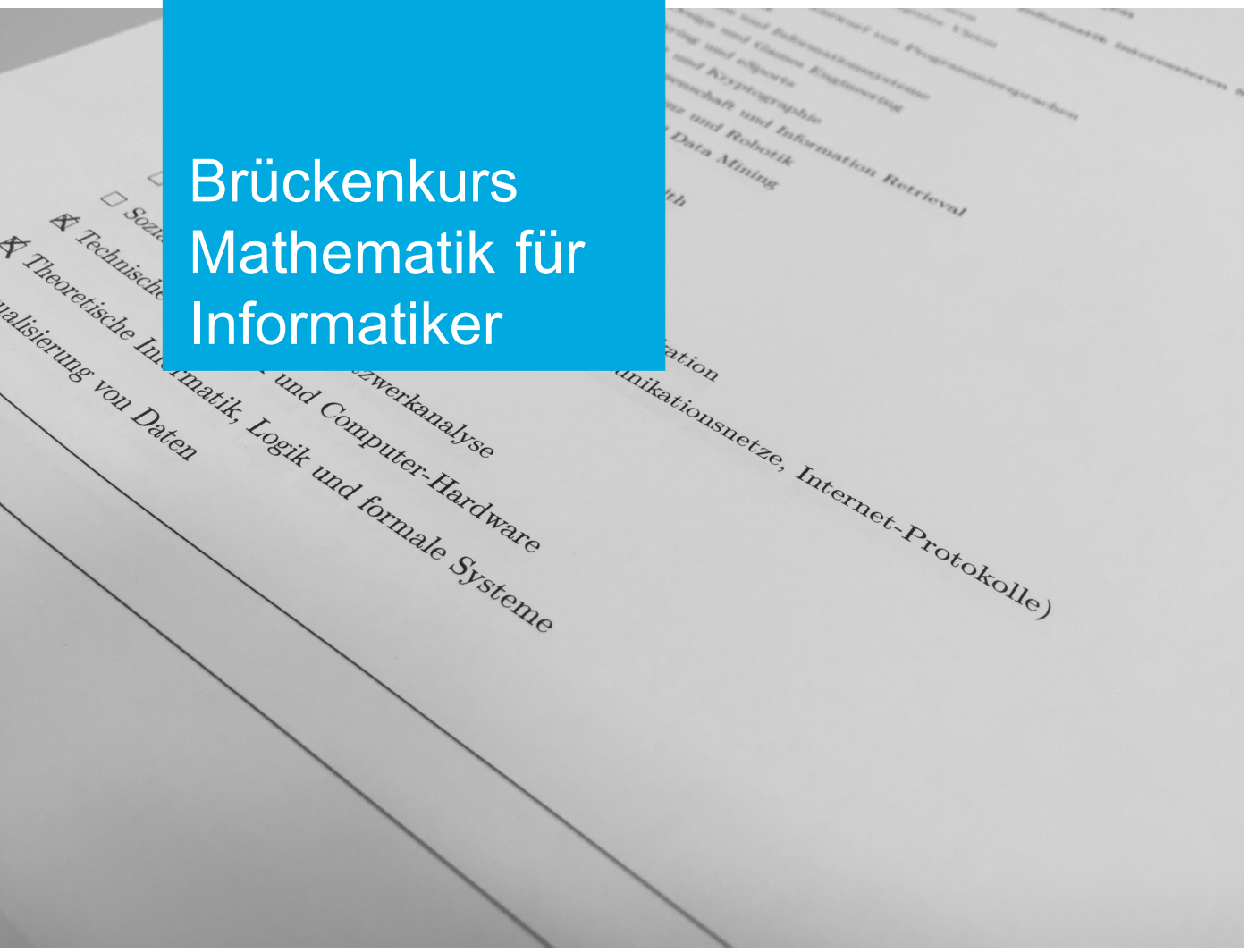
toc.uni.kn

Universität Konstanz

02.11.18

Brückenkurs Mathematik für Informatiker



Sven Kosub

Vorlesungsskriptum für das Wintersemester 2018/19 – Version: 1.0

Inhaltsverzeichnis

1 Arithmetik

1.1 Zahlenbereiche

Natürliche Zahlen

Mit $\mathbb{N}$ bezeichnen wir die Menge der natürlichen Zahlen: $0, 1, 2, 3, \ldots$ Die natürliche Zahl a ist dabei eine Abkürzung für $\underbrace{1 + 1 + \cdots + 1}_{a-\text{mal}}$; a^n ist eine Abkürzung für $\underbrace{a \cdot a \cdot \ldots \cdot a}_{a-\text{mal}}$. 0 ist eine natürliche Zahl. (In der Mathematik wird sehr häufig 0 nicht als natürliche Zahl aufgefasst; wenn 0 zu den natürlichen Zahlen gezählt werden soll, wird $\mathbb{N}_0$ verwendet.) Wird 0 als natürliche Zahl ausgeschlossen, so schreiben wir $\mathbb{N}_+$. (In der Mathematik wird dann $\mathbb{N}$ verwendet.)

Rechenregeln: Es seien k, n, m beliebige natürliche Zahlen.

1. $(k + n) + m = k + (n + m)$ — Assoziativgesetze
   $(k \cdot n) \cdot m \quad = k \cdot (n \cdot m)$
2. $k \cdot (n + m) \;=\; k \cdot n + k \cdot m$ — Distributivgesetz
3. $n + m = m + n$ — Kommutativgesetze
   $n \cdot m \;\; = m \cdot n$
4. $n + 0 = n$ — neutrale Elemente
   $n \cdot 1 \;\; = n$
5. $n \cdot 0 = 0$

Aus diesen Rechenregeln und den oben eingeführten Abkürzungen lassen sich leicht die Potenzrechenregeln herleiten (für alle natürlichen Zahlen a, b, n, m):

1. $a^n \cdot a^m = a^{n+m}$
2. $(a^n)^m = a^{n \cdot m}$
3. $a^n \cdot b^n = (a \cdot b)^n$

Insbesondere legt die 4. Regel nahe, dass die Definition $a^0 =_{\text{def}} 1$ für alle natürlichen Zahlen a vernünftig ist, um mit den Potenzen in natürlicher Weise rechnen zu können.

Ganze Zahlen

Mit $\mathbb{Z}$ bezeichnen wir die Menge der ganzen Zahlen: $\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$ Die ganzen Zahlen ermöglichen es, alle Subtraktionen stets ausführen zu können, z.B. $3 - 5 = -2$. Die Zahl $-a$ (mit der natürlichen Zahl a) ist dabei eine Abkürzung für $\underbrace{(-1) + (-1) + \ldots + (-1)}_{a-\text{mal}} = a \cdot (-1)$.

Rechenregeln:

1.–5. übertragen sich von den natürlichen Zahlen

6. $n + (-n) = 0$ für alle natürlichen Zahlen n — inverses Element

Eine Spezialfall für das Rechnen mit ganzen Zahlen ist die Vorzeichenregel: Wieso ist die Regel $(-1) \cdot (-1) = 1$ plausibel? – Mit Hilfe der Rechenregeln erhalten wir:

$$\begin{aligned} 0 &= (-1) \cdot 0 && \text{(5. Regel)} \\ &= (-1) \cdot (1 + (-1)) && \text{(6. Regel, inverses Element)} \\ &= (-1) \cdot 1 + (-1) \cdot (-1) && \text{(2. Regel, Distributivgesetz)} \\ &= -1 + (-1) \cdot (-1) && \text{(4. Regel, neutrales Element)} \end{aligned}$$

Somit folgt weiter:

$$\begin{aligned} 1 &= 1 + 0 && \text{(4. Regel, neutrales Element)} \\ &= 1 + (-1) + (-1) \cdot (-1) && \text{(siehe oben)} \\ &= 0 + (-1) \cdot (-1) && \text{(6. Regel, inverses Element)} \\ &= (-1) \cdot (-1) && \text{(4. Regel, neutrales Element)} \end{aligned}$$

Die Vorzeichenregel hängt wesentlich mit dem Distributivgesetz zusammen, das auch für alle ganzen Zahlen gelten soll.

Rationale Zahlen

Mit $\mathbb{Q}$ bezeichnen wir die Menge der rationalen Zahlen, d.h. die Menge der Brüche $\frac{p}{q}$ mit $q \neq 0$ sowie p, q ganze Zahlen. Die rationalen Zahlen ermöglichen es, jede lineare Gleichung $q \cdot x - p = 0$ stets zu lösen. Zur Definition der rationalen Zahlen genügt es auch zu fordern:

1. p ist ganze Zahl und q ist natürliche Zahl, $q \neq 0$
2. p ist natürliche Zahl und q ist ganze Zahl, $q \neq 0$

Eine alternative Darstellungsform rationaler Zahlen ist die Dezimalschreibweise:

- $\frac{1}{2} = 0,5$ (Periodenlänge 0)
- $\frac{1}{3} = 0,333\ldots = 0,\overline{3}$ (Periodenlänge 1)
- $\frac{1}{7} = 0,\overline{142857}$ (Periodenlänge 6)
- $\frac{1}{30} = 0,0\overline{3}$ (schließlich periodisch)

Beachte: Die Dezimalschreibweise ist nicht eindeutig. Zum Beispiel gilt $1 = 0,\overline{9}$, denn

$$\begin{aligned} x &= 0,\overline{9} \\ 10x &= 9,\overline{9} \end{aligned}$$

Somit gilt $9x = 10x - x = 9,\overline{9} - 0,\overline{9} = 9$, d.h. $x = 1$.

Rechenregeln:

1.–6. übertragen sich von den ganzen Zahlen

7. $\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = 1$ für $p \neq 0, q \neq 0$ — inverses Element

Als Schreibweise verwenden wir: $\left(\frac{p}{q}\right)^{-1} = \frac{1}{\frac{p}{q}} =_{\text{def}} \frac{q}{p}$.

