

8.7 Def. Eine Menge X mit einer binären Relation \succeq darauf heißt Poset (partiell geordnete Menge), wenn für alle $x, y, z \in X$ folgendes gilt:

- $x \preceq x$ (Reflexivität)
- $x \preceq y, y \preceq z \Rightarrow x \preceq z$ (Transitivität).
- $x \preceq y, y \preceq x \Rightarrow x = y$ (Antisymmetrie).

Die binäre Relation \succeq heißt in diesem Fall die partielle Ordnung auf X .

8.8 Def. Wenn für ein Poset (X, \succeq) für alle $x, y \in X$, die Bedingung $x \succeq y$ oder die Bedingung $y \succeq x$ erfüllt ist, so nennt man (X, \succeq) eine total geordnete Menge und \succeq eine totale Ordnung auf X .

Bsp. Bewertung nach mehreren Parametern (z.B. Preis, Qualität)

8.9 Bsp.

- 2^X mit Inklusion.
- \mathbb{N} mit Teilbarkeit.
- Substring-Relation auf Strings.

8.10 Def. Für $n \in \mathbb{N}$ ist eine n -stellige Relation auf Mengen X_1, \dots, X_n eine Teilmenge $R \subseteq X_1 \times \dots \times X_n$.

8.11 Bsp. Betrachten wir eine Tabelle, in welcher die Besucher:innen eines Hotels durch die Angaben **Name**, **Zimmer**, **Checkin-Datum**, **Checkout-Datum** geführt werden. Ist S die Menge aller Strings und D die Menge aller Daten, so kann man die Tabelle als eine 4-stellige Relation $R \subseteq S \times S \times D \times D$ auffassen. Die Bedingung $(p, z, d_1, d_2) \in R$, dass (p, z, d_1, d_2) sich in der Relation R befinden, bedeutet, dass die Person p am Tag d_1 im Zimmer z untergebracht wurde und am Tag d_2 das Hotel verlassen hat.

Wie man an diesem Beispiel sieht, sind die Tabellen eine Möglichkeit Relationen R durch eine Aufzählung (durch die Zeilen einer Tabelle) zu beschreiben.

9 Beweisansätze

$$A \Rightarrow B \Rightarrow C \Rightarrow D \Rightarrow E \Rightarrow F$$

9.1 Widerspruchsbeweis und Kontraposition

↳

⊥

Das wollte
ich aus

A ableiten.

9.1. Ein Widerspruchsbeweis ist ein Beweis, bei dem man eine Implikation $a \Rightarrow b$ folgendermaßen bestätigt. Man nimmt a und \bar{b} an, und leitet daraus einen Widerspruch her. Ein Widerspruch ist eine falsche Aussage. Oft hat ein Widerspruch die Form $c \wedge \bar{c}$. Das Letztere bedeutet, dass eine Aussage c bestätigt aber auch gleichzeitig widerlegt wird. Der Widerspruchsbeweis basiert auf der Äquivalenz der folgenden beiden booleschen Formeln

- $a \Rightarrow b$
- $a \wedge \bar{b} \Rightarrow \text{Falsch}$

Die Äquivalenz der Formeln kann man dadurch erkennen, dass die beiden Formeln nur in einem Fall den Wahrheitswert Falsch haben: bei der ersten sowie der zweiten Formel tritt dieser genau dann Fall auf, wenn a wahr und b falsch ist.

$$\underline{2 \cdot 3 \cdot 5} + 1$$

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1$$

9.2 Lemma. Für $t \in \mathbb{N}$ seien $p_1, \dots, p_t \in \mathbb{Z}_{\geq 2}$ und sei $n := p_1 \cdots p_t + 1$. Dann ist n durch keine der Zahlen p_1, \dots, p_t teilbar.

Beweis. Angenommen, n wäre durch ein p_i mit $i = 1, \dots, t$ teilbar. Da aber das Produkt $p_1 \cdots p_t$ durch p_i teilbar ist, ist $1 = n - p_1 \cdots p_t$ ebenfalls durch p_i teilbar. Wir haben also gezeigt, dass die ganze Zahl p_i , mit $p_i \geq 2$, die Zahl 1 teilt. Das ist ein Widerspruch, der uns die Behauptung unseres Lemmas bestätigt. □

Lemma. Sei $t \in \mathbb{N}$ und seien $p_1, \dots, p_t \in \mathbb{Z}$ und
 $p_1, \dots, p_t \geq 2$. Dann ist $n := \prod_{i=1}^t p_i + 1$
durch keine der Zahlen p_1, \dots, p_t teilbar.

