mathbb{Q}$ und $V = \mathbb{Q}[X]_{\leqslant 3}$, wie in Beispiel 17.1(a). Wir definieren eine Abbildung $\varphi\colon V \to \mathbb{Q}^3$ durch

$$\varphi(f) := \begin{bmatrix} f(0) \\ f(-2) \\ f(1) \end{bmatrix} \in \mathbb{Q}^3 \qquad \text{für alle } f \in V.$$

Die so definierte Abbildung $\varphi\colon V \to \mathbb{Q}^3$ ist linear. (Das folgt sofort mit Beispiel 19.2(a).) Wir nehmen $B = \{1, X, X^2, X^3\}$ als Basis von $V = \mathbb{Q}[X]_{\leqslant 3}$; sei $C = \{e_1, e_2, e_3\}$ die Standardbasis von $\mathbb{Q}^3$. wir berechnen $\varphi(1)$, $\varphi(X)$, $\varphi(X^2)$, $\varphi(X^3) \in \mathbb{Q}^3$; diese Spaltenvektoren bilden dann die Matrix

$$A := M_C^B(\varphi) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & -2 & 4 & -8 \\ 1 & 1 & 1 & 1 \end{bmatrix} \in \mathbb{Q}^{3\times 4}.$$

Sei nun zum Beispiel $f = X^3 - 2X^2 + 7 \in \mathbb{Q}[X]_{\leqslant 3}$. Mit Lemma 19.17 erhalten wir:

$$\varphi(f) = M_C\big(\varphi(f)\big) = A \cdot M_C(f) = A \cdot \begin{bmatrix} 7 \\ 0 \\ -2 \\ 1 \end{bmatrix} = \begin{bmatrix} 7 \\ -9 \\ 6 \end{bmatrix}.$$

Satz 19.19. *Sei wie oben B eine Basis von V und C eine Basis von W. Dann ist die Abbildung $\Phi_C^B\colon \operatorname{Hom}(V,W) \to K^{m\times n}$, $\varphi \mapsto M_C^B(\varphi)$, linear und bijektiv (also ein Isomorphismus). Insbesondere folgt $\dim \operatorname{Hom}(V,W) = (\dim V) \cdot (\dim W) < \infty$.*

Beweis. Man rechnet sofort nach (selbst!), dass Φ_C^B linear ist. Ist $\Phi_C^B(\varphi) = 0_{m\times n}$, so folgt mit Lemma 19.17, dass $M_C(\varphi(v)) = 0_m$ gilt für alle $v \in V$. Aber dann ist $\varphi(v) = 0_W$ für alle $v \in V$, d.h., $\varphi = \underline{0}$. Also ist $\mathrm{Kern}(M_C^B) = \{\underline{0}\}$ und damit M_C^B injektiv.
Umgekehrt sei $A \in K^{m\times n}$ beliebig. Für $1 \leqslant j \leqslant n$ sei $z_j \in W$ der eindeutige Vektor, so dass $M_C(z_j) \in K^m$ die j-te Spalte von A ist. Nach Lemma 19.6(c) gibt es genau ein $\varphi \in \mathrm{Hom}(V,W)$ mit $\varphi(v_j) := z_j$ für $1 \leqslant j \leqslant n$. Nach Konstruktion ist $M_C^B(\varphi) = A$. Also ist M_C^B auch surjektiv, und damit bijektiv. Wegen $\dim(K^{m\times n}) = nm < \infty$ folgt damit $\dim \mathrm{Hom}(V,W) = \dim(K^{m\times n}) = mn$. □

Der folgende Satz liefert letztlich eine konzeptuelle Begründung dafür, dass die Multiplikation von Matrizen genau so wie in Definition 11.4 definiert wurde.

Satz 19.20. *Sei U ein K-Vektorraum mit $1 \leqslant p := \dim U < \infty$ und $\psi \in \mathrm{Hom}(U,V)$. Sei $D = \{u_1, \ldots, u_p\}$ eine Basis von U. Dann ist $\varphi \circ \psi \in \mathrm{Hom}(U,W)$ und es gilt*

$$\underbrace{M_C^D(\varphi\circ\psi)}_{m\times p} = \underbrace{M_C^B(\varphi)}_{m\times n} \cdot \underbrace{M_B^D(\psi)}_{n\times p} \qquad \textit{(Matrixprodukt).}$$

Beweis. Durch einfaches Nachrechnen sieht man, dass $\varphi\circ\psi\colon U \to W$ auch linear ist. Sei $M_C^B(\varphi) = A = [a_{ij}] \in K^{m\times n}$ und $M_B^D(\psi) = A' = [a'_{jk}] \in K^{n\times p}$. Dann gilt

$$\begin{aligned}(\varphi\circ\psi)(u_k) = \varphi\big(\psi(u_k)\big) &= \varphi\Big(\sum_{j=1}^{n} a'_{jk}.v_j\Big) = \sum_{j=1}^{n} a'_{jk}.\varphi(v_j)\\ &= \sum_{j=1}^{n} a'_{jk}.\Big(\sum_{i=1}^{m} a_{ij}.w_i\Big) = \sum_{i=1}^{m}\Big(\sum_{j=1}^{n} a_{ij}a'_{jk}\Big).w_i\end{aligned}$$

und damit $\sum_{j=1}^{n} a_{ij}a'_{jk}$ = Eintrag an der Position (i,k) von $M_C^D(\varphi\circ\psi) \in K^{m\times p}$. Aber die Summe auf der linken Seite ist genau der (i,k)-Eintrag von $A\cdot A'$. □

20. *Basiswechsel und Diagonalisierbarkeit*

In diesem Abschnitt sei stets V ein K-Vektorraum mit $1 \leqslant n := \dim V < \infty$ und $\varphi\colon V \to V$ linear, also $\varphi \in \mathrm{End}(V)$ ein Endomorphismus. Um darstellende Matrizen für φ zu bilden, ist es üblich und praktisch sinnvoll, im Definitions- und im Bildbereich die gleiche Basis zu nehmen. Ist also B eine Basis von V, so schreiben wir kurz $M_B(\varphi) := M_B^B(\varphi) \in M_n(K)$. Wählen wir eine andere Basis B' von V, so erhalten wir eine weitere Matrix $M_{B'}(\varphi) \in M_n(K)$. Frage: Wie hängen diese beiden Matrizen zusammen? Weitere Frage:

Normalformen–Problem. *Können wir eine Basis B von V finden, so dass die darstellende Matrix $A = M_B(\varphi) \in M_n(K)$ eine "möglichst einfache" Gestalt hat ?*

Was ist eine "möglichst einfache" Matrix? Dazu beachte zum Beispiel: Um zwei $n\times n$-Matrizen zu multiplizieren, braucht man im ungünstigsten Fall n^3 Multiplikationen und

$n^2(n-1)$ Additionen von Elementen im Grundkörper. Dies würde sich erheblich vereinfachen, wenn viele Einträge wenigstens einer der Matrizen, die multipliziert werden sollen, gleich 0 sind — was sicherlich eine sinnvolle Forderung für "möglichst einfach" ist.
Die allgemeine Theorie zeigt, dass man stets eine Basis B von V finden kann, so dass die darstellende Matrix $M_B(\varphi) \in M_n(K)$ höchstens $2n-1$ Einträge $\neq 0$ hat. Wir werden dies im 2. Semester ausführlich behandeln. Hier betrachten wir nur einen Spezialfall, der aber bereits für viele Anwendungen nützlich ist. Zuerst formulieren wir die obige Fragestellung in ein reines Matrixproblem um. Grundlage dafür ist der folgende Satz.