Reelle Zahlen

Mit $\mathbb{R}$ bezeichnen wir die Menge aller *reellen* Zahlen, d.h., die Menge der endlichen und unendlichen Dezimalzahlen. Beispielhaft seien folgende reelle Zahlen erwähnt:

1. Jede rationale Zahl ist reell; r ist rational genau dann, wenn r eine schließlich periodische Darstellung besitzt
2. $\pi = 3,141592\ldots$ ist irrational und transzendent
3. $e = 2,7182818\ldots$ ist irrational und transzendent
4. $\sqrt{2} = 1,41421356\ldots$ ist irrational und algebraisch
5. Irrationalität von $\pi + e$ ist offen

Rechenregeln:

1.–7. übertragen sich von den rationalen Zahlen (mit $r \cdot \frac{1}{r} = 1$ für $r \neq 0$ bei der 7. Regel)

Insbesondere lässt sich in den reellen Zahlen die Gleichung $a^x = b$ für alle positiven natürlichen Zahlen lösen, und wir definieren:

$$\log_a b =_{\text{def}} x$$

Es gilt also $a^{\log_a b} = b$. Aus den Potenzrechenregeln ergeben sich somit die Rechenregeln für den Logarithmus:

1. $\log_a(b \cdot c) = \log_a b + \log_a c$
2. $\log_a b^c = c \cdot \log_a b$
3. $\log_a c = \dfrac{\log_b c}{\log_b a}$

Reelle Zahlen können in natürlicher Weise angeordnet werden. Dies wird durch die folgenden Anordnungsaxiome beschrieben (für beliebige reellen Zahlen a, b, c):

1. Es gilt entweder $a = b$, $a < b$ oder $a > b$ — Trichotomie
2. Ist $a < b$ und ist $b < c$, so ist $a < c$ — Transitivität
3. Ist $a < b$, so ist $a + c < b + c$ — Monotonie der Addition
4. Ist $a < b$ und ist $0 < c$, so ist $a \cdot c < b \cdot c$ — Monotonie der Multiplikation

Komplexe Zahlen

Mit $\mathbb{C}$ bezeichnen wir die Menge der komplexen Zahlen, d.h. die Mengen der Zahlenpaare (a, b), wobei a und b reelle Zahlen sind, mit den folgenden Operationen:

1. Addition auf $\mathbb{C}$: $\quad (a, b) + (c, d) =_{\text{def}} (a + c, b + d)$
2. Multiplikation auf $\mathbb{C}$: $\quad (a, b) \cdot (c, d) =_{\text{def}} (ac - bd, ad + bc)$

Eine alternative und die übliche Schreibweise für komplexe Zahlen ist mit $i =_{\text{def}} (0, 1)$:

$$(a, b) = a + b \cdot i$$

Hierbei steht i für die imaginäre Einheit: $i = \sqrt{-1}$. Damit gilt

$$i^1 = i, \quad i^2 = -1, \quad i^3 = -i \quad \text{sowie} \quad i^4 = 1$$

Ist $z = a + b \cdot i$, so sind $\text{Re}(z)$ der Realteil von z und $\text{Im}(z)$ der Imaginärteil von z. Eine komplexe Zahl z heißt reell, falls $\text{Im}(z) = 0$ gilt; z heißt imaginär, falls $\text{Re}(z) = 0$.

Rechenregeln:

1.–7. übertragen sich von den rellen Zahlen

Für die komplexen Zahlen lassen sich einige bemerkenswerte Gleichungen formulieren:

1. $\sqrt{i} = \frac{1}{2} \cdot \sqrt{2}(1+i)$
2. $e^{i\pi} = -1$
3. $i^i = e^{-\frac{\pi}{2}}$

1.2 Primzahlen

Es seien n und m ganze Zahlen. Dann teilt m die Zahl n (symbolisch $m|n$), falls es eine ganze Zahl k gibt mit

$$n = k \cdot m.$$

Bei dieser Definition ist zu beachten, dass jede Zahl 0 teilt.

Eine Zahl n heißt Primzahl, falls 1 und n die einzigen natürlichen Zahlen sind, die n teilen. Die ersten Primzahlen sind somit: $1, 2, 3, 5, 7, 11, 13, 17, \ldots$, wobei 1 üblicherweise nicht zu den Primzahlen gezählt wird.

Theorem 1.1

Es sei n eine natürliche Zahl, $n \geq 2$. Dann gibt es eindeutig bestimmte Primzahlen $2 \leq p_1 < p_2 < \ldots < p_k$ und positive natürliche Zahlen $a_1, a_2, \ldots, a_k$ mit

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k}.$$

Bevor wir das Theorem beweisen, wollen wir es an einigen Beispielen verdeutlichen.

Beispiele: Die folgenden Zahlenbeispiele illustrieren das Konzept der Primzahlzerlegung (mit den zugehörigen Parametern nach obigem Theorem):

- $24 = 2 \cdot 12 = 2^3 \cdot 3^1 \quad (k = 2,\ p_1 = 2,\ p_2 = 3,\ a_1 = 3, a_2 = 1)$
- $36 = 2^2 \cdot 3^2 \quad (k = 2,\ p_1 = 2,\ p_2 = 3,\ a_1 = 2, a_2 = 2)$
- $111 = 3^1 \cdot 37^1 \quad (k = 2,\ p_1 = 3,\ p_2 = 37,\ a_1 = 1, a_2 = 1)$
- $113 = 113^1 \quad (k = 1,\ p_1 = 113,\ a_1 = 1)$
- $120 = 5 \cdot 24 = 2^3 \cdot 3^1 \cdot 5^1 \quad (k = 3,\ p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ a_1 = 3,\ a_2 = 1,\ a_3 = 1)$

Beweis: Wir beweisen die Aussage in zwei Schritten:

1. Existenz: Es sei $n \geq 2$ eine natürliche Zahl. Dann gibt es zwei Fälle:
   - Ist n eine Primzahl, dann sind wir fertig.

- Ist n keine Primzahl, dann gibt es natürliche Zahlen $n_1, n_2 \geq 2$ mit $n = n_1 \cdot n_2$. Für n_1 und n_2 können wir nun wieder die gleichen Überlegungen anstellen, d.h., sind $n_1 = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k}$ sowie $n_2 = q_1^{b_1} \cdot q_2^{b_2} \cdot \ldots \cdot q_m^{b_m}$ Primzahlzerlegungen, so gilt

$$n = n_1 \cdot n_2 = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k} \cdot q_1^{b_1} \cdot q_2^{b_2} \cdot \ldots \cdot q_m^{b_m}.$$

  Durch Zusammenfassen gleicher Faktoren erhalten wir die gewünschte Zerlegung. Da stets $n > n_1, n_2$ gilt, bricht das Verfahren nach endlich vielen Schritten ab.

Somit existiert eine Primzahlzerlegung stets.

2. Eindeutigkeit: Es seien für $n \geq 2$ zwei Zerlegungen gegeben:

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k} = q_1^{b_1} \cdot q_2^{b_2} \cdot \ldots \cdot q_m^{b_m}.$$

   Wir betrachten die kleinste als Faktor vorkommende Primzahl. Ohne Beeinträchtigung der Allgemeinheit sei dies p_1. Dann teilt p_1 sowohl die linke als auch die rechte Zerlegung. Somit gibt es ein j mit $p_1 | q_j$. Da q_j eine Primzahl ist, gilt $p_1 = q_j$. Dividieren wir also beide Primzahlzerlegungen durch p_1, so erhalten wir zwei Primzahlzerlegungen mit einem Faktor weniger. Diese Argumentation können wir wiederholen, bis auf einer Seite keine Faktoren mehr übrig sind. Dann sind aber auch auf der anderen Seite keine Faktoren übrig. Somit kommen alle Faktoren auf der linken Seite als Faktoren auf der rechten Seite vor und auch umgekehrt.

Damit ist das Theorem bewiesen. ■

1.3 Divisionsreste

Es seien n eine ganze Zahl, m eine natürliche Zahl, $m \geq 2$. Dann teilt m die Zahl n mit Rest r, $0 \leq r \leq m-1$, falls eine ganze Zahl k existiert mit

$$n = k \cdot m + r.$$

Die in der Definition vorkommende Zahlen k und r sind eindeutig, denn aus $k \cdot m + r = k' \cdot m + r'$ folgt

$$0 \leq |k \cdot m - k' \cdot m| = |k - k'| \cdot m = |r' - r| \leq m - 1,$$

somit $|k - k'| = 0$ und folglich $k = k'$ und $r = r'$. Damit definieren wir die Modulo-Funktion für zwei Argumente n und m:

$$\mathrm{mod}(n, m) = r \quad \Longleftrightarrow_{\mathrm{def}} \quad m \text{ teilt } n \text{ mit Rest } r$$

Beispiele: Wir bestimmen die Werte der Modulo-Funktion für verschiedene Argumente:

- $\mathrm{mod}(7, 3) = 1$, denn $7 = 2 \cdot 3 + 1$
- $\mathrm{mod}(-7, 3) = 2$, denn $-7 = (-3) \cdot 3 + 2$
- $\mathrm{mod}(9, 3) = 0$, denn $9 = 3 \cdot 3$
- $\mathrm{mod}(-9, 3) = 0$, denn $-9 = (-3) \cdot 3$

Das folgende Theorem, das wir ohne Beweis angeben, fasst wichtige Rechenregeln für Divisionsreste zusammen.

Theorem 1.2

Es seien k, n und m ganze Zahlen, $m \geq 2$.