Beweis: Angenommen, die Behauptung wäre falsch,
d.h. n ist durch eine der Zahlen, p_j mit $j = 1, \dots, t$, nicht teilbar.

Das Produkt $\prod_{i=1}^t p_i$ ist auch durch p_j
teilbar \Rightarrow

$1 = n - \prod_{i=1}^t p_i$ durch p_j
teilbar.

1 kann aber nicht durch p_j teilbar sein,
weil $p_j \in \mathbb{Z}$ mit $p_j \geq 2$ ist. \searrow Dieses
Widerspruch zeigt, dass die Behauptung
des Lemmas richtig ist. □

9.3. Indirekter Beweis ist ein Beweis der auf der Äquivalenz von $a \Rightarrow b$ und $\bar{b} \Rightarrow \bar{a}$ basiert. Manche Quellen beschreiben solche Art Beweise als Beweise durch Kontraposition und nutzen den Begriff indirekter Beweis als Oberbegriff für die beiden Arten der Beweise “Beweis durch Kontraposition” und “Widerspruchsbeweis”. Beweis durch Kontraposition und der Widerspruchsbeweis sind miteinander verwandt, denn einen Beweis durch Kontraposition kann man direkt in einen Widerspruchsbeweis konvertieren.

Ein weiteres Beispiel eines Widerspruch beweisen.

Thm. Es gibt unendlich viele Primzahlen.

Beweis: Angenommen, die Menge aller Primzahlen
wäre endlich, etwa $\{p_1, \dots, p_t\}$ und $t \in \mathbb{N}$.

Man betrachte die Zahl $n := \prod_{i=1}^t p_i + 1$. Nach 9.2

ist n durch keine der Zahlen p_1, \dots, p_t teilbar.

Aber offensichtlich ist $n \geq 2$ Produkt von Primzahlen
(vgl. Primfaktorzerlegung) und ist somit
durch eine von Primzahlen teilbar.

Fazit:

$n \geq 2$ durch keine der Primzahlen teilbar

n ist durch eine der Primzahlen teilbar.

⚡. \Rightarrow die Menge der Primzahlen ist
nicht endlich. \square

9.4 Lemma. Sei $a \in \mathbb{N}$. Dann sind die folgenden Aussagen äquivalent:

- (a) a ist gerade.
- (b) a^3 ist gerade.

Beweis. Wir zeigen $(a) \Rightarrow (b)$ direkt. Ist a gerade, so hat a die Form $a = 2k$ mit $k \in \mathbb{N}$. Somit ist $a^3 = (2k)^3 = 8k^3$ ebenfalls gerade.

Die Implikation $(b) \Rightarrow (a)$ können wir durch die Kontraposition herleiten: wir zeigen also $\neg (a) \Rightarrow \neg (b)$. Wenn a ungerade ist, so hat a die Form $a = 2k + 1$ mit $k \in \mathbb{N}_0$. Somit ist $a^3 = (2k + 1)^3 = (2k)^3 + 3(2k)^2 + 3(2k) + 1 = 2(4k^3 + 6k^2 + \textcolor{red}{3}k) + 1$ eine ungerade Zahl. \square

4

$$(x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3$$

9.5 Thm. Die Zahl $\sqrt[3]{2}$ ist nicht rational.

Beweis. Angenommen, $\sqrt[3]{2}$ wäre rational. Dann hätte die Zahl die Form $\sqrt[3]{2} = \frac{a}{b}$ mit $a, b \in \mathbb{N}$. Darüber hinaus können wir annehmen, dass a und b nicht beide gerade sind, denn sonst kann man a und b , solange sie beide gerade sind, durch 2 teilen, wodurch sich a und b um Faktor zwei verkleinern. Es ist klar, dass dieser Prozess nach endlich vielen Schritten terminiert.

$\sqrt[3]{2} = \frac{a}{b}$ folgt $2b^3 = a^3$. Es folgt also, dass a^3 gerade ist. Dann ist aber nach Lemma 9.4 die Zahl a gerade ist und somit die Form $a = 2k$ mit $k \in \mathbb{N}$ hat. Dann ist $2b^3 = a^3 = (2k)^3 = 8k^3$, woraus $b^3 = 4k^3$ folgt. Die Zahl b^3 ist also gerade. Nach Lemma 9.4, die wir nun zur Zahl b anwenden können, ist die Zahl b ebenfalls gerade. Wir haben also gezeigt, dass a und b beide gerade sind. Unsere Annahme war aber, dass a oder b ungerade ist. Dieser Widerspruch zeigt, dass die Zahl $\sqrt[3]{2}$ nicht rational ist. \square

$$2 = \frac{a^3}{b^3} \Rightarrow 2b^3 = a^3$$

9.2 Vollständige Induktion

9.6 Thm (Vollständige Induktion, Version 1). Sei P ein Prädikat auf \mathbb{N} . Dann sind die folgenden Bedingungen äquivalent:

(a) $P(n)$ gilt für alle $n \in \mathbb{N}$.