Satz 20.1 (***Basistransformation***)**.** *Sei* $\varphi \in \mathrm{End}(V)$ *und* $1 \leqslant n := \dim V < \infty$ *wie oben. Gegeben seien Basen* $B = \{v_1, \ldots, v_n\}$ *und* $B' = \{v'_1, \ldots, v'_n\}$ *von* V*. Für jedes* $j \in \{1, \ldots, n\}$ *schreiben wir* v'_j *auf eindeutige Weise als* $v'_j = \sum_{i=1}^{n} t_{ij} v_i$ *mit Koeffizienten* $t_{ij} \in K$*. Dann ist*

$$T := [t_{ij}]_{1 \leqslant i,j \leqslant n} \in M_n(K) \text{ invertierbar} \quad \text{und} \quad M_{B'}(\varphi) = T^{-1} \cdot M_B(\varphi) \cdot T.$$

Die Matrix T *heißt* ***Basiswechselmatrix****. Es gilt* $M_B(v) = T \cdot M_{B'}(v)$ *für alle* $v \in V$*.*

Beweis. Sei $\mathrm{id}_V \colon V \to V$, $v \mapsto v$, die identische Abbildung. Dann ist $T = M_B^{B'}(\mathrm{id}_V) \in M_n(K)$; analog setzen wir $T' := M_{B'}^{B}(\mathrm{id}_V) \in M_n(K)$. Mit Satz 19.20 folgt $T \cdot T' = M_B^{B'}(\mathrm{id}_V) \cdot M_{B'}^{B}(\mathrm{id}_V) = M_B^{B}(\mathrm{id}_V \circ \mathrm{id}_V) = M_B^{B}(\mathrm{id}_V)$ und die rechte Seite ist offenbar gleich I_n. Also ist T invertierbar mit $T^{-1} = T'$. Auf analoge Weise folgt

$$A \cdot T = M_B^{B}(\varphi) \cdot M_B^{B'}(\mathrm{id}_V) = M_B^{B'}(\varphi \circ \mathrm{id}_V) = M_B^{B'}(\varphi) \text{ und}$$
$$T \cdot A' = M_B^{B'}(\mathrm{id}_V) \cdot M_{B'}^{B'}(\varphi) = M_B^{B'}(\varphi \circ \mathrm{id}_V) = M_B^{B'}(\varphi).$$

Also gilt $A' = T^{-1} \cdot A \cdot T$. Sei schließlich $v \in V$. Mit Lemma 19.17 folgt $M_B(v) = M_B\big(\mathrm{id}_V(v)\big) = M_B^{B'}(\mathrm{id}_V) \cdot M_{B'}(v) = T \cdot M_{B'}(v)$. □

Sei $\varphi \in \mathrm{End}(V)$ gegeben und $A = M_B(\varphi) \in M_n(K)$ für irgendeine Basis B von V. Das Normalformen-Problem fragt dann danach, ob wir eine andere Basis B' von V finden können, so dass $A' = M_{B'}(\varphi) \in M_n(K)$ eine "möglichst einfache" Gestalt hat. Anders formuliert:

Matrix–Version des Normalformen-Problems. Gegeben sei eine Matrix $A \in M_n(K)$. Finde eine invertierbare Matrix $T \in M_n(K)$, so dass die transformierte Matrix $A' = T^{-1} \cdot A \cdot T$ (siehe Satz 20.1) eine "möglichst einfache" Gestalt hat.

Allgemein nennen wir $A, A' \in M_n(K)$ ***ähnliche Matrizen***, wenn es eine invertierbare Matrix $T \in M_n(K)$ gibt mit $A' = T^{-1} \cdot A \cdot T$. Man sieht sofort, dass dies eine Äquivalenzrelation auf $M_n(K)$ ist. Das Normalformen–Problem ist also letztlich die Frage, möglichst einfache (oder auf andere Weise ausgezeichnete) Repräsentanten dieser Äquivalenzklassen zu finden. Wir kommen nun zu dem angekündigten Spezialfall.

Definition 20.2. Sei $A \in M_n(K)$. Dann heißt A ***diagonalisierbar***, wenn es eine invertierbare Matrix $T \in M_n(K)$ gibt, so dass $A' := T^{-1} \cdot A \cdot T$ eine Diagonalmatrix ist, also

$$A' = \begin{bmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{bmatrix} \in M_n(K) \qquad \text{mit } \lambda_1, \ldots, \lambda_n \in K.$$

(Dies ist der optimale Fall einer "Normalform" und für viele Anwendungen sehr nützlich.)

Beachte: Sei $T \in M_n(K)$ invertierbar und seien $v_1, \ldots, v_n \in K^n$ die Spalten von T. Dann ist $B = \{v_1, \ldots, v_n\}$ eine Basis von K^n; siehe Beispiel 17.12. Sei $A' = T^{-1} \cdot A \cdot T$. Sei $e_j \in K^n$ der j-te Standardvektor; dann ist $v_j = T \cdot e_j$ für $1 \leqslant j \leqslant n$. Nun gilt:

$$\begin{aligned} A' \text{ Diagonalmatrix wie oben} \quad &\Leftrightarrow \quad A' \cdot e_j = \lambda_j e_j \quad \text{für } 1 \leqslant j \leqslant n. \\ &\Leftrightarrow \quad (T^{-1} \cdot A \cdot T) \cdot e_j = \lambda_j e_j \quad \text{für } 1 \leqslant j \leqslant n. \\ &\Leftrightarrow \quad A \cdot (T \cdot e_j) = \lambda_j (T \cdot e_j) \quad \text{für } 1 \leqslant j \leqslant n. \\ &\Leftrightarrow \quad A \cdot v_j = \lambda_j v_j \quad \text{für } 1 \leqslant j \leqslant n. \end{aligned}$$

Die letzte Bedingung besagt genau, dass jedes v_j ein ***Eigenvektor*** von A ist. Also gilt:

$$\boxed{A \in M_n(K) \text{ diagonalisierbar} \quad \Leftrightarrow \quad \exists \text{Basis von } K^n, \text{ die aus Eigenvektoren von } A \text{ besteht.}}$$

Definition 20.3. Sei $A \in M_n(K)$ und $\lambda \in K$. Dann setzen wir

$$E_A(\lambda) := N(A - \lambda I_n) = \{x \in K^n \mid (A - \lambda I_n) \cdot x = 0_n\} \in K^n.$$

Als Lösungsmenge eines homogenen LGS ist dies ein Teilraum von K^n. Nach Bemerkung 14.1 gilt $E_A(\lambda) \neq \{0_n\}$ genau dann, wenn λ ein Eigenwert von A ist; in diesem Fall heißt $E_A(\lambda)$ der zugehörige ***Eigenraum*** und $\dim E_A(\lambda) \geqslant 1$ die ***geometrische Vielfachheit*** von λ.

Beispiel 20.4. Sei $K = \mathbb{Q}$ und $A = \begin{bmatrix} -1 & 0 & 1 \\ 3 & 0 & -3 \\ 1 & 0 & -1 \end{bmatrix} \in M_3(\mathbb{Q})$.