1. $\text{mod}(k + n, m) = \text{mod}(\text{mod}(k, m) + \text{mod}(n, m))$
2. $\text{mod}(k \cdot n, m) = \text{mod}(\text{mod}(k, m) \cdot \text{mod}(n, m))$
3. $\text{mod}(n^k, m) = \text{mod}(\text{mod}(n, m)^k, m)$

Beispiele: Die ersten drei Beispiele veranschaulichen die Korrektheit der drei Rechenregeln aus Theorem 1.2:

$$\begin{aligned}
\text{mod}(5+7,4) &= \text{mod}(\text{mod}(5,4)+\text{mod}(7,4),4)\\
&= \text{mod}(1+3,4)\\
&= 0\\
&= \text{mod}(12,4)
\end{aligned}$$

$$\begin{aligned}
\text{mod}(5\cdot 7,4) &= \text{mod}(\text{mod}(5,4)\cdot\text{mod}(7,4),4)\\
&= \text{mod}(1\cdot 3,4)\\
&= 3\\
&= \text{mod}(35,4)
\end{aligned}$$

$$\begin{aligned}
\text{mod}(5^7,4) &= \text{mod}(\text{mod}(5,4)^7,4)\\
&= \text{mod}(1^7,4)\\
&= 1\\
&= \text{mod}(78125,4)
\end{aligned}$$

Die Rechenregeln können verwendet werden, um Divisionsreste komplexer Ausdrücke zu bestimmen, ohne diese explizit auszurechnen:

$$\begin{aligned}
&\text{mod}\left(13^{73}\cdot 17^{25}+(-2)^{113},4\right)\\
&= \text{mod}\left(\text{mod}(13,4)^{73}\cdot\text{mod}(17,4)^{25}+\text{mod}\left((-2)^2,4\right)^5 6\cdot\text{mod}(-2,4),4\right)\\
&= \text{mod}\left(1^{73}\cdot 1^{25}+0,4\right)\\
&= 1
\end{aligned}$$

Wie finden wir die in der Definition der Teilbarkeit von n durch m mit Rest r angegegebene Zahl k, für die $n = k \cdot m + r$ gilt? Dazu verwenden wir Rundungsregeln, die durch Gaußklammern ausgedrckt werden. Für eine beliebige reelle Zahl x definieren wir:

$$\begin{aligned}
\lfloor x \rfloor &=_{\text{def}} \text{ größte ganze Zahl } z \text{ mit } z \leq x\\
\lceil x \rceil &=_{\text{def}} \text{ kleinste ganze Zahl } z \text{ mit } z \geq x
\end{aligned}$$

Die untere Gaußklammer $\lfloor x \rfloor$ bewirkt, dass die Zahl x auf die nächst kleinere ganze Zahl abgerundet wird; mit der oberen Klammer $\lceil x \rceil$ wird x zur nächst größeren ganzen Zahl aufgerundet.

Beispiele: Einige Zahlbeispiele verdeutlichen die Rundungsregeln:

$$\left\lfloor \frac{3}{2} \right\rfloor = 1, \quad \left\lceil \frac{3}{2} \right\rceil = 2, \quad \left\lfloor \frac{-3}{2} \right\rfloor = -2, \quad \left\lceil \frac{-3}{2} \right\rceil = -1$$

Mit Hilfe der Gaußklammern kann die Modulo-Funktion wie folgt dargestellt werden (ohne dass auf ein geeignetes k referenziert werden muss):

$$n = \left\lfloor \frac{n}{m} \right\rfloor \cdot m + \mathrm{mod}(n, m)$$

für ganze Zahlen n und m mit $m \geq 2$. Dies ist leicht einzusehen: Für $r = \mathrm{mod}(n, m)$ gibt es ein k mit $n = k \cdot m + r$. Also gilt wegen $r < m$

$$\left\lfloor \frac{n}{m} \right\rfloor = \left\lfloor k + \frac{r}{m} \right\rfloor = k$$

Proposition 1.3

Für jede ganze Zahl n gilt $\left\lfloor \frac{n}{2} \right\rfloor + \left\lceil \frac{n}{2} \right\rceil = n$.

Beweis: (Fallunterscheidung) Es sei n eine ganze Zahl.

- 1. Fall: n ist gerade, d.h., es gilt $n = 2k$ für eine ganze Zahl k. Dann gilt

$$\left\lfloor \frac{n}{2} \right\rfloor + \left\lceil \frac{n}{2} \right\rceil = \left\lfloor \frac{2k}{2} \right\rfloor + \left\lceil \frac{2k}{2} \right\rceil = \lfloor k \rfloor + \lceil k \rceil = 2k = n.$$

- 2. Fall: n ist ungerade, d.h., es gilt $n = 2k + 1$ für eine ganze Zahl k. Dann gilt

$$\left\lfloor \frac{n}{2} \right\rfloor + \left\lceil \frac{n}{2} \right\rceil = \left\lfloor \frac{2k+1}{2} \right\rfloor + \left\lceil \frac{2k+1}{2} \right\rceil = \left\lfloor k + \frac{1}{2} \right\rfloor + \left\lceil k + \frac{1}{2} \right\rceil = k + (k+1) = 2k + 1 = n.$$

Damit ist die Proposition bewiesen. ■

1.4 Algorithmus von Euklid

Definition 1.4

Es seien n und m positive natürliche Zahlen.

1. Das kleinste gemeinsame Vielfache von n und m, symbolisch $\mathrm{kgV}(n, m)$, ist die kleinste natürliche Zahl k, sodass n und m jeweils k teilen.
2. Der größte gemeinsame Teiler von n und m, symbolisch $\mathrm{ggT}(n, m)$, ist die größte natürliche Zahl k, sodass k jeweils n und m teilt.

Beispiele: Einige Zahlbeispiele verdeutlichen die Begriffsbildung:

- $\mathrm{kgV}(3,5) = 15$ und $\mathrm{ggT}(3,5) = 1$
- $\mathrm{kgV}(3,6) = 6$ und $\mathrm{ggT}(3,6) = 3$
- $\mathrm{kgV}(4,6) = 12$ und $\mathrm{ggT}(4,6) = 2$

Der Standardweg, um das kleinste gemeinsame Vielfache und den größten gemeinsamen Teiler von $n$und m zu bestimmen, geht über die Primzahlzerlegungen von n und m, die wir uns in folgendem Lemma in geeigneter Weise zurechtlegen.

Lemma 1.5

Es seien n und m positive natürliche Zahlen mit den Primfaktordarstellungen $n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ \cdots \ \cdot p_k^{a_k}$ und $m = p_1^{b_1} \cdot p_2^{b_2} \cdot \ \cdots \ \cdot p_k^{b_k}$, wobei $a_i = 0$ bzw. $b_i = 0$, falls n bzw. m nicht durch p_i teilbar ist. Es gelte weiterhin $b_k > 0$ oder $a_k > 0$. Dann gelten folgende Gleichungen:

$$\begin{aligned} \mathrm{kgV}(n,m) &= p_1^{\max(a_1,b_1)} \cdot p_2^{\max(a_2,b_2)} \cdot \ \cdots \ \cdot p_k^{\max(a_k,b_k)} \\ \mathrm{ggT}(n,m) &= p_1^{\min(a_1,b_1)} \cdot p_2^{\min(a_2,b_2)} \cdot \ \cdots \ \cdot p_k^{\min(a_k,b_k)} \end{aligned}$$

Beweis: (nur erste Gleichung) Es seien n und m mit den Primfaktordarstellungen wie oben beschrieben gegeben. Es sei $x =_{\mathrm{def}} p_1^{\max(a_1,b_1)} \cdot p_2^{\max(a_2,b_2)} \cdot \ \cdots \ \cdot p_k^{\max(a_k,b_k)}$. Dann teilen die Primfaktoren $p_i^{a_i}$ von n und $p_i^{b_i}$ von m jeweils $p_i^{\max(a_i,b_i)}$. Mithin teilen n und m die Zahl x. Jede weitere Zahl y, die von n und m geteilt wird, muss durch die Promfaktoren $p_i^{a_i}$ und $p_i^{b_i}$ teilbar sein, also auch durch $p_i^{\max(a_i,b_i)}$. Damit teilt x die Zahl y. Also gilt $x \leq y$. Folglich gilt $\mathrm{kgV}(n,m) = x$ und das Lemma ist bewiesen. ■

Beispiele: Mit den Primfaktordarstellungen $120 = 2^3 \cdot 3^1 \cdot 5^1$ und $36 = 2^2 \cdot 3^2 \cdot 5^0$ gilt

$$\mathrm{kgV}(120,36) = 2^3 \cdot 3^2 \cdot 5^1 = 360 \quad \text{sowie} \quad \mathrm{ggT}(120,36) = 2^2 \cdot 3^1 \cdot 5^0 = 12.$$

Theorem 1.6

Es seien n und m positive natürliche Zahlen. Dann gilt:

$$n \cdot m = \mathrm{kgV}(n,m) \cdot \mathrm{ggT}(n,m)$$

Beweis: Es seien $n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ \cdots \ \cdot p_k^{a_k}$ und $mn = p_1^{b_1} \cdot p_2^{b_2} \cdot \ \cdots \ \cdot p_k^{b_k}$ die Primfaktordastellungen von n und m wie in Lemma 1.5 beschrieben. Dann folgt nach Lemma 1.5:

$$\begin{aligned} &\mathrm{kgV}(n,m) \cdot \mathrm{ggT}(n,m) \\ &= p_1^{\max(a_1,b_1)} \cdot p_2^{\max(a_2,b_2)} \cdot \ \cdots \ \cdot p_k^{\max(a_k,b_k)} \cdot p_1^{\min(a_1,b_1)} \cdot p_2^{\min(a_2,b_2)} \cdot \ \cdots \ \cdot p_k^{\min(a_k,b_k)} \\ &= p_1^{\max(a_1,b_1)+\min(a_1,b_1)} \cdot p_2^{\max(a_2,b_2)+\min(a_2,b_2)} \cdot \ \cdots \ \cdot p_k^{\max(a_k,b_k)+\min(a_k,b_k)} \\ &= p_1^{a_1+b_1} \cdot p_2^{a_2+b_2} \cdot \ \cdots \ \cdot p_k^{a_k+b_k} \\ &= p_1^{a_1} \cdot p_2^{a_2} \cdot \ \cdots \ \cdot p_k^{a_k} \cdot p_1^{b_1} \cdot p_2^{b_2} \cdot \ \cdots \ \cdot p_k^{b_k} \\ &= n \cdot m \end{aligned}$$

Algorithmus: Euklid
Eingabe: positive natürliche Zahl n, m mit $n \geq m$
Augsabe: $\mathrm{ggT}(n, m)$

```
[1]   if m teilt n then
[2]      return m
[3]   else
[4]      return Euklid(mod(n, m), m)
```

Abbildung 1 Algorithmus von Euklid

Damit ist das Theorem bewiesen. ■

Korollar 1.7

Es seien n und m positive natürliche Zahlen. Dann gilt:

$$\mathrm{kgV}(n, m) = \frac{n \cdot m}{\mathrm{ggT}(n, m)} \quad \text{bzw.} \quad \mathrm{ggT}(n, m) = \frac{n \cdot m}{\mathrm{kgV}(n, m)}$$

Wie bestimmen wir $\mathrm{ggT}(n, m)$? Sin die Primfaktorzerlegungen von n und m bekannt, so gibt uns Lemma 1.5 eine einfache Möglichkeit dafür an die Hand. Allerdings ist die Bestimmung von Primfaktorzerlegungen algorithmisch nicht einfach. Einen eleganten Ausweg, der ohne die Primfaktorzerlegung auskommt, ist der Algorithmus von Euklid (siehe Abbildung 1). Dieser ist eine direkte Umsetzung der rekursiven Anwendung der folgenden Resultate.