(b) $P(1)$ gilt und, aus $P(n)$ folgt $P(n+1)$, für alle $n \in \mathbb{N}$.

Beweis. Die Implikation (a) \Rightarrow (b) ist klar: $P(1)$ ist erfüllt und da $P(n)$ und $P(n+1)$ beide Wahr ist die Implikation $P(n) \Rightarrow P(n+1)$ für jedes n eine wahre Aussage.

Nun zeigen wir ~~(a)~~ \Rightarrow ~~(b)~~ durch Kontraposition. Angenommen, (a) ist nicht erfüllt. Dann gibt ein $n \in \mathbb{N}$ für welches $P(n)$ falsch ist. Wir fixieren das kleinste solche $n \in \mathbb{N}$. Ist unser $n = 1$ so, ist (b) nicht erfüllt, weil $P(1)$ nicht erfüllt ist. Ist $n > 1$ so ist (b) nicht erfüllt, weil $P(n)$ falsch und $P(n-1)$ wahr ist, wodurch die Implikation $P(n-1) \Rightarrow P(n)$ nicht erfüllt ist. □

$$P(1) \wedge (P(1) \Rightarrow P(2)) \wedge (P(2) \Rightarrow P(3)) \wedge \dots\dots\dots$$

9.7. Beim Verwenden von Theorem 9.6 unterteilt sich die Argumentation in die folgende Schritte.

- Induktionsanfang (IA): man verifiziert, dass $P(1)$ gilt.
- Induktionsvoraussetzung (IV): man macht die Annahme: sei $n \in \mathbb{N}$ und sei die Aussage $P(n)$ erfüllt.
- Induktionsschritt (IS): man folgert $P(n + 1)$ aus der Induktionsvoraussetzung.

9.8 Thm. Für jedes $n \in \mathbb{N}$ gilt

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

Beweis. Das Prädikat mit dem wir uns in dieser Aussage befassen ist die Gleichung

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

die von einem variablen $n \in \mathbb{N}$ abhängig ist.

Diese Formel ist für $n = 1$ erfüllt, denn $\sum_{i=1}^1 i = 1$ und $\frac{1}{2}1 \cdot (1+1) = 1$.

Sei nun $n \in \mathbb{N}$ ein beliebiger Wert, für welche die Formel $\sum_{i=1}^n i = \frac{1}{2}n(n+1)$ erfüllt ist.

Beweis: $\sum_{i=1}^n i = \frac{1}{2} n(n+1)$ für jedes $n \in \mathbb{N}$.

IA: $n=1 \Rightarrow \sum_{i=1}^1 i = \frac{1}{2} \cdot 1 \cdot (1+1) \Leftrightarrow 1=1 \quad \checkmark$

IV: Sei $n \in \mathbb{N}$ ein Wert, für welchen
 $\sum_{i=1}^n i = \frac{1}{2} n(n+1)$ gilt.

2.2: die Formel gilt mit $n+1$ an der Stelle
von n .

$$\sum_{i=1}^{n+1} i = \sum_{i=1}^n i + (n+1) \stackrel{IV}{=} \frac{1}{2} n \cdot (n+1) + (n+1)$$

$$= \left(\frac{1}{2} n + 1 \right) \cdot (n+1) = \frac{1}{2} (n+2) \cdot (n+1) \\ = \frac{1}{2} (n+1) \cdot (n+2).$$

$$\Rightarrow \sum_{i=1}^{n+1} i = \frac{1}{2} (n+1) \cdot (n+2).$$

$$\sum_{i=1}^1 i = \underset{\substack{\uparrow \\ \text{starting}}}{\frac{1}{2}} \cdot 1 \cdot (1+1) \Rightarrow \sum_{i=1}^2 i = \frac{1}{2} \cdot 2 \cdot (2+1)$$

$$\Rightarrow \sum_{i=1}^3 i = \frac{1}{2} \cdot 3 \cdot (3+1)$$

$$\Rightarrow \dots$$

Wir zeigen, dass die Formel mit $n + 1$ an der Stelle von n ebenfalls erfüllt ist. Es gilt