Man rechnet nach, dass $A^2 = -2A$ gilt, also ist $\mu_A = X * (X + 2)$. Damit haben wir 2 Eigenwerte $\lambda_1 = 0$ und $\lambda_2 = -2$. Durch Lösen der entsprechenden LGSe erhält man die zugehörigen Eigenräume; Basen für diese Eigenräume sind wie folgt gegeben:

$$E_A(0) = \left\langle \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} \right\rangle_{\mathbb{Q}} \qquad \text{und} \qquad E_A(-2) = \left\langle \begin{bmatrix} -1 \\ 3 \\ 1 \end{bmatrix} \right\rangle_{\mathbb{Q}}.$$

Man prüft leicht nach (Gauß–Verfahren, siehe Beispiel 17.4), dass obige 3 Eigenvektoren zusammen eine Basis von $\mathbb{Q}^3$ bilden. Also ist A diagonalisierbar. Sei $T \in M_3(\mathbb{Q})$ die invertierbare Matrix, deren Spalten genau durch die 3 obigen Vektoren gegegen ist. Dann gilt

$$T^{-1}AT = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -2 \end{bmatrix} \qquad \text{wobei} \qquad T = \begin{bmatrix} 0 & 1 & -1 \\ 1 & 0 & 3 \\ 0 & 1 & 1 \end{bmatrix} \in M_3(\mathbb{Q}).$$

Lemma 20.5. *Seien $v_1, \ldots, v_r \in K^n$ ($r \geqslant 1$) Eigenvektoren von $A \in M_n(K)$, mit paarweise verschiedenen Eigenwerten $\lambda_1, \ldots, \lambda_r \in K$. Dann ist das Tupel $(v_1, \ldots, v_r)$ l.u.*

Beweis. (Vollständige Induktion nach r.) Ist $r = 1$, so ist $v_1 \neq 0_n$, also das Tupel (v_1) l.u. Sei nun $r > 1$ und die Aussage bereits für $r-1$ Eigenvektoren gezeigt. Seien $s_1, \ldots, s_r \in K$ gegegen mit $s_1v_1 + \ldots + s_rv_r = 0_n$. Wir multiplizieren diese Gleichung einserseits mit A und andererseits mit λ_r. Dies ergibt die beiden Gleichungen:

$$0_n = s_1(A \cdot v_1) + \ldots + s_r(A \cdot v_r) = s_1\lambda_1v_1 + \ldots + s_r\lambda_rv_r \quad \text{und} \quad 0_n = s_1\lambda_rv_1 + \ldots + s_r\lambda_rv_r.$$

Durch Subtraktion der ersten von der zweien Gleichung erhalten wir

$$0_n = s_1(\lambda_r - \lambda_1)v_1 + \ldots + s_{r-1}(\lambda_{r-1} - \lambda_r)v_{r-1}.$$

Nach Induktionsvoraussetzung ist das Tupel $(v_1, \ldots, v_{r-1})$ l.u., also gilt $s_i(\lambda_r - \lambda_i) = 0$ für $1 \leqslant i \leqslant r-1$. Weil die λ_i paarweise verschieden sind, folgt $s_1 = \ldots = s_{r-1} = 0$. Aber dann ist schließlich auch $s_rv_r = 0_n$ und damit $s_r = 0$. □

Satz 20.6 (1. Kriterium für Diagonalisierbarkeit)**.** *Seien $\lambda_1, \ldots, \lambda_r \in K$ die verschiedenen Eigenwerte von $A \in M_n(K)$. Gilt $\dim E_A(\lambda_1) + \ldots + \dim E_A(\lambda_r) = n$, so ist A diagonalisierbar.*

Beweis. Sei $n_i := \dim E_A(\lambda_i)$ für $1 \leqslant i \leqslant r$. Sei $B_i = \{v_1^{(i)}, \ldots, v_{n_i}^{(i)}\} \subseteq K^n$ eine Basis von $E_A(\lambda_i)$. Dann betrachte das $(n_1 + \ldots + n_r)$-Tupel

$$\big(v_1^{(1)}, \ldots, v_{n_1}^{(1)}, v_1^{(2)}, \ldots, v_{n_2}^{(2)}, \ldots, v_1^{(r)}, \ldots, v_{n_r}^{(r)}\big).$$

Seien Koeffizienten $s_j^{(i)} \in K$ gegegen mit $\sum_{i=1}^{r} \sum_{j=1}^{n_i} s_j^{(i)} v_j^{(i)} = 0_n$. Setze $w_i := \sum_{j=1}^{n_i} s_j^{(i)} v_j^{(i)}$ für $i = 1, \ldots, r$. Dann ist $w_1 + \ldots + w_r = 0_n$ und $w_i \in E_A(\lambda_i)$ für alle i. Also folgt $w_i = 0_n$ mit Lemma 20.5. Aber jedes B_i ist ebenfalls l.u., also folgt dann auch $s_i^{(j)} = 0$ für alle i, j.

Also ist obiges Tupel l.u. Nach Voraussetzung enthält es genau n Vektoren. Also ist die Menge, die durch das Tupel gegeben ist, eine Basis von K^n (siehe Satz 17.11). □

Definition 20.7. Sei $0 \neq f \in K[X]$ mit $r := \mathrm{Grad}(f) \geqslant 1$. Gibt es $c_1, \ldots, c_r \in K$ und ein $0 \neq c \in K$ mit $f = c(X - c_1) * (X - c_2) * \ldots * (X - c_r)$, so heißt f ***zerfallend***. Sind die c_i alle verschieden, so heißt f ***einfach-zerfallend***.

Sei zum Beispiel $f = X^2 + 1 \in K[X]$. Für $K = \mathbb{R}$ ist f nicht zerfallend; für $K = \mathbb{C}$ ist $f = (X + i) * (X - i)$ einfach-zerfallend. Für $K = \mathbb{F}_2$ ist $f = X^2 + \overline{1} = (X + \overline{1})^2$ zerfallend, aber nicht einfach-zerfallend. Nach dem Fundamentalsatz der Algebra sind alle nicht-konstanten Polynome in $\mathbb{C}[X]$ zerfallend.

Satz 20.8 (2. Kriterium für Diagonalisierbarkeit)**.** *Sei $A \in M_n(K)$ und $0 \neq f \in K[X]$ normiert mit $f(A) = 0_{n \times n}$ (z.B. $f = \mu_A$). Ist f einfach-zerfallend, so ist A diagonalisierbar.*

Beweis. Wegen $f(A) = 0_{n\times n}$ ist $r := \mathrm{Grad}(f) \geqslant 1$. Sei nun f einfach-zerfallend, also $f = (X-\lambda_1) * \ldots * (X-\lambda_r)$ mit paarweise verschiedenen $\lambda_1, \ldots, \lambda_r \in K$. Für $k \in \{1, \ldots, r\}$ sei $0 \neq g_k \in K[X]$ das Produkt der $r-1$ Faktoren $X-\lambda_j$ mit $j \neq k$. Dann ist $\mathrm{Grad}(g_k) = r-1$ und $f = (X-\lambda_k) * g_k = g_k * (X-\lambda_k)$ für $1 \leqslant k \leqslant r$. Beachte: Weil $\lambda_1, \ldots, \lambda_r$ paarweise verschieden sind, gilt $g_k(\lambda_k) \neq 0$ und $g_k(\lambda_j) = 0$ für $j \neq k$.

Behauptung (1): $\qquad g := g_1(\lambda_1)^{-1}g_1 + \ldots + g_r(\lambda_r)^{-1}g_r = 1.$

Dazu: Wegen $g_k(\lambda_j) = 0$ für $j \neq k$ folgt $g(\lambda_j) = 1$ für alle j. Also hat $g - 1 \in K[X]$ die r Nullstellen $\lambda_1, \ldots, \lambda_r$. Wegen $g \neq \underline{0}$ und $\mathrm{Grad}(g) \leqslant r-1$ folgt $g - 1 = \underline{0}$, also (1).

Wir setzen nun A in Polynome in $K[X]$ ein, wie in §14; insbesondere können wir also $f(A)$ und $g_k(A)$ in $M_n(K)$ bilden, wobei die Regeln in Definition 14.3 gelten.

Behauptung (2): $\qquad V_k := \{g_k(A)\cdot v \mid v \in K^n\} \subseteq E_A(\lambda_k) \quad$ für $1 \leqslant k \leqslant r$.

Dazu: Sei $v \in K^n$ und $v' := g_k(A)\cdot v \in V_k$. Wegen $f = (X-\lambda_k) * g_k$ und $f(A) = 0_{n\times n}$ folgt $0_n = f(A)\cdot v = \big((A-\lambda_k I_n)\cdot g_k(A)\big)\cdot v = (A-\lambda_k I_n)\cdot v'$, also $A\cdot v' = \lambda_k v'$, d.h., $v' \in E_A(\lambda_k)$.