Lemma 1.8

Sind n und m positive natürliche Zahlen mit $m \leq n$, so gilt

$$\mathrm{ggT}(n, m) = \mathrm{ggT}(n - m, m).$$

Beweis: Wir zeigen: Jeder Teiler von m und n ist auch ein Teiler von $n - m$ und m und umgekehrt. Zunächst sei d ein Teiler von n und m, d.h., $d|n$ und $d|m$. Mithin gilt $n = k \cdot d$ und $m = k' \cdot d$ für geeignete k, k'. Somit gilt $n - m = k \cdot d - k' \cdot d = (k - k') \cdot d$ und folglich $d|n - m$. Es sei nun d ein Teiler von $n - m$ und m, d.h., $d|n - m$ und $d|m$. Es gilt wieder $n - m = k \cdot d$ und $m = k' \cdot d$ für geeignete k, k'. Somit erhalten wir $n = n - m + m = k \cdot d + k' \cdot d = (k + k') \cdot d$ und mithin $d|n$. Damit ist das Lemma bewiesen. ■

Korollar 1.9

Sind n und m positive natürliche Zahlen mit $m \leq n$, so gilt

$$\mathrm{ggT}(n, m) = \mathrm{ggT}(m, \mathrm{mod}(n, m)).$$

Beweis: Es sei $n = k \cdot m + \mathrm{mod}(n, m)$ für ein geeignetes $k \geq 0$. Durch wiederholte Anwendung von Lemma 1.8 erhalten wir

$$\begin{aligned} \mathrm{ggT}(n, m) &= \mathrm{ggT}(n - m, m) \\ &= \mathrm{ggT}(n - 2m, m) \\ &\vdots \\ &= \mathrm{ggT}(n - (k-1) \cdot m, m) \\ &= \mathrm{ggT}(m, n - k \cdot m) \\ &= \mathrm{ggT}(m, \mathrm{mod}(n, m)) \end{aligned}$$

Damit ist das Korollar bewiesen. ■

Beispiele: Wir wollen die Anwendung des Euklidischen Algorithmus an zwei Beispielen verdeutlichen, die auch einen Eindruck davon geben, wie unterschiedlich die Anzahlen der rekursiven Aufrufe sein können.

$$\begin{aligned} \mathrm{Euklid}(120, 36) &= \mathrm{Euklid}(36, 12) \\ &= 12 \end{aligned}$$

Die jeweiligen Primfaktorzerlegungen sind $120 = 2^3 \cdot 3^1 \cdot 5^1$ und $36 = 2^2 \cdot 3^2$. Gemäß Lemma 1.5 gilt $\mathrm{ggT}(120, 36) = 2^2 \cdot 3^1 \cdot 5^0 = 12$.

$$\begin{aligned} \mathrm{Euklid}(144, 89) &= \mathrm{Euklid}(89, 55) \\ &= \mathrm{Euklid}(55, 34) \\ &= \mathrm{Euklid}(34, 21) \\ &= \mathrm{Euklid}(21, 13) \\ &= \mathrm{Euklid}(13, 8) \\ &= \mathrm{Euklid}(8, 5) \\ &= \mathrm{Euklid}(5, 3) \\ &= \mathrm{Euklid}(3, 2) \\ &= \mathrm{Euklid}(2, 1) \\ &= 1 \end{aligned}$$

Die beiden Zahlen 89 und 144 sind benachbarte Fibonacci-Zahlen, die für den Algorithmus von Euklid schlechteste Eingaben bezüglich der Rekursionsanzahl darstellen.

Der Algorithmus von Euklid kann benutzt werden, um Brüche teilerfremd zu machen, ohne die Primzahlzerlegungen zu bestimmen. Zwei Zahlen n und m heißen teilerfremd, falls $\mathrm{ggT}(n, m) = 1$ Für beliebige positive natürliche Zahlen n und m gilt nun einerseits

$$\mathrm{ggT}\left(\frac{n}{\mathrm{ggT}(n, m)}, \frac{m}{\mathrm{ggT}(n, m)}\right) = 1$$

und andererseits

$$\frac{n}{m} = \frac{n}{m} \cdot \frac{\mathrm{ggT}(n, m)}{\mathrm{ggT}(n, m)} = \frac{n/\mathrm{ggT}(n, m)}{m/\mathrm{ggT}(n, m)}.$$

Der rechte Bruch ist mithin ein äquivalenter teilerfremder Bruch zu dem gegebenen Bruch auf der linken Seite und nicht weiter kürzbar.

Beispiele: Wenden wir den Algorithmus von Euklid auf die Zahlen 9724 und 10166 an, so erhalten wir

$$\begin{aligned} \mathrm{Euklid}(10166, 9724) &= \mathrm{Euklid}(9724, 442) \\ &= 442 \end{aligned}$$

und weiter

$$\frac{9724}{10166} = \frac{22}{23}.$$

2 Polynome*

2.1 Definitionen

Ein univariates Polynom p ist eine Funktion der Form

$$p(x) = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \cdots + a_1 \cdot x + a_0,$$

wobei n eine natürliche Zahl und $a_0, a_1, \ldots, a_n$ die Koeffizienten des Polynoms sind. Sind die Koeffzienten reelle Zahlen, so heißt p reelles Polynom; sind die Koeffizienten komplex, so heißt p komplexes Polynom. Ein Term x^n heißt Monom.

Der Grad eines Polynoms $p(x) = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \cdots + a_1 \cdot x + a_0$ ist die größte Zahl m mit $a_m \neq 0$.

Beispiele: Einige Beispiele sollen die Terminologie verdeutlichen.

- $x^2 - x + 1$ ist ein Polynom vom Grad 2.
- Die (quasi-)lineare Funktion $a \cdot x + b$ mit $a \neq 0$ ist ein Polynom vom Grad 1.
- Konstante Funktionen $f(x) = c$ sind Polynome vom Grad 0.

2.2 Horner-Schema

Um den Wert eines Polynoms p an einer Stelle x_0 auszurechnen, sollte man wie folgt vorgehen:

$$\begin{aligned}
p(x) &= a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + a_{n-2} \cdot x^{n-2} + \cdots + a_2 \cdot x^2 + a_1 \cdot x + a_0 \\
&= (a_n \cdot x^{n-1} + a_{n-1} \cdot x^{n-2} + a_{n-2} \cdot x^{n-3} + \cdots + a_2 \cdot x + a_1) \cdot x + a_0 \\
&= ((a_n \cdot x^{n-2} + a_{n-1} \cdot x^{n-3} + a_{n-2} \cdot x^{n-4} + \cdots + a_2) \cdot x + a_1) \cdot x + a_0 \\
&\vdots \\
&= ((\ldots((a_n \cdot x + a_{n-1}) \cdot x + a_{n-2}) \cdot x + \cdots) \cdot x + a_1) \cdot x + a_0
\end{aligned}$$

In dieser gewonnenen Darstellung wird das Polynom nun an der Stelle x_0 von innen nach außen sukzessive ausgewertet.

Beispiele: Wir wollen den Wert von $p(x) =_{\text{def}} x^4 + 3x^3 - 2x^2 + 11x - 1 = (((x+3)x - 2)x + 11)x - 1$ an der Stelle $x_0 = 3$ bestimmen. Die Auswertung kann durch folgendes Schema von Horner veranschaulicht werden:

	a_5	a_4	a_3	a_2	a_1	a_0
p	–	1	3	-2	11	-1
	–	0	3	18	48	177
$p(3)$	0	1	6	16	59	**176**

Wenn die Koeffizienten in einem Feld (Array) `A[0..n]` (mit `A[i]`=a_i) gespeichert sind, so wird der Funktionswert $p(x_0)$ wie folgt berechnet:

```
p=A[n];
for (int i=n-1; i>=0; i--) p=p*x0+A[i]
```

Mit dem Horner-Schema sind somit nur n Multiplikationen notwendig. Im Vergleich benötigt die Standardauswertung gemäß der Polynomdefinition insgesamt

$$\sum_{i=1}^{n} i = \frac{n(n-1)}{2} = \frac{1}{2}n^2 - \frac{1}{2}n = O(n^2)$$

Multiplikationen.

2.3 Rechnen mit Polynomen

Addition

Es seien zwei Polynome $a(x) =_{\text{def}} a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \cdots + a_1 \cdot x + a_0$ und $b(x) =_{\text{def}} b_n \cdot x^n + b_{n-1} \cdot x^{n-1} + \cdots + b_1 \cdot x + b_0$ gegeben. Bei unterschiedlichem Grad der Polynome werden die fehlenden Koeffizienten auf 0 gesetzt. Die Summe von a und b ist definiert als

$$(a+b)(x) =_{\text{def}} c_n \cdot x^n + c_{n-1} \cdot x^{n-1} + \cdots + c_1 \cdot x + c_0,$$

wobei $c_i =_{\text{def}} a_i + b_i$.

Es gilt $\text{grad}(a+b) \leq \max(\text{grad}(a), \text{grad}(b))$.

Beispiel: Für $a(x) =_{\text{def}} x^4 + 2x^2 - 3x + 7$ und $b(x) =_{\text{def}} -x^5 + 7x^3 + 4x^2 + 5x - 4$ gilt

$$(a+b)(x) = -x^5 + x^4 + 7x^3 + 6x^2 + 2x + 3$$

und $\text{grad}(a+b) = 5 = \text{grad}(b)$. Auf der anderen Seite kann Polynomaddition den Grad des resultierenden Polynoms drastisch reduzieren. Für die Polynome $a(x) =_{\text{def}} x^4 + 1$ und $b(x) =_{\text{def}} -x^4 + 1$ gilt beispielsweise $(a+b)(x) = 2$ $\text{grad}(a+b) = 0 < 4 = \max(\text{grad}(a), \text{grad}(b))$.

Multiplikation

Es seien zwei Polynome $a(x) =_{\text{def}} a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \cdots + a_1 \cdot x + a_0$ und $b(x) =_{\text{def}} b_m \cdot x^m + b_{m-1} \cdot x^{m-1} + \cdots + b_1 \cdot x + b_0$ gegeben. Das Produkt von a und b ist definiert als

$$(a \cdot b)(x) =_{\text{def}} c_{n+m} \cdot x^{n+m} + \cdots + c_1 \cdot x + c_0,$$

wobei $c_i =_{\text{def}} \sum_{j=0}^{i} a_j \cdot b_{i-j}$ (mit $a_{n+1} = \cdots = a_{n+m} = b_{m+1} = \cdots = b_{n+m} = 0$).