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

da wir in der Summe den Summanden zum Index $i = n + 1$ abspalten können. Nach der Induktionsvoraussetzung ist $\sum_{i=1}^n i = \frac{1}{2}n(n + 1)$. Somit hat man

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

Zusammenfassend: Unsere Formel gilt für $n = 1$ und wenn unsere Formel für ein $n \in \mathbb{N}$ erfüllt ist, so ist sie auch mit $n + 1$ an der Stelle von n erfüllt. Aus Theorem 9.6 folgt, dass unsere Formel für jedes $n \in \mathbb{N}$ erfüllt ist. □

9.9 Bsp. Formel für $\sum_{i=0}^n q^i$. Sei $q \in \mathbb{R} \setminus \{1\}$. Dann gilt

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

für alle $n \in \mathbb{N}$.

Beweis: 1A: Behauptung im Fall $n=1$

$$\Downarrow q^0 + \dots + q^1 = \frac{q^2 - 1}{q - 1}$$

$$\Downarrow q^0 + q^1 = \frac{q^2 - 1}{q - 1}$$

$$\Downarrow 1 + q = \frac{q^2 - 1}{q - 1} \Leftrightarrow$$

$$\begin{aligned} a^2 - b^2 \\ = (a - b)(a + b) \end{aligned}$$

$$1 + q = \frac{(q-1)(q+1)}{\cancel{q-1}} \Leftrightarrow 1 + q = \cancel{q-1} + q$$

IV: $\sum_{i=0}^n q^i = \frac{q^{n+1} - 1}{q - 1}$ gelte für ein $n \in \mathbb{N}$.

IS: z.z. dann gilt die Formel auch mit $n+1$ an der Stelle von n .

Zu zeigen: $\sum_{i=0}^{n+1} q^i = \frac{q^{n+2} - 1}{q - 1}$

Es gilt: $\sum_{i=0}^{n+1} q^i = \sum_{i=0}^n q^i + q^{n+1} \stackrel{IV}{=}$

$$= \frac{q^{n+1} - 1}{q - 1} + q^{n+1} = \frac{q^{n+1} - 1}{q - 1} + \frac{q^{n+1}(q - 1)}{q - 1}$$

$$= \frac{q^{n+1} - 1 + q^{n+1}(q - 1)}{q - 1} = \frac{\cancel{q^{n+1}} - 1 + q^{n+2} - \cancel{q^{n+1}}}{q - 1}$$

$$= \frac{q^{n+2} - 1}{q - 1} \Rightarrow \left[\sum_{i=0}^{n+1} q^i = \frac{q^{n+2} - 1}{q - 1} \right]$$

9.10 Bsp. Formel für $\sum_{i=1}^n iq^i$.

9.11. Durch Induktion lassen sich nicht nur Gleichung^{en} herleiten. Es gibt viele verschiedene Situationen aus diskreter Mathematik, in denen man durch die Induktion Aussagen verifizieren

kann. (In der Theorie der Algorithmen nutzt man oft die Induktion, um die Korrektheit und die Laufzeit von Algorithmen zu analysieren).

9.12 Thm. $n \leq 2^n$ gilt für alle $n \in \mathbb{N}$.

Beweis. Diese Ungleichung kann man mit der Verwendung Ihrer Schulkenntnisse aus der Analysis herleiten. Der folgende Beweis durch die Induktion ist aber elementarer.

Die Ungleichung gilt für $n = 1$, denn $1 \leq 2^1$. Sei nun $n \in \mathbb{N}$ ein Wert, für welchen $n \leq 2^n$ gilt. Im Induktionsschritt sollen wir nun $n + 1 \leq 2^{n+1}$ herleiten. Da wir $n \leq 2^n$ voraussetzen, gilt $n + 1 \leq 2^n + 1$, daher reicht es zu verifizieren, dass $2^n + 1 \leq 2^{n+1}$ erfüllt ist. Das letztere ist Äquivalent zur Ungleichung $2^n \geq 1$, die trivialerweise für $n \in \mathbb{N}$ erfüllt ist. \square

$$1 \leq 2^1 \wedge (1 \leq 2^1 \Rightarrow 2 \leq 2^2) \wedge (2 \leq 2^2 \Rightarrow 3 \leq 2^3) \\ \wedge (3 \leq 2^3 \Rightarrow 4 \leq 2^4) \wedge \dots$$

$$n \leq 2^n \text{ für alle } n \in \mathbb{N}.$$

IA: $n=1$. $1 \leq 2^1 \Leftrightarrow 1 \leq 2 \quad \checkmark$

IV: Angenommen, $n \leq 2^n$ gelte für ein $n \in \mathbb{N}$.