Schließlich zeigen wir, dass die Menge der Eigenvektoren von A ein Erzeugendensystem von K^n ist. Dazu: Sei $v \in V$ beliebig. Nach Behauptung (1) ist $1 = a_1g_1 + \ldots + a_rg_r$ mit $a_k = g_k(\lambda_k)^{-1} \in K$ für alle k. Einsetzen von A und Multiplizieren mit v ergibt

$$v = I_n\cdot v = \big((a_1g_1 + \ldots + a_rg_r)(A)\big)\cdot v = a_1(g_1(A)\cdot v) + \ldots + a_r(g_r(A)\cdot v).$$

Nach Behauptung (2) ist $g_k(A)\cdot v \in V_k \subseteq E_A(\lambda_k)$ für $1 \leqslant k \leqslant r$. Also ist v in der Tat eine Linearkombination von Eigenvektoren von A. Aber dann gibt es auch eine Basis von K^n, die aus Eigenvektoren von A besteht (siehe Satz 17.6), also ist A diagonalisierbar. □

Beispiel 20.9. (a) Sei $K = \mathbb{C}$ und $A \in M_n(\mathbb{C})$ so, dass $A^d = I_n$ gilt für ein $d \in \mathbb{N}$. Dann ist A diagonalisierbar. Denn sei $f := X^d - 1 \in \mathbb{C}[X]$; dann ist $f(A) = 0_{n\times n}$. Nach Beispiel 10.6 sind die Nullstellen von f genau die d-ten Einheitswurzeln in $\mathbb{C}$; insbesondere ist f einfach-zerfallend. Also ist A diagonalisierbar nach Satz 20.8.

(b) Sei $\lambda \in K$ und $J_d(\lambda) := \begin{bmatrix} \lambda & 1 & 0 & \ldots & 0 \\ 0 & \lambda & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \ldots & 0 & \lambda & 1 \\ 0 & & \ldots & 0 & \lambda \end{bmatrix} \in M_n(K).$

(Obere Dreiecksmatrix mit λ auf der Diagonalen und 1 direkt über der Diagonalen; alle anderen Einträge sind 0.) Eine solche Matrix heißt λ-***Jordan–Block***. Dann kann man zeigen, dass $\mu_{J_n(\lambda)} = (X-\lambda)^n$ gilt. (Machen Sie sich dies klar im Fall $n = 2$.) Also gibt es genau einen Eigenwert, nämlich λ. Aber $J_n(\lambda) - \lambda I_n$ hat Stufenform mit $n-1$ Stufen, also ist $\mathrm{Rang}\big(J_n(\lambda) - \lambda I_n\big) = n-1$; siehe Definition 19.13. Damit ist $\dim E_{J_n(\lambda)}(\lambda) = 1$. Für $n \geqslant 2$ ist also $J_n(\lambda)$ niemals diagonalisierbar.

Ab hier Woche 15

21. *Zwei Anwendungen: Lineare Rekursionen und endliche Körper*

In diesem Abschnitt betrachten wir zwei Anwendungen. Dies wird eine gute Illustration für die Zusammenhänge zwischen den Themen sein, die wir in den letzten Kapiteln behandelt haben: Polynome, Matrizen, Vektorräume.

Wir beginnen mit ***linearen Rekursionen***, im einfachsten Fall von 2×2-Matrizen. Gegeben seien Startwerte $x_0, y_0 \in K$ sowie eine Matrix $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(K)$. Dann definieren wir zwei Folgen $(x_n)_{n\in\mathbb{N}_0}$ und $(y_n)_{n\in\mathbb{N}_0}$ rekursiv durch

$$x_{n+1} := ax_n + by_n \qquad \text{und} \qquad y_{n+1} := cx_n + dy_n \qquad \text{für } n = 0, 1, 2, \dots$$

Frage: Können wir eine geschlossene (nicht-rekursive) Formel für x_n und y_n finden? Dazu beachte, dass wir obige Formeln auch als Matrixgleichung schreiben können:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} ax_n + by_n \\ cx_n + dy_n \end{bmatrix} = A \cdot \begin{bmatrix} x_n \\ y_n \end{bmatrix} \qquad \text{für } n = 0, 1, 2, \dots$$

Dann folgt:

$$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = A^n \cdot \begin{bmatrix} x_0 \\ y_0 \end{bmatrix} \qquad \text{für } n = 0, 1, 2, \dots$$

Wir müssen also versuchen, geschlossene Formeln für die Einträge von A^n zu finden.

Satz 21.1. *Die Matrix $A \in M_2(K)$ besitze zwei Eigenwerte $\lambda_1 \neq \lambda_2$ in K. Setze*

$$A_1 := (\lambda_1 - \lambda_2)^{-1}(A - \lambda_2 I_2) \in M_2(K) \quad \textit{und} \quad A_2 := (\lambda_2 - \lambda_1)^{-1}(A - \lambda_1 I_2) \in M_2(K).$$

Dann gilt $A^n = \lambda_1^n A_1 + \lambda_2^n A_2$ für alle $n \in \mathbb{N}_0$.

Beweis. Der Trick des Beweises ist es, das Minimalpolynom $\mu_A \in K[X]$ von A zu betrachten. Setzen wir $p := a + d$ und $q := ad - bc = \det(A)$, so zeigt eine einfache Rechnung, dass $A^2 - pA + qI_2 = 0_{2\times 2}$ gilt, also folgt $\operatorname{Grad}(\mu_A) \leqslant 2$ und $\mu_A \mid X^2 - pX + q$; siehe Folgerung 14.10. Andererseits hat μ_A nach Satz 14.7 die beiden Nullstellen $\lambda_1 \neq \lambda_2$; also ist auch $\operatorname{Grad}(\mu_A) \geqslant 2$. Damit folgt $\operatorname{Grad}(\mu_A) = 2$ und $\mu_A = X^2 - pX + q = (X - \lambda_1)(X - \lambda_2)$. Ausmultiplizieren ergibt $p = \lambda_1 + \lambda_2$ und $q = \lambda_1\lambda_2$. Wir erhalten nun

$$0_{2\times 2} = \mu_A(A) = A^2 - pA + qI_2 = A^2 - (\lambda_1 + \lambda_2)A + \lambda_1\lambda_2 I_2 = \underbrace{(A - \lambda_1 I_2)}_{=(\lambda_2-\lambda_1)A_2} \cdot \underbrace{(A - \lambda_2 I_2)}_{=(\lambda_1-\lambda_2)A_1}.$$

Wegen $\lambda_1 \neq \lambda_2$ folgt hieraus $A_2 \cdot A_1 = 0_{2\times 2}$; mit einer analogen Rechnung auch $A_1 \cdot A_2 = 0_{2\times 2}$.

Nun ist $0_{2\times 2} = (\lambda_2 - \lambda_1)A_1 \cdot A_2 = A_1 \cdot (A - \lambda_1 I_2)$ und damit $A_1 \cdot A = \lambda_1 A_1$. Es folgt $A_1 \cdot A^2 = (A_1 \cdot A) \cdot A = \lambda_1(A_1 \cdot A) = \lambda_1^2 A_1$, dann $A_1 \cdot A^3 = \ldots = \lambda_1^3 A_1$ und so weiter, also $A_1 \cdot A^n = \lambda_1^n A_1$ für alle $n \in \mathbb{N}_0$. Genauso folgt aus $A_2 \cdot A_1 = 0_{2\times 2}$, dass $A_2 \cdot A^n = \lambda_2^n A_2$ für alle $n \in \mathbb{N}_0$ gilt. Aus der Definition von A_1, A_2 ergibt sich $A_1 + A_2 = (\lambda_1 - \lambda_2)^{-1}(A - \lambda_2 I_2 - A + \lambda_1 I_2) = I_2$. Also schließlich: $A^n = I_2 \cdot A^n = (A_1 + A_2) \cdot A^n = A_1 \cdot A^n + A_2 \cdot A^n = \lambda_1^n A_1 + \lambda_2^n A_2$. □