Es gilt $\text{grad}(a+b) = \text{grad}(a) + \text{grad}(b)$.

Beispiel: Für $a(x) =_{\text{def}} x^2 - 3x + 5$ und $b(x) =_{\text{def}} 4x + 2$ ergibt sich

$$\begin{aligned}(a \cdot b)(x) &= (1 \cdot 4)x^3 + (1 \cdot 2 + (-3) \cdot 4)x^2 + ((-3) \cdot 2 + 5 \cdot 4)x + (5 \cdot 2) \\ &= 4x^3 - 10x^2 + 14x + 10\end{aligned}$$

Division

Die Division von zwei Polynomen ist analog zur Division ganzer Zahlen mit Rest definiert. Wir führen sie daher an Hand eines Beispiels vor.

Beispiel: Für $a(x) =_{\text{def}} 2x^4 + x^3 + x + 3$ und $b(x) =_{\text{def}} x^2 + x - 1$ berechne

$$\begin{array}{rrrrl} 2^4 + & x^3 & + & x+3 & : \; x^2+x-1 \;=\; 2x^2 - x + 3 \\ \cline{1-3} -2x^4 - & 2x^3 + & 2x^2 & & \\ \cline{1-3} & -x^3 + & 2x^2 + & x & \\ & x^3 + & x^2 - & x & \\ \cline{2-4} & & 3x^2 & +3 & \\ & & -3x^2 - & 3x+3 & \\ \cline{3-4} & & & -3x+6 & \end{array}$$

Damit gilt

$$\underbrace{2x^4 + x^3 + x + 3}_{a(x)} = \underbrace{(2x^2 - x + 3)}_{t(x)} \cdot \underbrace{(x^2 + x + 1)}_{b(x)} + \underbrace{(-3x + 6)}_{r(x)}$$

mit $\text{grad}(r) < \text{grad}(b)$.

Das folgende Theorem (ohne Beweis) zeigt, dass mit Polynomen genauso gerechnet werden kann wie mit ganzen Zahlen.

Theorem 2.1

Für Polynome $a(x)$ und $b(x)$ mit $b \neq 0$ gibt es eindeutig bestimmte Polynome $t(x)$ und $r(x)$ mit $a(x) = t(x) \cdot b(x) + r(x)$ und $r = 0$ oder $\text{grad}(r) < \text{grad}(b)$.

2.4 Binomische Formeln

Es gelten die folgenden binomischen Formeln:

$$\begin{aligned} (x+y)^2 &= x^2 + 2xy + y^2 \\ (x-y)^2 &= x^2 - 2xy + y^2 \\ (x+y)\cdot(x-y) &= x^2 - y^2 \end{aligned}$$

Eine Verallgemeinerung auf die dritte Potenz ist wie folgt:

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

Im Allgemeinen kann man den Ansatz

$$(x+y)^n = \sum_{k=0}^{n} a_{n,k} x^k y^{n-k}$$

aufstellen, wobei $a_{n,k}$ gerade die Anzahl der Möglichkeiten angibt, die Binome $x^k y^{n-k}$ aus den Faktoren x und y zusammenzusetzen. Damit gilt:

$$a_{n,k} = \binom{n}{k} =_{\text{def}} \frac{n!}{k!(n-k)!}$$

Dabei setzen wir $\binom{n}{k} =_{\text{def}} 0$ für $n < k$ bzw. $k < 0$ sowie $\binom{n}{k} =_{\text{def}} 1$.

Theorem 2.2 (Binomialtheorem)

Für alle reellen Zahlen x und y und jede natürliche Zahl n gilt

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

Wie können wir den Binomialkoeffizienten $\binom{n}{k}$ bestimmen, ohne algorithmisch teure Multiplikationen auszuführen?

Lemma 2.3 (Pascalsches Dreieck)

Für natürliche Zahlen $n > 0$ und k gilt

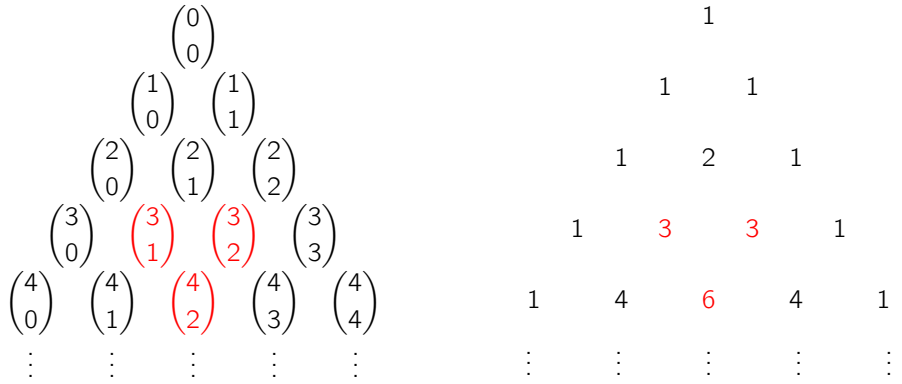
$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}.$$

Beweis: (rechnerisch; ohne Randfälle) Für $0 < k < n$ rechnen wir aus:

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

Damit ist das Lemma durch Nachrechnen bewiesen. ■

Beispiel: Der Dreiecksaufbau des rekursiven Zusammenhangs in Lemma 2.3 lässt sich leicht veranschaulichen und ist schon aus der Schule bekannt:



2.5 Nullstellen

Es sei $p(x)$ ein Polynom. Eine Zahl x_0 heißt Nullstelle von $p(x)$, falls $p(x_0) = 0$ gilt.

Beispiel: Nullstellen sollen für einige Polynome beispielhaft diskutiert werden.

- Das Polynom $x^2 - 1$ hat die Nullstellen 1 und -1.
- Das Polynom $x^2 + 1$ hat keine Nullstellen (in den reellen Zahlen).
- Es sei $p(x) =_{\text{def}} ax^2 + bx + c$ mit den reellen Zahlen a, b, c gegeben. Zur Bestimmung der Nullstellen von p rechnen wir:

$$\begin{aligned} ax^2 + bx + c &= a\left(x^2 + \frac{b}{a} \cdot x + \frac{c}{a}\right) \\ &= a\left(x + \frac{b}{2a}\right)^2 - \frac{b^2}{4a} + c \end{aligned}$$

  Für $p(x) = 0$ gilt somit

$$a\left(x + \frac{b}{2a}\right)^2 = \frac{b^2}{4a} - c \quad \text{bzw.} \quad \left(x + \frac{b}{2a}\right)^2 = \frac{b^2}{4a^2} - \frac{c}{a}.$$

  Durch Ziehen der Wurzel auf beiden Seiten erhalten wir

$$\left|x + \frac{b}{2a}\right| = \sqrt{\frac{b^2}{4a^2} - \frac{c}{a}},$$

  oder aufgelöst nach x:

$$x = -\frac{b}{2a} \pm \sqrt{\frac{b^2}{4a^2} - \frac{c}{a}} = -\frac{b}{2a} \pm \frac{1}{2a}\sqrt{b^2 - 4ac}$$

  Damit eine Lösungen im Bereich der reellen Zahlen existiert, muss also $b^2 - 4ac \geq 0$ gelten. Gilt $b^2 - 4ac > 0$, so hat das Polynom p zwei verschiedene reelle Nullstellen.
- Das Polynom $p(x) =_{\text{def}} -x^3 + 3x^2 - x - 1$ hat die Nullstellen $1, 1 + \sqrt{2}$ und $1 - \sqrt{2}$, denn:

$$(x - 1)\left(x - \left(1 + \sqrt{2}\right)\right)\left(x - \left(1 - \sqrt{2}\right)\right) = x^3 + 3x^2 - x - 1.$$

Theorem 2.4

Ein reelles Polynom $p(x) \neq 0$ mit dem Grad n hat höchstens n Nullstellen in den reellen Zahlen.

Beweis: Ist p vom Grad 0, so gilt die Aussage wegen $p(x) \neq 0$. Ist p vom Grad $n > 0$, so hat p entweder keine Nullstelle (womit die Aussage gilt) oder p besitzt mindestens eine Nullstelle x_0. Nach Theorem **??** gibt es somit Polynome $t(x)$ und $r(x)$ mit

$$p(x) = t(x) \cdot (x - x_0) + r(x)$$

und $\text{grad}(r) < \text{grad}(x - x_0)$. Wegen $\text{grad}(x - x_0) = 1$ gilt $\text{grad}(r) = 0$, d.h., $r(x) = r_0$ für eine reelle Zahl r_0. Damit gilt aber

$$0 = p(x_0) = t(x_0)(x_0 - x_0) + r_0 = r_0$$

Mithin gilt $p(x) = t(x) \cdot (x - x_0)$ mit $\text{grad}(t) = n - 1$. Wenn wir bereits wissen, dass Polynome bis zum Grad $n - 1$ höchstens $n - 1$ Nullstellen besitzen, so hat folglich p höchstens n Nullstellen. ■

Ohne Beweis geben wir die allgemeine Aussage für die Anzahl der Nullstellen von Polynomen an.

Theorem 2.5 (Fundamentalsatz der Algebra)

Jedes komplexe Polynom p mit $p \neq 0$ und Grad n hat genau n komplexe Nullstellen (mit Vielfachheiten).

Ein Polynom $p(x) =_{\text{def}} a_n x^n + \cdots + a_0$ von Grad n heißt normiert, falls $a_n = 1$.

Korollar 2.6

Es seien p und q normierte Polynome vom Grad n. Stimmen p und q bei n paarweise verschiedenen Argumenten überein, so sind p und q identisch.

Als Anmerkung sei erwähnt, dass das Korollar auch für komplexe Argumente gilt.