IS: zu zeigen: $n+1 \leq 2^{n+1}$:

$$n+1 \stackrel{IV}{\leq} 2^n + 1 \stackrel{?}{\leq} 2^{n+1}$$



$$2^n + 1 \leq 2 \cdot 2^n$$



$$1 \leq 2^n$$

← gilt für jedes $n \in \mathbb{N}$.

$$\Rightarrow n+1 \leq 2^{n+1}.$$



Man kann nach dem gleichen Prinzip auch Aussagen der Form " $P(n)$ gilt für jedes $n \in \mathbb{Z}$ mit $n \geq a$ " verifizieren. In diesem Fall hat man a als den Induktionsanfang.

$100n \leq 2^n$ gilt für alle $n \in \mathbb{N}$ mit $n \geq 10$

IA: $n=10 \quad 100 \cdot 10 \leq 2^{10} \Leftrightarrow 1000 \leq 1024$

IV: $100 \cdot n \leq 2^n$ gelte für ein $n \in \mathbb{N}$ mit $n \geq 10$.

IS: zu zeigen: $100 \cdot (n+1) \leq 2^{n+1}$

$$100 \cdot (n+1) = 100 \cdot n + 100 \stackrel{IV}{\leq} 2^n + 100 \stackrel{?}{\leq} 2^{n+1}$$

$$\Rightarrow \Leftrightarrow 2^n + 100 \leq 2 \cdot 2^n \Leftrightarrow 100 \leq 2^n$$

Das gilt weil $n \geq 10$ ist
(vgl. Induktionsvoraussetzung). \square

Ein anderer Induktionsanfang als die 1:

• $\sum_{i=0}^n q^i = \frac{q^{n+1} - 1}{q - 1}$ kann man auch für alle $q \neq 1$ und $n \in \mathbb{N}_0$ zeigen. In diesem Fall ist der Induktionsanfang $n=0$ sogar noch einfacher zu verifizieren als der Fall $n=1$: $q^0 = \frac{q^1 - 1}{q - 1} \Rightarrow 1 = 1.$

• $100 \cdot n \leq 2^n$ gilt für alle $n \in \mathbb{N}$ mit $n \geq 10$.

IA: $n=10$. $100 \cdot 10 \leq 2^{10} \Rightarrow 1000 \leq 1024 \vee$

IS: Sei $n \in \mathbb{N}$, $n \geq 10$ und sei $100 \cdot n \leq 2^n$ erfüllt.

IS: z.z.: $100 \cdot (n+1) \leq 2^{n+1}$

$$100 \cdot (n+1) \leq 100 \cdot n + 100 \stackrel{IV}{\leq} 2^n + 100 \stackrel{?}{\leq} 2^{n+1}$$

$$2^n + 100 \leq 2^{n+1} \Rightarrow 2^n + 100 \leq 2 \cdot 2^n \Rightarrow 100 \leq 2^n$$

das gilt, weil $n \geq 10$ ist ($100 \leq 2^{10}$).

9.13 Thm (Vollständige Induktion, Version 2). Sei P ein Prädikat auf \mathbb{N} . Dann sind die folgenden Bedingungen äquivalent:

(a) $P(n)$ gilt für alle $n \in \mathbb{N}$.

(b) $P(1)$ gilt und, für jedes $n \in \mathbb{N}$, folgt aus der Gültigkeit der Aussagen $P(i)$ mit $i \in \{1, \dots, n\}$, die Gültigkeit von $P(n+1)$.