Bemerkung 21.2. Allgemeiner stellt sich die Frage, wie man effizient Potenzen einer Matrix $A \in M_n(K)$ berechnen kann, mit $n \geqslant 1$ beliebig. Nehmen wir an, A ist diagonalisierbar. Dann gibt es eine invertiebare Matrix $T \in M_n(K)$ so dass $D := T^{-1} \cdot A \cdot T$ eine Diagonalmatrix ist. Seien $d_1 \ldots, d_n \in K$ die Einträge auf der Diagonalen von D. Wegen $A = T \cdot D \cdot T^{-1}$ folgt dann sofort für alle $m \in \mathbb{N}$:

$$A^m = (T{\cdot}D{\cdot}\underbrace{T^{-1}) \cdot (T}_{=I_n}{\cdot}D{\cdot}T^{-1}) \cdots \underbrace{(T}_{=I_n}{\cdot}D{\cdot}T^{-1}) = T{\cdot}D^m{\cdot}T^{-1} = T{\cdot}\begin{bmatrix} d_1^n & & 0 \\ & \ddots & \\ 0 & & d_n^m \end{bmatrix}{\cdot}T^{-1}.$$

Dies ist eine der nützlichen Anwendungen der Diagonalisierbarkeit von Matrizen.

Beispiel 21.3. Betrachte noch einmal die ***Fibonacci–Folge*** $(f_n)_{n\in\mathbb{N}_0}$ wie in Beispiel 6.4, mit $f_0 = 0$, $f_1 = 1$ und $f_{n+1} = f_n + f_{n-1}$ für alle $n \geqslant 1$. Wie dort besprochen, erhalten wir zwei Folgen $(x_n)_{n\in\mathbb{N}_0}$ und $(y_n)_{n\in\mathbb{N}_0}$ mit $x_0 = 0$, $y_0 = 1$ sowie $y_n = x_{n+1} = x_n + x_{n-1}$ für alle $n \in \mathbb{N}$, wobei $x_n = f_n$ für alle $n \in \mathbb{N}_0$. Anders ausgedrückt:

$$x_{n+1} = y_n \qquad \text{und} \qquad y_{n+1} = x_{n+2} = x_{n+1} + x_n = x_n + y_n \qquad \text{für } n = 0, 1, 2, \ldots$$

Es liegt also eine lineare Rekursion mit der 2×2-Matrix $A = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$ vor, wobei wir $K = \mathbb{R}$ nehmen. Schreibe $A^n = \begin{bmatrix} a^{(n)} & b^{(n)} \\ c^{(n)} & d^{(n)} \end{bmatrix}$ für $n \in \mathbb{N}_0$, wobei $a^{(n)}, b^{(n)}, c^{(n)}, d^{(n)} \in \mathbb{R}$. Dann ist

$$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = A^n \cdot \begin{bmatrix} x_0 \\ y_0 \end{bmatrix} = A^n \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} b^{(n)} \\ d^{(n)} \end{bmatrix} \qquad \text{für } n = 0, 1, 2, \ldots$$

Wir wollen also eine geschlossene Formel für den $(1,2)$-Eintrag $b^{(n)} = x_n = f_n$ von A^n finden. Dazu verwende Satz 21.1. Hier ist $\mu_A = X^2 - X - 1 \in \mathbb{R}[X]$ mit den zwei Nullstellen $\lambda_1 = \frac{1}{2}(1 + \sqrt{5}) \in \mathbb{R}$ und $\lambda_2 = \frac{1}{2}(1 - \sqrt{5}) \in \mathbb{R}$; siehe Beispiel 14.6(b). Wir bilden dann die Matrizen A_1 und A_2 wie oben. Wegen $\lambda_1 - \lambda_2 = \sqrt{5}$ ist

$$A_1 = \sqrt{5}^{-1}(A - \lambda_2 I_2) = \sqrt{5}^{-1}\begin{bmatrix} * & 1 \\ * & * \end{bmatrix} \quad \text{und} \quad A_2 = -\sqrt{5}^{-1}(A - \lambda_1 I_2) = \sqrt{5}^{-1}\begin{bmatrix} * & -1 \\ * & * \end{bmatrix}.$$

Also folgt: $f_n = b^{(n)} = \sqrt{5}^{-1}\big(\lambda_1^n - \lambda_2^n\big) = \dfrac{1}{\sqrt{5}}\Big(\Big(\dfrac{1+\sqrt{5}}{2}\Big)^n - \Big(\dfrac{1-\sqrt{5}}{2}\Big)^n\Big)$ für alle $n \in \mathbb{N}_0$.

Dies ist die berühmte Formel von Moivre/Binet (um 1718/1843).

Für mehr zu linearen Rekursionen siehe §2.8 im Buch von Huppert und Willems. Der obige Satz 21.1 ist entnommen aus Abschnitt §2.3 in dem Buch:
T. Andreescu, Essential Linear Algebra with Applications, Birkhäuser, 2014.

Ab hier nicht mehr relevant für die Prüfung

Schließlich wollen wir die Frage untersuchen, ob es außer den Körpern $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ (mit p Primzahl) noch weitere Körper mit endlich vielen Elementen gibt. Solche endlichen Körper

spielen zum Beispiel in der ***Kodierungstheorie*** eine wichtige Rolle; für eine Einführung dazu siehe §3.7 im Buch von Huppert und Willems.

Sei zunächst K ein beliebiger Körper. Für $m \in \mathbb{Z}$ können wir $m \cdot 1_K \in K$ definieren (wobei 1_K das Eins-Element von K ist), mit den üblichen Konventionen; also etwa $3 \cdot 1_K = 1_K + 1_K + 1_K$, $0 \cdot 1_K = 0_K$, $(-5) \cdot 1_K = -(5 \cdot 1_K)$ usw. (wobei 0_K das Null-Element von K sei). Durch einfaches Nachrechnen zeigt man sofort die Regeln

$$(m+n) \cdot 1_K = m \cdot 1_K + n \cdot 1_K, \qquad (-m) \cdot 1_K = -(m \cdot 1_K), \qquad (mn) \cdot 1_K = (m \cdot 1_K) \cdot (n \cdot 1_K)$$

für alle $n, m \in \mathbb{Z}$. Daraus wiederum folgt, dass die Teilmenge

$$K_0 := \{m \cdot 1_K \mid m \in \mathbb{Z}\} \subseteq K$$

ein Teilring von K ist, also abgeschlossen unter Addition, Subtraktion und Multiplikation. Sei von nun an $|K| < \infty$. Dann können die Elemente $m \cdot 1_K \in K$ für $m \in \mathbb{Z}$ nicht alle verschieden sein, also gibt es $n, m \in \mathbb{Z}$ mit $n < m$ und $n \cdot 1_K = m \cdot 1_K$. Dann ist aber auch $(m-n) \cdot 1_K = m \cdot 1_K - n \cdot 1_K = 0_K$. Also ist die Menge $\{n \in \mathbb{N} \mid n \cdot 1_K = 0_K\} \subseteq \mathbb{N}$ nicht-leer. Nach Peano hat diese Menge ein kleinstes Element; sei dieses $p \in \mathbb{N}$. Diese Zahl p wird mit $p = \mathrm{char}(K)$ bezeichnet und heißt die ***Charakteristik*** von K. (Ist $|K| = \infty$ und sind die Elemente $m \cdot 1_K$ für $m \in \mathbb{Z}$ alle verschieden, so setzen wir $\mathrm{char}(K) := 0$.)