Beweis: Es seien p und q normiert vom Grad n. Es seien $x_1, \ldots, x_n$ paarweise verschiedene reelle Zahlen mit $p(x_i) = q(x_i)$. Betrachten wir das Differenzpolynom $r(x) =_{\text{def}} p(x) - q(x)$, so gilt $r(x_i) = 0$ für alle x_i, d.h., r besitzt n Nullstellen. Da p und q normiert sind, gilt $\text{grad}(r) \leq n - 1$. Nach Theorem 2.4 muss folglich $r = 0$ gelten. Damit gilt $p = q$. ■

Korollar 2.7

Es sei p ein normiertes Polynom vom Grad n mit den paarweise verschiedenen Nullstellen $\alpha_1, \ldots, \alpha_n$. Dann gilt

$$p(x) = (x - \alpha_1) \cdot (x - \alpha_2) \cdot \ldots \cdot (x - \alpha_n).$$

Beweis: Es sei $q(x) =_{\text{def}} (x - \alpha_1) \cdot (x - \alpha_2) \cdot \ldots \cdot (x - \alpha_n)$. Dann ist q normiert und vom Grad n. Weiterhin besitzen p und q die gleichen n Nullstellen. Folglich gilt $p = q$. ■

Eine Verallgemeinerung des Korollars auf vielfache Nullstellen ist möglich.

3 Induktion

3.1 Vollständige Induktion

Die vollständige Induktion ist eine Methode zur Lösung des folgenden Problems: Wie weisen wir nach, dass alle natürlichen Zahlen eine bestimmte Eigenschaft E erfüllen?

Die Lösungsmethode „Vollständige Induktion von $n-1$ nach n“ besteht in zwei Schritten, die zusammengenommen folgenden logischen Schluss ermöglichen:

- Induktionsanfang: *Erfüllt* 0 *die Eigenschaft* E *und*
- Induktionsschritt: *folgt für alle* $n > 0$ *die Gültigkeit von* E *für* n *aus der Tatsache, dass* $n-1$ *die Eigenschaft* E *erfüllt* (Induktionsvoraussetzung),

so erfüllen alle Zahlen die Eigenschaft E.

Wir wollen diese Beweismethode an einigen Beispielaussagen nachvollziehen:

Proposition 3.A

Für alle natürlichen Zahlen n gilt $\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$.

Beweis: (Induktion) Wir definieren zunächst für alle natürlichen Zahlen n:

$$a_n =_{\text{def}} \sum_{k=0}^{n} k$$

Die Eigenschaft E, die wir für alle natürlichen Zahlen zeigen wollen, ist die Gleichheit:

$$E(n) \quad : \qquad a_n = \frac{n(n+1)}{2}$$

Wir führen einen Beweis mittels vollständiger Induktion über n.

- Induktionsanfang: Für $n = 0$ gilt $a_0 = \sum_{k=0}^{0} k = 0 = \frac{0 \cdot (0+1)}{2}$, d.h., $E(0)$ gilt.
- Induktionsschritt: Für $n > 0$ führen wir die Aussage $E(n)$ auf die Aussage $E(n-1)$ zurück, um daraus mittels Induktionsvoraussetzung die Aussage $E(n)$ zu beweisen. Für $n-1$ lautet die als wahr vorausgesetzte Aussage

$$E(n-1) \quad : \qquad a_{n-1} = \frac{(n-1)((n-1)+1)}{2} = \frac{(n-1)n}{2}$$

Damit erhalten wir durch Abspalten des Summanden für $k = n$ aus a_n:

$$\begin{aligned} a_n &= n + a_{n-1} \\ &= n + \frac{(n-1)n}{2} && \text{(nach Induktionsvoraussetzung)} \\ &= \frac{2n + (n-1)n}{2} \\ &= \frac{n(2 + (n-1))}{2} \\ &= \frac{n(n+1)}{2} \end{aligned}$$

Damit ist die Proposition bewiesen. ■

Proposition 3.B

Für alle natürlichen Zahlen n gilt $\sum_{k=0}^{n}(2k+1) = (n+1)^2$.

Beweis: (Induktion) Die Eigenschaft E, die wir für alle natürlichen Zahlen zeigen wollen, ist die Gleichheit:

$$E(n) \quad : \quad \sum_{k=0}^{n}(2k+1) = (n+1)^2$$

Wir führen einen Beweis mittels vollständiger Induktion über n.

- Induktionsanfang: Für $n = 0$ gilt $\sum_{k=0}^{0}(2k+1) = (2 \cdot 0 + 1) = 1 = (0+1)^2$, d.h., $E(0)$ gilt.
- Induktionsschritt: Für $n > 0$ führen wir die Aussage $E(n)$ auf die Aussage $E(n-1)$ zurück, um daraus mittels Induktionsvoraussetzung die Aussage $E(n)$ zu beweisen. Für $n-1$ lautet die Aussage

  $$E(n-1) \quad : \quad \sum_{k=0}^{n-1}(2k+1) = ((n-1)+1)^2 = n^2$$

  Damit erhalten wir durch Abspalten des Summanden für $k = n$:

  $$\begin{aligned} \sum_{k=0}^{n}(2k+1) &= 2n + 1 + \sum_{k=0}^{n-1}(2k+1) \\ &= 2n + 1 + n^2 && \text{(nach Induktionsvoraussetzung)} \\ &= (n+1)^2 \end{aligned}$$

Damit ist die Proposition bewiesen. ■

Proposition 3.C

Für alle natürlichen Zahlen n gilt $\sum_{k=0}^{n} k^3 = \frac{n^2(n+1)^2}{4}$.

Beweis: (Induktion) Die Eigenschaft E, die wir für alle natürlichen Zahlen zeigen wollen, ist die Gleichheit:

$$E(n) \quad : \qquad \sum_{k=0}^{n} k^3 = \frac{n^2(n+1)^2}{4}$$

Wir führen einen Beweis mittels vollständiger Induktion über n.

- Induktionsanfang: Für $n = 0$ gilt $\sum_{k=0}^{0} k^3 = 0^3 = 0 = \frac{0^2 \cdot (0+1)^2}{4}$, d.h., $E(0)$ gilt.
- Induktionsschritt: Für $n > 0$ führen wir die Aussage $E(n)$ auf die Aussage $E(n-1)$ zurück. Für $n-1$ lautet die Eigenschaft E:

$$E(n-1) \quad : \qquad \sum_{k=0}^{n-1} k^3 = \frac{(n-1)^2((n-1)+1)^2}{4} = \frac{(n-1)^2 n^2}{4}$$

Damit erhalten wir durch Abspalten des Summanden für $k = n$:

$$\begin{aligned}
\sum_{k=0}^{n} k^3 &= n^3 + \sum_{k=0}^{n-1} k^3 \\
&= n^3 + \frac{(n-1)^2 n^2}{4} && \text{(nach Induktionsvoraussetzung)} \\
&= \frac{4n^3 + n^4 - 2n^3 + n^2}{4} \\
&= \frac{n^4 + 2n^3 + n^2}{4} \\
&= \frac{n^2(n^2 + 2n + 1)}{4} \\
&= \frac{n^2(n+1)^2}{4}
\end{aligned}$$

Damit ist die Proposition bewiesen. ■

Ein wichtiges Resultat ist die folgende explizite Formel für die geometrische Reihe.

Proposition 3.D

Es sei $q \neq 1$. Für alle natürlichen Zahlen n gilt $\sum_{k=0}^{n} q^k = \frac{q^{n+1} - 1}{q - 1}$.

Insbesondere ergibt sich für den Spezialfall $q = 2$:

$$\sum_{k=0}^{n} 2^k = 2^{n+1} - 1$$

Beweis: (Induktion) Die Eigenschaft E, die für alle natürlichen Zahlen bewiesen werden soll, lautet:

$$E(n) \quad : \qquad \sum_{k=0}^{n} q^k = \frac{q^{n+1} - 1}{q - 1}$$

Wir führen einen Beweis mittels vollständiger Induktion über n.

- Induktionsanfang: Für $n = 0$ gilt $\sum_{k=0}^{0} q^k = q^0 = 1 = \frac{q^{0+1} - 1}{q - 1}$ für $q \neq 1$, d.h., $E(0)$ gilt.
- Induktionsschritt: Für $n > 0$ führen wir die Aussage $E(n)$ wieder geeignet auf die Aussage $E(n-1)$ zurück. Dieses hat folgendes Aussehen:

$$E(n-1) \quad : \quad \sum_{k=0}^{n-1} q^k = \frac{q^{(n-1)+1} - 1}{q - 1} = \frac{q^n - 1}{q - 1}$$

Durch Abspalten des Summanden für $k = n$ erhalten wir somit:

$$\begin{aligned}
\sum_{k=0}^{n} q^k &= q^n + \sum_{k=0}^{n-1} q^k \\
&= q^n + \frac{q^n - 1}{q - 1} && \text{(nach Induktionsvoraussetzung)} \\
&= \frac{q^n(q-1) + q^n - 1}{q - 1} \\
&= \frac{q^{n+1} - q^n + q^n - 1}{q - 1} \\
&= \frac{q^{n+1} - 1}{q - 1}
\end{aligned}$$

Damit ist die Proposition bewiesen. ■

Proposition 3.E

Für alle natürlichen Zahlen n gilt $(n+1)! \geq 2^n$.

Beweis: (Induktion) Wir führen einen Beweis mittels vollständiger Induktion über n.

- Induktionsanfang: Für $n = 0$ gilt $(0+1)! = 1 \geq 1 = 2^0$.
- Induktionsschritt: Für $n > 0$ erhalten wir mittels Abspaltung des größten Faktors:

$$\begin{aligned}
(n+1)! &= (n+1) \cdot n! \\
&\geq (n+1) \cdot 2^{n-1} && \text{(nach Induktionsvoraussetzung)} \\
&\geq 2 \cdot 2^{n-1} && \text{(wegen } n \geq 1\text{)} \\
&= 2^n
\end{aligned}$$

Damit ist die Proposition bewiesen. ■

Mit Hilfe der vollständigen Induktion kann auch ein alternativer Beweis für das Binomialtheorem gegeben werden.

Theorem 2.2 (Binomialtheorem)

Für alle reellen Zahlen x und y und jede natürliche Zahl n gilt

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

Beweis: (Induktion) Für beliebige reelle Zahlen x und y führen wir einen Beweis mittels vollständiger Induktion über n.