Beweis. Es gibt zwei einfache Weisen, diese Version der vollständigen Induktion herzuleiten. Zum einen kann man den Beweis von Theorem 9.6 sehr geringfügig modifizieren, um dieses Theorem herzuleiten. Zum anderen kann man die Behauptung von Theorem 9.6 für das Prädikat $Q(n) := P(1) \wedge \dots \wedge P(n)$ benutzen. □

$$P(1) \wedge (P(1) \Rightarrow P(2)) \wedge (P(1) \wedge P(2) \Rightarrow P(3)) \wedge \\ (P(1) \wedge P(2) \wedge P(3) \Rightarrow P(4)) \wedge \dots$$

(a) $P(n)$ gilt für alle $n \in \mathbb{N}$



(b) $P(n)$ gilt auch für jedes $n \in \mathbb{N}$ gilt:

$$P(1) \wedge P(2) \wedge \dots \wedge P(n) \Rightarrow P(n+1).$$

9.14 Thm (Primfaktorzerlegung - Existenz). Für jedes $n \in \mathbb{N}$ existieren ~~$t \in \mathbb{N}_0$~~ Primzahlen p_1, \dots, p_t mit (mit $t \in \mathbb{N}_0$), sodass die Gleichung

$$n = \prod_{i=1}^t p_i.$$

erfüllt ist.

(Man beachte: die Zahlen p_1, \dots, p_t müssen nicht paarweise verschieden sein und bei $t = 0$ ist $\prod_{i=1}^t p_i$ das Produkt von 0 Zahlen und somit gleich 1).

Beweis. Die Behauptung "es existieren $t \in \mathbb{N}_0$ Primzahlen p_1, \dots, p_t mit $n = \prod_{i=1}^t p_i$ " ist wahr für $n \in \{1, 2\}$. Denn $n = 1$ ist Produkt von 0 Primzahlen ($t = 0$) und $n = 2$ ist Produkt von einer Primzahl ($t = 1$ und $p_1 = 2$).

Sei nun $n \in \mathbb{N}$ mit $n \geq 3$ so, dass jede Zahl $a \in \{1, \dots, n-1\}$ Produkt von endlich vielen Primzahlen ist (im Sinne der Behauptung). Ist n Primzahl, so gilt die Behauptung mit $t = 1$ und $p_1 = n$. Ist n keine Primzahl, so besitzt n einen Teiler $a \in \{2, \dots, n-1\}$. Es folgt $n = ab$

$$\frac{n}{2} \leq n-1 \Leftrightarrow 0 \leq \frac{n}{2} - 1 \Leftrightarrow \frac{n}{2} \geq 1 \Leftrightarrow n \geq 2$$

9. BEWEISANSÄTZE

123



mit $b = n/a \in \mathbb{N}$ und $b \leq \frac{n}{2} \leq n-1$. Die Anwendung der Induktionsvoraussetzung zu a und b ergibt, dass man a sowie b als Produkt von Primzahlen darstellen hat. Es gilt also

$$a = \prod_{i=1}^r u_i,$$

$$b = \prod_{i=1}^s v_i.$$

mit $r, s \in \mathbb{N}$ für gewisse Primzahlen $u_1, \dots, u_r, v_1, \dots, v_s$ (hier ist weder r noch s gleich 0, denn $a, b \geq 2$). Dann ist n Produkt von $t = r + s$ Primzahlen p_1, \dots, p_t mit $p_i = u_i$ für $i \in \{1, \dots, r\}$ und $p_i = v_{i-r}$ für $i \in \{r+1, \dots, r+s\}$. □

$$70 = 2 \cdot 35$$

2
ist Primzahl!

$$5 \cdot 7$$

5

Primzahl!

7

Primzahl!

$A(70) \rightarrow A(2)$

$A(70) \rightarrow A(35) \rightarrow A(5)$

$A(70) \rightarrow A(35) \rightarrow A(7)$

9.15. Ein weiteres verbreitetes Element eines Beweises ist die Fallunterscheidung. Im vorigen Beweis haben wir z.B. zwischen den Fällen n eine Primzahl und n keine Primzahl unterschieden, und in jedem der beiden Fällen ein anderes Argument benutzt.

10 Schnupperstunde in Algebra

10.1 Was ist Algebra?

10.1. Algebra ist die Theorie algebraischer Strukturen. Während man in der Schule mit einer relativ kleiner Anzahl algebraischer Strukturen wie $(\mathbb{R}, +, \cdot)$ oder dem Vektorraum \mathbb{R}^3 arbeitet, befasst man sich in Algebra mit verschiedenen Kategorien algebraischer Strukturen, wie z.B. Halbgruppen, Gruppen, Ringe, Körper und Vektorräume *und viele mehr.*

Man entwickelt auch Mittel, neue *in Algebra* eigene algebraische Strukturen anzulegen. Wenn man diesen Prozess mit der Programmierung vergleicht, so ist der Prozess sehr ähnlich zur Entwicklung eigener Datenstrukturen (im Gegensatz zur Nutzung der standardmäßig vorhandenen Datenstrukturen). *bzw.*