Satz 21.4. *Sei $|K| < \infty$ und $p := \mathrm{char}(K) \geqslant 1$ die Charakteristik von K, wie oben definiert. Dann ist p eine Primzahl und K_0 ist ein Körper mit p Elementen.*

Beweis. Angenommen, p wäre keine Primzahl. Dann gilt $p = nm$ mit $m, n \in \mathbb{N}$ mit $m < p$ und $n < p$. Mit Hilfe der obigen Regeln folgt $(m \cdot 1_K) \cdot (n \cdot 1_K) = (mn) \cdot 1_K = p \cdot 1_K = 0_K$. Wegen $m < p$ und $n < p$ gilt aber $m \cdot 1_K \neq 0_K$ und $n \cdot 1_K \neq 0_K$, Widerspruch zur Nullteilerfreiheit in K; siehe Lemma 7.5. Also war die Annahme falsch, d.h., p ist eine Primzahl.

Als nächstes zeigen wir $|K_0| = p$ und $K_0 = \{0 \cdot 1_K, 1 \cdot 1_K, \ldots, (p-1) \cdot 1_K\}$. Dazu: Sei $m \in \mathbb{Z}$ beliebig. Teilen mit Rest ergibt $m = qp + r$ mit $q, r \in \mathbb{Z}$ und $0 \leqslant r < p$. Mit den obigen Regeln folgt $m \cdot 1_K = (qp + r) \cdot 1_K = (q \cdot 1_K) \cdot (p \cdot 1_K) + r \cdot 1_K = (q \cdot 1_K) \cdot 0_K + r \cdot 1_K = r \cdot 1_K$. Also ist $K_0 = \{r \cdot 1_K \mid 0 \leqslant r < p\}$ und damit $|K_0| \leqslant p$. Schließlich seien $r, r' \in \mathbb{Z}$ gegeben mit $0 \leqslant r, r' < p$ und $r < r'$. Wäre $r \cdot 1_K = r' \cdot 1_K$, so folgt $(r' - r) \cdot 1_K = r' \cdot 1_K - r \cdot 1_K = 0_K$. Wegen $1 \leqslant r' - r \leqslant r' < p$ ist dies ein Widerspruch zur Minimalität von p. Also ist $|K_0| = p$.

Zum Schluss müssen wir noch zeigen, dass K_0 ein Körper ist. Wir haben bereits festgehalten, dass K_0 ein Teilring von K ist. Wegen $1_K \in K_0$ und da die Multiplikation in K kommutativ ist, ist also K_0 ein kommutativer Ring mit 1. Es bleibt zu zeigen, dass jedes $0 \neq x \in K_0$ ein Inverses bezüglich der Multiplikation in K_0 besitzt. Da K_0 abgeschlossen bezüglich der Multiplikation ist, erhalten wir eine Abbildung $f\colon K_0 \to K_0$, $y \mapsto x \cdot y$. Diese ist injektiv, denn seien $y, y' \in K_0$ mit $x \cdot y = f(y) = f(y') = x \cdot y'$. Nun existiert $x^{-1} \in K$; Multiplikation mit

x^{-1} ergibt dann $y = x^{-1} \cdot (x \cdot y) = x^{-1} \cdot (x \cdot y') = y'$, wie gewünscht. Wegen $|K_0| < \infty$ folgt mit Lemma 5.8(c), dass f automatisch bijektiv ist. Also gibt es ein $x' \in K_0$ mit $x \cdot x' = f(x') = 1_K$, d.h., x' ist das Inverse von x bezüglich der Multiplikation in K_0. □

Folgerung 21.5. *Sei* $|K| < \infty$ *und* $p := \mathrm{char}(K)$ *wie oben. Dann gilt* $|K| = p^d$ *mit* $d \in \mathbb{N}$.

Beweis. Nach Satz 21.4 ist $K_0 \subseteq K$ ein Teilkörper mit $|K_0| = p$. Wie in Beispiel 16.1(b) können wir dann K als K_0-Vektorraum auffassen. Wegen $|K| < \infty$ ist natürlich auch $d := \dim K < \infty$; sei $\{v_1, \ldots, v_d\}$ eine Basis. Dann hat jedes $x \in K$ eine eindeutige Darstellung als Linearkombination $x = s_1 v_1 + \ldots + s_d v_d$ mit $s_i \in K_0$ für $i = 1, \ldots, d$. Für jedes s_i gibt es hier genau p Möglichkeiten, also ist insgesamt $|K| = p^d$. □

Jetzt stellt sich natürlich die offensichtliche Frage, ob es auch umgekehrt zu jeder beliebigen Primzahlpotenz p^d einen endlichen Körper K mit $|K| = p^d$ gibt. Dies ist in der Tat der Fall; es gibt sogar eine explizite Konstruktion eines solchen K, die wir hier kurz beschreiben wollen. Dazu bringen wir wieder Matrizen und Polynome ins Spiel.

Sei $K[X]$ der Polynomring in der Unbestimmten X über K. Eine gegebene Matrix $A \in M_n(K)$ können wir dann in Polynome $f \in K[X]$ einsetzen; siehe Definition 14.3. Wir definieren $K[A] := \{f(A) \mid f \in K[X]\} \subseteq M_n(K)$, d.h. $K[A]$ besteht aus allen Linearkombinationen $a_0 I_n + a_1 A + a_2 A^2 + \ldots + a_m A^m$ mit $m \in \mathbb{N}_0$ und $a_0, a_1, \ldots, a_m \in K$. Man sieht sofort, dass $K[A]$ ein Teilraum von $M_n(K)$ ist, und auch ein kommutativer Ring mit 1 (bezüglich der üblichen Matrix-Multiplikation; das Eins-Element ist wieder I_n).

Lemma 21.6. *Sei* $\mu_A \in K[X]$ *das Minimalpolynom von* A. *Dann ist* $\{I_n, A, A^2, \ldots, A^{d-1}\}$ *eine Basis von* $K[A]$ *wobei* $d = \mathrm{Grad}(\mu_A)$*; insbesondere ist* $\dim K[A] = \mathrm{Grad}(\mu_A)$.

Beweis. Für $f \in K[X]$ teilen wir mit Rest (Lemma 14.8) und erhalten $f = \mu_A * h + r$ mit $h, r \in K[X]$, wobei $r = \underline{0}$ oder $r \neq \underline{0}$ und $\mathrm{Grad}(r) < \mathrm{Grad}(\mu_A)$. Es folgt $f(A) = (\mu_A * h + r)(A) = \mu_A(A) \cdot h(A) + r(A) = 0_{n \times n} \cdot h(A) + r(A) = r(A)$. Jedes Element von $K[A]$ ist also eine Linearkombination von $I_n, A, A^2, \ldots, A^{d-1}$, wobei $d := \mathrm{Grad}(\mu_A)$. Das Tupel $(I_n, A, A^2, \ldots, A^{d-1})$ ist l.u., denn sonst gäbe es nach Lemma 17.5 ein $j \in \{0, 1, \ldots, d-1\}$ mit $A^j \in \langle I_n, A, A^2, \ldots, A^{j-1} \rangle_K$, Widerspruch zur Definition von μ_A. □

Beispiel 21.7. Als Spezialfall der obigen Konstruktion erhalten wir ein Matrix-Modell der komplexen Zahlen. Betrachten wir dazu $K = \mathbb{R}$ und die Matrix $J := \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \in M_2(\mathbb{R})$, mit $\mu_J = X^2 + 1 \in \mathbb{R}[X]$, wie man sofort nachrechnet. Dann ist

$$\mathbb{R}[J] = \langle I_2, J \rangle_{\mathbb{R}} = \{ aI_2 + bJ \mid a, b \in \mathbb{R} \} = \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \;\middle|\; a, b \in \mathbb{R} \right\}.$$

Nun ist $\mathbb{R}[J]$ nicht nur ein kommutativer Ring mit 1, sondern sogar ein Körper, wobei J die Rolle von $i \in \mathbb{C}$ mit $i^2 = -1$ spielt. Dazu beachte: Ist $a \neq 0$ oder $b \neq 0$, so folgt

$$\det\left(\begin{bmatrix} a & -b \\ b & a \end{bmatrix}\right) = a^2 + b^2 > 0 \qquad \text{und} \qquad \begin{bmatrix} a & -b \\ b & a \end{bmatrix}^{-1} = (a^2+b^2)^{-1} \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in \mathbb{R}[J].$$

Anstelle der Konstruktion in §10 könnte man $\mathbb{C}$ auch als $\mathbb{R}[J]$ *definieren*, und dann $\mathbb{R}$ als Teilmenge von $\mathbb{C} = \mathbb{R}[J]$ auffassen, indem man $a \in \mathbb{R}$ mit der Matrix $aI_2 \in \mathbb{R}[J]$ identifiziert.