- Induktionsanfang: Es sei $n = 0$. Dann gilt $(x+y)^0 = 1 = \binom{0}{0} x^0 y^0 = \sum_{k=0}^{0} \binom{0}{k} x^0 y^{0-k}$.
- Induktionsschritt: Es sei $n > 0$. Dann gilt:

$$\begin{aligned}
&(x+y)^n \\
&= (x+y) \cdot (x+y)^{n-1} \\
&= (x+y) \cdot \sum_{k=0}^{n-1} \binom{n-1}{k} x^k y^{n-1-k} && \text{(nach Induktionsvoraussetzung)} \\
&= \sum_{k=0}^{n-1} \binom{n-1}{k} x^{k+1} y^{n-(k+1)} + \sum_{k=0}^{n-1} \binom{n-1}{k} x^k y^{n-k} \\
&= \sum_{k=1}^{n} \binom{n-1}{k-1} x^k y^{n-k} + \sum_{k=0}^{n-1} \binom{n-1}{k} x^k y^{n-k} \\
&= \binom{n-1}{n-1} x^n y^{n-n} + \sum_{k=1}^{n-1} \left[\binom{n-1}{k-1} + \binom{n-1}{k} \right] x^k y^{n-k} + \binom{n-1}{0} x^0 y^{n-0} \\
&= \binom{n}{n} x^n y^{n-n} + \sum_{k=1}^{n-1} \binom{n}{k} x^k y^{n-k} + \binom{n}{0} x^0 y^{n-0} && \text{(nach Lemma 2.3)} \\
&= \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}
\end{aligned}$$

Damit ist das Theorem bewiesen. ∎

Mittels Induktion können wir sogar die folgende sensationelle Proposition beweisen.

Proposition 3.F

Alle natürlichen Zahlen sind gleich.

Beweis: Um die Aussage der Proposition zu beweisen, zeigen wir folgende Aussage. Für alle natürlichen Zahlen m, a, b gilt:

$$\text{Ist } \max(a,b) = m, \text{ so gilt } a = b. \tag{3.1}$$

Dies ist leicht einzusehen mittels folgenden Induktionsbeweises über m:

- Induktionsanfang: Es sei $m = 0$. Ist $\max(a, b) = 0$, so folgt $a = b = 0$.
- Induktionsschritt: Es sei $m > 0$. Ist $\max(a, b) = m$, so ist $\max(a - 1, b - 1) = m - 1$. Nach Induktionsvoraussetzung gilt somit $a - 1 = b - 1$ und mithin $a = b$.

Damit ist die Aussage (3.1) bewiesen.

Es seien nun a und b natürliche Zahlen. Es sei $m =_{\text{def}} \max(a, b)$. Wegen Aussage (3.1) sind alle natürlichen Zahlen gleich m. ■

Da die Aussage der Proposition ganz offensichtlich falsch ist, haben wir im Beweis einen Fehler gemacht. Welchen?

3.2 Allgemeine Form der vollständigen Induktion

Die Lösungsmethode besteht in zwei Schritten, die zusammengenommen folgenden logischen Schluss ermöglichen:

E sei die nachzuweisende Eigenschaft E und n_0 sie eine natürliche Zahl:

- Induktionsanfang: *Erfüllen* $0, 1, \ldots, n_0$ *die Eigenschaft* E *und*
- Induktionsschritt: *folgt für alle* $n > n_0$ *die Gültigkeit von* E *für* n *aus der Tatsache, dass alle* $m < n$ *die Eigenschaft* E *erfüllen* (Induktionsvoraussetzung),

so erfüllen alle Zahlen die Eigenschaft E*.*

Wir wollen auch diese Beweismethode an einigen Beispielaussagen nachvollziehten:

Proposition 3.G

Für alle natürlichen Zahlen $n \geq 4$ gilt $n! \geq 2^n$.

Beweis: (Induktion) Wir führen einen Bewies mittels Induktion über n für $n \geq 4$. (Wir setzen $n_0 =_{\text{def}} 4$.)

- Induktionsanfang: Für $n = 0, 1, 2, 3$ muss nichts gezeigt werden, d.h., die Aussage ist richtig. Für $n = 4$ gilt $4! = 24 \geq 16 = 2^4$.
- Induktionsschritt: Für $n > 4$ erhalten wir mittels Abspaltung des größten Faktors:

$$\begin{aligned} n! &= n \cdot (n-1)! \\ &\geq n \cdot 2^{n-1} && \text{(nach Induktionsvoraussetzung)} \\ &\geq 2 \cdot 2^{n-1} && \text{(wegen } n \geq 5\text{)} \\ &= 2^n \end{aligned}$$

Damit ist die Proposition bewiesen. ■

Die Fibonacci-Folge (in der hier verwendeten Form) ist wie folgt rekursiv definiert:

$$F_0 =_{\text{def}} 1, \qquad F_1 =_{\text{def}} 2, \qquad F_n =_{\text{def}} F_{n-1} + F_{n-2} \quad \text{fr } n \geq 2$$

Die ersten Glieder dieser Folge sind: $1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \ldots$ Im Folgenden wollen wir zeigen, dass die Fibonacci-Folge exponentiell wächst. Wegen der rekursiven Definition der Folgenglieder bietet sich dafür ein Induktionsbeweis geradezu an.

Proposition 3.H

Für alle natürlichen Zahlen n gilt $F_n \geq \left(\frac{\sqrt{5}+1}{2}\right)^n$.

Beweis: (Induktion) Wir führen einen Beweis mittels Induktion über n.

- Induktionsanfang: Wir überprüfen zwei Fälle. Für $n = 0$ gilt $F_0 = 1 = \left(\frac{\sqrt{5}+1}{2}\right)^0$ und für $n = 1$ gilt $F_1 = 2 \geq \left(\frac{\sqrt{5}+1}{2}\right)^1$.
- Induktionsschritt: Für $n > 1$ erhalten aus der Definition von F_n:

$$\begin{aligned} F_n &= F_{n-1} + F_{n-2} \\ &\geq \left(\frac{\sqrt{5}+1}{2}\right)^{n-1} + \left(\frac{\sqrt{5}+1}{2}\right)^{n-2} && \text{(nach Induktionsvoraussetzung)} \\ &= \left(\frac{\sqrt{5}+1}{2}\right)^{n-2} \left(\frac{\sqrt{5}+1}{2} + 1\right) \\ &= \left(\frac{\sqrt{5}+1}{2}\right)^{n-2} \left(\frac{\sqrt{5}+1}{2}\right)^2 \\ &= \left(\frac{\sqrt{5}+1}{2}\right)^n \end{aligned}$$

Damit ist die Proposition bewiesen. ■

4 Lineare Gleichungssysteme*

4.1 Matrizen

Es seien n und m natürliche Zahlen. Unter einer (reellen) $m \times n$-Matrix A verstehen wir folgendes Rechteckschema

$$A = (a_{i,j}) = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

Hierbei sind die reellen Zahlen a_{ij} die Koeffizienten der Matrix. Die i-te Zeile der Matrix ist der Vektor $(a_{i1}, a_{i2}, \dots, a_{in})$ und heißt i-ter Zeilenvektor; die i-te Spalte der Matrix ist der Vektor $(a_{1j}, a_{2j}, \dots, a_{mj})^T$ und heißt j-ter Spaltenvektor.

Beispiele: Wir wollen die Begriffsbildung an einigen Beispielen verdeutlichen.

- $\begin{pmatrix} 31 \\ 57 \\ 97 \end{pmatrix}$ ist eine 3×1-Matrix bzw. ein Spaltenvektor der Dimension 3.
- $(1, 2, -1, 3)$ ist eine 1×4-Matrix bzw. ein Zeilenvektor der Dimension 4.
- $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 2 & -1 \\ 3 & 5 & -7 \end{pmatrix}$ ist eine 3×3-Matrix und damit eine quadratische Matrix.
- $\begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix}$ ist eine 3×2-Matrix und damit eine Rechteck-Matrix.

Wir betrachten die folgenden Operationen auf Matrizen.

Addition

Sind A und B zwei $m \times n$-Matrizen, so ist $A + B$ eine $m \times n$-Matrix und wie folgt definiert:

$$A + B =_{\text{def}} \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} & \dots & a_{1n} + b_{1n} \\ a_{21} + b_{21} & a_{22} + b_{22} & \dots & a_{2n} + b_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} + b_{m1} & a_{m2} + b_{m2} & \dots & a_{mn} + b_{mn} \end{pmatrix}$$

Multiplikation

Ist A eine $m \times k$-Matrix und ist B eine $k \times n$-Matrix, so ist $A\dot{B}$ eine $m \times n$-Matrix und wie folgt definiert:

$$A \cdot B =_{\text{def}} \left(c_{ij}\right)$$

mit $c_{ij} =_{\text{def}} \sum_{\ell=1}^{k} a_{i\ell} b_{\ell j}$.

Beispiel: Wir führen drei beispielhafte Matrizenmutliplikationen aus:

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 2 & -1 \\ 3 & 5 & -7 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 2 & 4 \\ -17 & -16 \end{pmatrix}$$

$$\begin{pmatrix} 31 \\ 57 \\ 97 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & -1 & 3 \end{pmatrix} = \begin{pmatrix} 31 & 62 & -31 & 93 \\ 57 & 114 & -57 & 171 \\ 97 & 194 & -97 & 291 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} = 14$$

Multiplikation mit Skalaren

Ist A eine $m \times n$-Matrix und ist λ eine reelle Zahl, so ist λA eine $m \times n$-Matrix und wie folgt definiert:

$$\lambda A =_{\text{def}} \left(\lambda a_{ij}\right)$$

Die folgenden Rechenregeln für obige Operationen gelten nur dann, wenn die jeweiligen Operationen auf Grund der Matrizenstruktur auch ausführbar sind.

Rechenregeln: Es seien A, B, C Matrizen und λ eine reelle Zahl.

1. $A \cdot (\lambda B) = \lambda (A \cdot B)$
2. $(A + B) + C = A + (B + C)$
 $(A \cdot B) \cdot C \quad = A \cdot (B \cdot C)$ — Assoziativgesetze
3. $A \cdot (B + C) \;=\; A \cdot B + A \cdot C$ — Distributivgesetz
4. $A + B = B + A$ — Kommutativgesetz

Die Kommutativität für die Multiplikation vom Matrizen gilt im Allgemeinen nicht.

Beispiel: Wir betrachen die beiden folgenden Matrizen;

$$A =_{\text{def}} \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \qquad B =_{\text{def}} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

Dann erhalten wir für die Multiplikation $A \cdot B$

$$\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$$

und für die Multiplikation $B \cdot A$

$$\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

Mithin gilt $A \cdot B \neq B \cdot A$. Somit ist die Kommutativität der Multiplikation nicht für alle Matrizen erfüllt.