10.2 (Algebraische Struktur). Eine algebraische Struktur ist (in der Regel) eine Menge A , die mit einer oder mehreren Verknüpfungen ausgestattet ist. In den allermeisten Fällen sind die Verknüpfungen, die man betrachtet, binär: sie sind Abbildungen $* : A \times A \rightarrow A$. Für solche Abbildungen schreibt man dann $a * b$ an der Stelle von $*(a, b)$. Sehr oft handelt es sich auch um ~~an~~ Verknüpfungen, für welche (zumindest) das Assoziativgesetz $a * (b * c) = (a * b) * c$ erfüllt ist.

in Algebren

der Form

10.3 (Polymorphismus in Algebra). Man benutzt oft zum Bezeichnen der Verknüpfungen (bzw. der Verknüpfung) einer algebraischen Struktur die Symbole $+$ (Plus) und \cdot (Mal). Hierbei meint man dann die Plus-Operation bzw. die Mal-Operation innerhalb der gegebenen algebraischen Struktur A . Das heißt, diese Operationen müssen $+$ und/oder \cdot innerhalb einer algebraischen Struktur A nicht unbedingt mit Operation $+$ und \cdot innerhalb der Menge \mathbb{R} der reellen Zahlen etwas zu tun haben. Das bedeutet: genau so, wie Symbole a, b, c, d, \dots in Mathematik kontextabhängig sind (können verschiedene Bedeutung in verschiedenen Kontexten haben), sind auch die Bezeichnungen wie $+$ und \cdot kontextabhängig (bzw. Strukturabhängig) und können so, wie man es sich wünscht, eingeführt werden. Wenn man also $+$ in der Struktur A hat, so ist das streng genommen $+_A$ – die Plusoperation aus der Struktur A – man schreibt aber einfach nur $+$ und nimmt stillschweigend an, dass es aus dem Kontext klar ist, welche Struktur A gemeint ist. Die Nutzung der selben Bezeichnungen für verschiedene Operationen nennt man in der Programmierung den Polymorphismus.



10.4 Bsp. Für $n \in \mathbb{N}$ heißt die Menge S_n aller bijektiven Abbildungen von $\{1, \dots, n\}$ nach $\{1, \dots, n\}$ mit der Multiplikation

$$(\sigma \cdot \tau)(i) := \sigma(\tau(i))$$

die symmetrische Gruppe. Was eine (allgemeine) Gruppe ist, wird in IT-2 diskutiert.

10.5 Bsp. Die algebraische Struktur \mathbb{F}_2 , welche man als Menge $\{0, 1\}$ mit den binären Operationen

			$1+1=0=2$ $1+1+1=1=3$ $1+1+1+1=0=4$					
			$255+3892$ $=1$					
+	0	1						
0	0	1						
1	1	0						

und

			$1+1+1+1=0=4$					

eingeführt, ist ein sogenannter binärer Körper. Die Bezeichnungen $+$, \cdot , 0 und 1 , die wir hier verwenden, sind polymorph.

Wir meinen $+\mathbb{F}_2$, $\cdot\mathbb{F}_2$, $0\mathbb{F}_2$ und $1\mathbb{F}_2$ schreiben aber in unserem Kontext von \mathbb{F}_2 vereinfachend $+$, \cdot , 0 , 1 .

Der binäre Körper spielt in der Kodierungstheorie und der Kryptographie eine wichtige Rolle.

10.2 Kommutativer Ring

ausschl. oder	f	w
f	f	w
w	w	f

und	f	w
f	f	f
w	f	w

und \leftrightarrow

$f \leftrightarrow 0$
 $w \leftrightarrow 1$

10.6 Def. Eine Menge R mit zwei binären Verknüpfungen $+$, \cdot und zwei verschiedenen ausgezeichneten Elementen $0, 1 \in R$ heißt kommutativer Ring, wenn für alle $a, b, c \in R$ Folgendes erfüllt ist:

- $a + b = b + a$ und $a \cdot b = b \cdot a$
- $a + 0 = a$ und $a \cdot 1 = a$
- $(a + b) + c = a + (b + c)$ und $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- Zu jedem a gibt es ein eindeutiges Element aus R , das man als $-a$ bezeichnet, für welches $a + (-a) = 0$ erfüllt ist.
- $a \cdot (b + c) = a \cdot b + a \cdot c$

Auch hier: ${}^t\mathbb{R}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}$

Beispiel
in Sage
mcr.