Wie können wir das obige Beispiel auch auf andere Situationen übetragen? Dazu bemerken wir, dass das Polynom $\mu_J = X^2 + 1 \in \mathbb{R}[X]$ irreduzibel ist im folgenden Sinn:

Definition 21.8. Sei $f \in K[X]$ mit $f \neq \underline{0}$ und $\mathrm{Grad}(f) \geqslant 1$. Wir sagen dass f ***reduzibel*** ist, wenn es ein Polynom $\underline{0} \neq g \in K[X]$ gibt mit $g \mid f$ und $1 \leqslant \mathrm{Grad}(g) < \mathrm{Grad}(f)$. Andernfalls heißt f ***irreduzibel***.

Sei $\underline{0} \neq f \in K[X]$. Ist $f = X - c$ mit $c \in K$, so ist f offensichtlich irreduzibel. Sei nun $\mathrm{Grad}(f) \geqslant 2$. Ist f irreduzibel, so kann f keine Nullstelle in K haben. Denn sonst würde gelten $f = (X-c) * g$, wobei $c \in K$ und $\underline{0} \neq g \in K[X]$ mit $\mathrm{Grad}(g) = \mathrm{Grad}(f) - 1 \geqslant 1$; siehe Bemerkung 9.10. Um ein Polynom vom Grad 2 oder 3 auf Irreduzibilität zu testen, genügt es also zu zeigen, dass f keine Nullstellen in K hat. Im Allgemeinen ist es ein schwieriges Problem zu zeigen, dass ein Polynom irreduzibel ist oder nicht (so ähnlich wie es für große natürliche Zahlen schwierig ist zu zeigen, dass sie Primzahlen sind oder nicht). Solche Fragestellungen werden in einer Algebra-Vorlesung weiter untersucht. Es gilt nun:

Satz 21.9. *Sei $A \in M_n(K)$ so, dass das Minimalpolynom $\mu_A \in K[X]$ irreduzibel ist. Dann ist $K[A]$ ein Körper. Insbesondere: Ist $K = \mathbb{F}_p$ mit einer Primzahl p und $d := \mathrm{Grad}(\mu_A) \geqslant 1$, so ist $\mathbb{F}_p[A]$ ein Körper mit p^d Elementen.*

Beweis. Sei $\alpha \in K[A]$. Dann gilt $\alpha = g(A)$, wobei $g = a_0 + a_1 X + \ldots + a_{d-1}X^{d-1}$ mit $a_i \in K$; siehe Lemma 21.6. Sei nun $\alpha \neq 0$; also auch $g \neq \underline{0}$. Wir wenden den erweiterten Euklidischen Algorithmus in Bemerkung 14.9 auf g und μ_A an. Damit erhalten wir Polynome $c, f, h \in K[X]$ mit $c = f * g + h * \mu_A$ und so, dass $c \neq \underline{0}$ ein gemeinsamer Teiler von g und μ_A ist.

Da μ_A irreduzibel ist und $c \mid \mu_A$ gilt, folgt $\mathrm{Grad}(c) = 0$ oder $\mathrm{Grad}(c) = \mathrm{Grad}(\mu_A) = d$. Letzteres ist aber unmöglich wegen $c \mid g$ und damit $\mathrm{Grad}(c) \leqslant \mathrm{Grad}(g) \leqslant d - 1$. Also ist $\mathrm{Grad}(c) = 0$, d.h., $0 \neq c \in K$. Einsetzen von A in $c = f * g + h * \mu_A$ ergibt $cI_n = f(A) \cdot g(A) + h(A) \cdot \mu_A(A) = f(A) \cdot g(A)$, also ist $\alpha = g(A)$ invertierbar mit $\alpha^{-1} = c^{-1} f(A)$.

Sei schließlich $K = \mathbb{F}_p$. Nach Lemma 21.6 lässt sich jedes $\alpha \in \mathbb{F}_p[A]$ auf eindeutige Weise schreiben als $\alpha = a_0 I_n + a_1 A + \ldots + a_{d-1}A^{d-1}$ mit $a_i \in \mathbb{F}_p$. Für jeden Koeffizienten a_i haben wir genau p Möglichkeiten, also folgt insgesamt $|\mathbb{F}_p[A]| = p^d$. □

Damit haben wir jetzt eine allgemeine Erklärung für Beispiel 21.7: Weil $\mu_J = X^2 + 1 \in \mathbb{R}[X]$ irreduzibel ist, muss $\mathbb{R}[J]$ ein Körper sein.

Kommen wir schließlich zu unserer Ausgangsfrage zurück, ob es zu jeder Primzahl $p \in \mathbb{N}$ und jedem $d \in \mathbb{N}$ einen Körper mit p^d Elementen gibt. Wir wollen Satz 21.9 mit $K = \mathbb{F}_p$ anwenden. Dann stellen sich noch zwei Fragen:

(1) Gibt es zu jedem $d \in \mathbb{N}$ ein normiertes irreduzibles $f \in \mathbb{F}_p[X]$ mit $\mathrm{Grad}(f) = d$?

(2) Angenommen, f sei wie in (1). Gibt es dann auch eine Matrix $A \in M_n(\mathbb{F}_p)$ mit $\mu_A = f$?

Frage (2) hat eine ganz allgemeine Antwort. Sei K beliebiger Körper, $d \in \mathbb{N}$ und $f \in K[X]$ ein beliebiges normiertes Polynom mit $\mathrm{Grad}(f) = d$; also $f = a_0 + a_1X + \ldots + a_dX^d \in K[X]$ mit $a_d = 1$. Dann ist die (Frobenius-)***Begleitmatrix*** zu f definiert als

$$A_f := \begin{bmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & \ldots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & -a_{d-1} \end{bmatrix} \in M_d(K)$$

Ist $\{e_1, \ldots, e_d\}$ die Standardbasis von K^d, so gilt also

$(*)$ $\quad A_f \cdot e_d = -(a_0e_1 + a_1e_2 + \ldots + a_{d-1}e_d) \quad$ und $\quad A_f \cdot e_i = e_{i+1}$ für $1 \leqslant i \leqslant d-1$.

Lemma 21.10. *Es gilt $\mu_{A_f} = f$, d.h., jedes normierte Polynom vom Grad $d \geqslant 1$ in $K[X]$ ist Minimalpolynom einer Matrix in $M_n(K)$.*

Beweis. Ist $d = 1$, so ist $f = X + a_0$ also $A_f = [-a_0]$. In diesem Fall ist also klar, dass $\mu_{A_f} = X + a_0 = f$ gilt. Sei nun $d \geqslant 2$. Aus $(*)$ erhält man $A_fe_1 = e_2$, $A_f^2e_1 = A_f(A_fe_1) = A_fe_2 = e_3$, $A_f^3 = A_f(A_f^2e_1) = A_fe_3 = e_4$ und so weiter, d.h., $A_f^ie_1 = e_{i+1}$ für $1 \leqslant i \leqslant d-1$. Sei nun

$$\mu_{A_f} = b_0 + b_1X + \ldots + b_{m-1}X^{m-1} + X^m \in K[X] \quad \text{mit } m \geqslant 1 \text{ und } b_i \in K.$$