4.2 Lösbarkeit linearer Gleichungssysteme

Ein lineares Gleichungssystem ist durch ein Paar (A, b) gegeben, wobei A eine $m \times n$-Matrix und b ein m-dimensionaler Spaltenvektor ist. Eine Lösung für (A, b) ist ein n-dimensionaler Spaltenvektor x mit $A \cdot x = b$. $(A, 0)$ heißt homogenes lineares Gleichungssystem, wobei 0 der Nullvektor ist.

Proposition 4.1

Es seien A eine $m \times n$-Matrix und b ein m-dimensionaler Vektor.

1. Sind x und y Lösungen von $(A, 0)$, so ist auch $x + y$ eine Lösung von $(A, 0)$.
2. Ist x eine Lösung von $(A, 0)$, so ist auch λx eine Lösung von $(A, 0)$ für jede reelle Zahl λ.
3. Ist x eine Lösung von (A, b) und ist y eine Lösung von $(A, 0)$, so ist $x + y$ eine Lösung von (A, b).
4. Sind x und y Lösungen von (A, b), so ist $x - y$ eine Lösung von $(A, 0)$.

Beweis: Wir beweisen die Aussagen einzeln mit Hilfe der Rechenregeln für Matrizen.

1. Es gilt $A \cdot (x + y) = A \cdot x + A \cdot y = 0 + 0 = 0$.
2. Es gilt $A \cdot (\lambda x) = \lambda(A \cdot x) = \lambda 0 = 0$.
3. Es gilt $A \cdot (x + y) = A \cdot x + A \cdot y = b + 0 = b$.
4. Es gilt $A \cdot (x - y) = A \cdot x - A \cdot y = b + b = 0$.

Damit ist die Proposition bewiesen. ■

Beispiele: Wir wollen beispielhaft Lösungen für lineare Gleichungssysteme bestimmen.

- Gegeben sei das lineare Gleichungssytem

$$\begin{pmatrix} 3 & 5 \\ 7 & 4 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 29 \\ 60 \end{pmatrix}$$

  oder in linearen Gleichungen geschrieben:

$$\begin{aligned} 3x_1 + 5x_2 &= 29 \\ 7x_1 + 4x_2 &= 60 \end{aligned}$$

  Die eindeutige Lösung ist $x_1 = 8$ und $x_2 = 1$.

- Das lineare Gleichungssystem

$$\begin{pmatrix} 1 & -2 & 4 \\ 3 & -2 & 4 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 2 \\ 6 \end{pmatrix}$$

  besitzt keine eindeutige Lösung. Für beliebige t ist $x_1 = 2, x_2 = 2t, x_3 = t$ stets eine Lösung.

- Das lineare Gleichungssystem

$$\begin{pmatrix} 1 & 1 \\ 3 & 1 \\ 0 & 2 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 6 \\ 7 \\ 8 \end{pmatrix}$$

besitzt keine Lösung. Angenommen es gibt eine Lösung, dann ist mit Hilfe der linearen Gleichungen

$$\begin{aligned} x_1 + x_2 &= 6 \\ 3x_1 + x_2 &= 7 \\ 2x_2 &= 8 \end{aligned}$$

ersichtlich, dass $x_2 = 4$ gelten muss. Daraus folgt aber einerseits $x_1 + 4 = 6$, d.h., $x_1 = 2$, und andererseits $3x_1 + 4 = 7$, d.h., $x_1 = 1$. Dies ist eine Widerspruch. Also existiert keine Lösung.

4.3 Gauß-Elimination

Folgende Operationen lassen die Lösungsmenge eines linearen Gleichungssystems unverändert:

- Vertauschung zweier Gleichungen
- Multiplikation einer Gleichung mit einem Faktor $a \neq 0$
- Subtraktion einer Gleichung von einer anderen Gleichung

Durch kombinierte Anwendung dieser Operationen verfolgen wir nun das Ziel der sukzessiven Elimination von Variablen: Wir versuchen für das Gleichungssystem eine Dreiecksgestalt zu erzeugen.

Beispiel: Gegeben sei das folgende lineare Gleichungssystem:

$$\begin{aligned} -2x_2 + 5x_3 &= 7 \\ -8x_1 - 4x_2 &= -12 \\ 4x_1 + 3x_2 + x_3 &= 6 \end{aligned}$$

Zunächst vertauschen wir die erste und dritte Zeile und erhalten:

$$\begin{aligned} 4x_1 + 3x_2 + x_3 &= 6 \\ -8x_1 - 4x_2 &= -12 \\ -2x_2 + 5x_3 &= 7 \end{aligned}$$

Nun addieren wir zweimal die erste Zeile zur zweiten Zeile und erhalten:

$$\begin{aligned} 4x_1 + 3x_2 + x_3 &= 6 \\ 2x_2 + 2x_3 &= 0 \\ -2x_2 + 5x_3 &= 7 \end{aligned}$$

Zuletzt addieren wir noch die zweite Zeile zur dritten Zeile und erhalten als Gleichungssystem in Dreiecksgestalt:

$$\begin{aligned} 4x_1 + 3x_2 + x_3 &= 6 \\ 2x_2 + 2x_3 &= 0 \\ 7x_3 &= 7 \end{aligned}$$

Durch Rückwärtseinsetzen können aus diesem Gleichungssystem die Werte für x_1, x_2 und x_3 wie folgt bestimmt werden:

- Aus der dritten Zeile folgt $x_3 = 1$.
- Aus der zweiten Zeile folgt somit $2x_2 + 2 = 0$, also $x_2 = -1$.
- Aus der ersten Zeilen folgt somit $4x_1 - 2 = 6$, also $x_1 = 2$.

Damit ist $x_1 = 2, x_2 = -1, x_3 = 1$ die einzige Lösung für das Gleichungssystem.

Das in dem Beispiel exemplarisch vorgeführte Gaußsche Eliminationsverfahren zur Erzeugung einer (oberen) Dreiecksgestalt kann für den Fall quadratischer Matrizen durch den Algorithmus in Abbildung 2 beschrieben werden.

Algorithmus: GaussElimination
Eingabe: $n \times n$-Matrix $A = (a_{ij})$, n-dimensionaler Vektor b
Augsabe: Dreiecksmatrix A, Vektor b

```
[1]  for i = 1 to n − 1 do
[2]    if es gibt k ≥ i mit a_{k,i} ≠ 0 then
[3]      if a_{ii} = 0 then
[4]        vertausche Zeile i mit einer Zeile k mit a_{k,i} ≠ 0
[5]      for k = i + 1 to n do
[6]        q_k = a_{k,i} / a_{ii}
[7]        for j = i to n
[8]          a_{kj} = a_{kj} − q_k a_{ij}
[9]        b_k = b_k − q_k b_i
```

Abbildung 2 Eliminationsalgorithmus von Gauß

Beispiel: Wir wollen den Algorithmus in Abbildung 2 auf das folgende lineare Gleichungssystem anwenden:

$$A =_{\text{def}} \begin{pmatrix} 0 & 2 & 1 & -1 \\ 3 & 2 & 0 & 1 \\ 3 & 1 & -2 & 1 \\ 6 & 4 & -1 & 1 \end{pmatrix}, \qquad b =_{\text{def}} \begin{pmatrix} 4 \\ 1 \\ -3 \\ 2 \end{pmatrix}$$

Nach dem Durchlauf der äußeren Schleife für $i = 1$ erhalten wir dann die Matrix-Vektor-Kombination:

$$\left(\begin{array}{cccc|c} 3 & 2 & 0 & 1 & 1 \\ 0 & 2 & 1 & -1 & 4 \\ 0 & -1 & -2 & 0 & -4 \\ 0 & 0 & -1 & -1 & 0 \end{array}\right)$$

Nach dem Durchlauf für $i = 2$ erhalten wir:

$$\left(\begin{array}{cccc|c} 3 & 2 & 0 & 1 & 1 \\ 0 & 2 & 1 & -1 & 4 \\ 0 & 0 & -\frac{3}{2} & -\frac{1}{2} & -2 \\ 0 & 0 & -1 & -1 & 0 \end{array}\right)$$

Nach dem letzten Durchlauf für $i = 3$ erhalten wir als Ausgabe (in Matrix-Vektor-Kombination):

$$\left(\begin{array}{cccc|c} 3 & 2 & 0 & 1 & 1 \\ 0 & 2 & 1 & -1 & 4 \\ 0 & 0 & -\frac{3}{2} & -\frac{1}{2} & -2 \\ 0 & 0 & 0 & -\frac{2}{3} & \frac{4}{3} \end{array}\right)$$

Bei linearen Gleichungssystemen (A, b) mit (oberer) Dreiecksmatrix A, d.h.,

$$A =_{\text{def}} \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ 0 & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & a_{nn} \end{pmatrix},$$

mit $\prod_{i=1}^{n} a_{ii} \neq 0$ kann die Lösung algorithmisch wie in Abbildung **??** beschrieben bestimmt werden.

Algorithmus: Backward
Eingabe: obere $n \times n$-Dreiecksmatrix $A = (a_{ij})$ mit $a_{11} \cdot a_{22} \cdot \ldots \cdot a_{nn} \neq 0$, n-dimensionaler Vektor b
Augsabe: Lösung $(x_1, \ldots, x_n)$ von (A, b)

```
[1]  x_n = b_n / a_nn
[2]  for i = n − 1 downto 1
[3]      h = 0
[4]      for k = i + 1 to n
[5]          h = h + a_ik x_k
[6]      x_i = (b_i − h) / a_ii
[7]  return (x_1, ..., x_n)
```

Abbildung 3 Algorithmus zum Rückwärtseinsetzen in oberen Dreiecksmatrizen

Beispiel: Mit Hilfe des Algorithmus 3 ergibt sich als Fortsetzung für unser Beispielsystem die Lösung:

$$\begin{aligned}
x_4 &= \frac{4/3}{-2/3} = -2 \\
x_3 &= \frac{-2 - ((-1/2) \cdot (-2))}{-3/2} = 2 \\
x_2 &= \frac{4 - (1 \cdot 2 + (-1) \cdot (-2))}{2} = 0 \\
x_1 &= \frac{1 - (2 \cdot 0 + 0 \cdot 2 + 1 \cdot (-2))}{3} = 1
\end{aligned}$$