Wäre $m < d$, so $0_d = \mu_{A_f}(A_f) \cdot e_1 = b_0e_1 + b_1(A_f \cdot e_1) + \ldots + b_{m-1}(A_f^{m-1} \cdot e_1) + (A_f^m \cdot e_1) = b_0e_1 + b_1e_2 + \ldots + b_{m-1}e_m + e_{m+1}$. Aber die rechte Seite ist ein Spaltenvektor in K^d mit Eintrag 1 in der $(m+1)$-ten Komponente, Widerspruch. Also ist $m \geqslant d$.
Jetzt genügt es nach Satz 14.5 zu zeigen, dass $f(A_f) = 0_{d\times d}$ gilt. Dazu zeigen wir, dass alle Spalten von $f(A_f)$ gleich 0_n sind, d.h., es gilt $f(A_f) \cdot e_i = 0$ für $1 \leqslant i \leqslant d$.
Für $i = 1$ ist $f(A_f) \cdot e_1 = a_0(A_f^0 \cdot e_1) + a_1(A_f^1 \cdot e_1) + \ldots + a_{d-1}(A_f^{d-1} \cdot e_1) + (A_f^d \cdot e_1) = a_0e_1 + a_1e_2 + \ldots + a_{d-1}e_d + A_fe_d = 0_d$, siehe $(*)$. Für $2 \leqslant i \leqslant d$ ist $e_i = A_f^{i-1} \cdot e_1$, und damit $f(A_f) \cdot e_i = \big(f(A_f) \cdot A_f^{i-1}\big) \cdot e_1 = (f * X^{i-1})(A_f) \cdot e_1 = (X^{i-1} * f)(A_f) \cdot e_1 = A_f^{i-1} \cdot \big(f(A_f) \cdot e_1\big) = 0_d$. $\square$

Frage (1) hat ebenfalls eine allgemeine Antwort: Diese ist stets JA. Für den Beweis kann man zum Beispiel ein Zählargument benutzen. Für jedes $d \in \mathbb{N}$ und jede Primzahl $p \in \mathbb{N}$ sei $N_d(p) \geqslant 0$ die Anzahl der normierten irreduziblen Polynome $f \in \mathbb{F}_p[X]$ mit $\mathrm{Grad}(f) = d$.

(Hier ist zunächst $N_d(p) = 0$ erlaubt.) Insgesamt gibt es p^d normierte Polynome in $\mathbb{F}_p[X]$ mit Grad d; also ist auch $N_d(p) \leqslant p^d$. Dann kann man die viel genauere Formel zeigen:

$$p^d = \sum_{d'} d' N_{d'}(p) \qquad \big(\text{Summe über alle } d' \in \{1, \dots, d\} \text{ mit } d' \mid d\big).$$

(Es gibt viele Beweise für diese Formel, die bereits voraussetzen, dass es endliche Körper mit p^d Elementen gibt. Ein Beweis, der dies nicht voraussetzt, ist zum Beispiel zu finden in §23.9 im Buch von Biggs.)

Diese Formel zeigt zunächst $d' N_{d'}(p) \leqslant p^{d'}$ für alle $d' \geqslant 1$. Sei $\alpha := \sum_{d'} d' N_d(p)$, wobei die Summe nur über alle $d' \in \{1, \dots, d-1\}$ mit $d' \mid d$ läuft; dann ist $p^d = d N_d(p) + \alpha$. Andererseits erhalten wir mit Hilfe der Formel für die geometrische Reihe die Abschätzung

$$\alpha \leqslant \sum_{d'=0}^{d-1} d' N_{d'}(p) \leqslant \sum_{d'=0}^{d-1} p^{d'} = \frac{p^d - 1}{p - 1} \leqslant p^d - 1 < p^d,$$

Es folgt $d N_d(p) = p^d - \alpha > 0$ und damit $N_d(p) > 0$: Es muss also normierte irreduzible Polynome in $\mathbb{F}_p[X]$ mit Grad d geben! Man kann diese finden, indem man nach Teilern von $X^{p^d} - X \in \mathbb{F}_p[X]$ sucht. (Diese Aussage ist Bestandteil des Beweises der obigen Formel).

Beispiel 21.11. (a) Sei $p = 2$ und $d = 2$. Dann erhalten wir die Faktorisierung $X^{2^2} - X = X(X^3 - \bar{1}) = X(X - \bar{1})(X^2 + X + \bar{1})$, und $f_0 = X^2 + X + \bar{1} \in \mathbb{F}_2[X]$ ist irreduzibel (keine Nullstelle in $\mathbb{F}_2$). Ein endlicher Körper mit 4 Elementen ist also gegeben durch $K := \mathbb{F}_2[A_{f_0}]$. Konkret:

$$K = \left\{ \begin{bmatrix} \bar{0} & \bar{0} \\ \bar{0} & \bar{0} \end{bmatrix}, \begin{bmatrix} \bar{1} & \bar{0} \\ \bar{0} & \bar{1} \end{bmatrix}, \begin{bmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{1} \end{bmatrix}, \begin{bmatrix} \bar{1} & \bar{1} \\ \bar{1} & \bar{0} \end{bmatrix} \right\} \subseteq M_2(\mathbb{F}_2) \quad \text{wobei} \quad A_{f_0} = \begin{bmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{1} \end{bmatrix}.$$

(b) Sei $p = 2$ und $d = 3$. Man berechnet die Faktorisierung

$X^{2^3} - X = X(X^7 - \bar{1}) = X(X + \bar{1})(X^3 + X + \bar{1})(X^3 + X^2 + \bar{1})$. Die beiden Faktoren vom Grad 3 sind irreduzibel, weil sie keine Nullstellen in $\mathbb{F}_2$ haben. Wir können also einen endlichen Körper mit 8 Elementen bilden als $K = \mathbb{F}_2[A_f]$, wobei $f \in \{X^3 + X + \bar{1}, X^3 + X^2 + \bar{1}\}$. Hier sind

$$A_{X^3+X+\bar{1}} = \begin{bmatrix} \bar{0} & \bar{0} & \bar{1} \\ \bar{1} & \bar{0} & \bar{1} \\ \bar{0} & \bar{1} & \bar{0} \end{bmatrix} \qquad \text{und} \qquad A_{X^3+X^2+\bar{1}} = \begin{bmatrix} \bar{0} & \bar{0} & \bar{1} \\ \bar{1} & \bar{0} & \bar{0} \\ \bar{0} & \bar{1} & \bar{1} \end{bmatrix}.$$

(c) Sei $p = 3$ und $d = 2$. Dann ist

$X^{3^2} - X = X(X^8 - \bar{1}) = X(X^4 - \bar{1})(X^4 + \bar{1}) = X(X - \bar{1})(X + \bar{1})(X^2 + \bar{1})(X^4 + \bar{1}) \in \mathbb{F}_3[X]$.
Hier ist $X^2 + 1$ irreduzibel (keine Nullstellen in $\mathbb{F}_3$). Außerdem stellt man fest, dass $X^4 + \bar{1} = (X^2 + X - \bar{1})(X^2 - X - \bar{1})$ gilt, wobei $X^2 + X - \bar{1}$ und $X^2 - X - \bar{1}$ irreduzibel sind (wiederum keine Nullstellen in $\mathbb{F}_3$). Wir können also einen endlichen Körper mit 9 Elementen bilden als $K = \mathbb{F}_3[A_f]$, wobei $f \in \{X^2 + \bar{1}, X^2 + X - \bar{1}, X^2 - X - \bar{1}\}$. Hier sind

$$A_{X^2+\bar{1}} = \begin{bmatrix} \bar{0} & -\bar{1} \\ \bar{1} & \bar{0} \end{bmatrix}, \qquad A_{X^2+X-\bar{1}} = \begin{bmatrix} \bar{0} & \bar{1} \\ \bar{1} & -\bar{1} \end{bmatrix} \qquad \text{und} \qquad A_{X^2-X-\bar{1}} = \begin{bmatrix} \bar{0} & \bar{1} \\ \bar{1} & \bar{1} \end{bmatrix}.$$