10.7 Aufgabe. Ist R kommutativer Ring mit 1, dann gilt $a \cdot 0 = 0$ für alle $a \in R$. Zeigen Sie das.

$$a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$$

$$\Rightarrow a \cdot 0 = a \cdot 0 + a \cdot 0$$

$$\Rightarrow a \cdot 0 + (-a \cdot 0) = a \cdot 0 + a \cdot 0 + (-a \cdot 0)$$

$$\Rightarrow 0 = a \cdot 0 + 0$$

$$\Rightarrow 0 = a \cdot 0.$$

10.8 Bsp.

- $(\mathbb{N}, +, \cdot)$ kein Ring.
 - $(\mathbb{N}_0, +, \cdot)$ (immer noch) kein Ring.
 - $(\mathbb{Z}, +, \cdot)$ ein kommutativer Ring.
 - $(\mathbb{Q}, +, \cdot)$ ein kommutativer Ring.
 - $(\mathbb{R}, +, \cdot)$ ein kommutativer Ring.
 - $(\mathbb{C}, +, \cdot)$ ein kommutativer Ring.
- Was für Gesetze sind nicht erfüllt?*

10.3 Körper

10.9 Def. Eine Menge K mit zwei binären Verknüpfungen $+$ und \cdot heißt Körper, wenn K bzgl. $+$ und \cdot kommutativer Ring ist und darüber hinaus für jedes $a \in K \setminus \{0\}$ ein eindeutiges Element $a^{-1} \in K$ existiert, für welches $a \cdot a^{-1} = 1$ gilt.

10.10 Bsp.

- $(\mathbb{F}_2, +, \cdot)$
- Führen Sie auf einer dreielementigen Menge $\{0, 1, a\}$ die Verknüpfungen $+$ und \cdot so ein, dass die Menge mit diesen Verknüpfungen zu einem Körper wird.
- $(\mathbb{Z}, +, \cdot)$ kein Körper, da in $\mathbb{Z} \setminus \{0\}$ nichts außer -1 und 1 invertierbar ist.
- $(\mathbb{Q}, +, \cdot)$ ein Körper.
- $(\mathbb{R}, +, \cdot)$ ein Körper.
- $(\mathbb{C}, +, \cdot)$ ein Körper.

$$2x - 3 = 0$$

$$x = \frac{3}{2}$$

$$x^2 - 4 = 0$$

$$x \in \{-2, 2\}$$

$$x^2 - 2 = 0$$

$$x \in \{-\sqrt{2}, \sqrt{2}\}$$

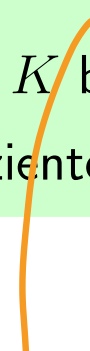
$$x^2 + 1 = 0$$

∅
hat keine
Lösungen
in \mathbb{R} !

10.11 Def. Ein Körper K heißt algebraisch abgeschlossen, wenn für jede Wahl von $d \in \mathbb{N}$ und alle $a_d \in K \setminus \{0\}, a_{d-1}, \dots, a_0 \in K$ die Gleichung

$$a_d x^d + a_{d-1} x^{d-1} + \dots + a_0 = 0$$

mindestens eine Lösung x aus K besitzt. Eine Gleichung wie oben nennt man Polynomgleichung vom Grad d mit Koeffizienten in K .


$$\sum_{i=0}^d a_i x^i = 0$$

(mit Summenzeichen
aufgeschrieben).

10.12 Bsp.

- \mathbb{Q} ist nicht algebraisch abgeschlossen, vgl. die Gleichung $x^2 - 2 = 0$, mit den Koeffizienten $-2, 0, 1 \in \mathbb{Q}$, die keine Lösung x in \mathbb{Q} besitzt.
- \mathbb{R} ist nicht algebraisch abgeschlossen, vgl. die Gleichung $x^2 + 1 = 0$ mit den Koeffizienten $1, 0, 1 \in \mathbb{R}$, die keine Lösung x in \mathbb{R} besitzt.

10.13 Def. Sind A und B Mengen mit $A \subseteq B$ und $*_A : A \times A \rightarrow A$ und $*_B : B \times B \rightarrow B$ binäre Verknüpfungen, so nennt man $*_B$ Erweiterung von $*_A$ und $*_A$ Einschränkung von $*_B$ auf A , wenn $x *_A y = x *_B y$ für alle $a, b \in A$ erfüllt ist (mit anderen Worten: $*_B$ wirkt genau so wie $*_A$ innerhalb von A).

10.14 Def. Sind $(F, +, \cdot)$ und $(K, +, \cdot)$ Körper mit $F \subseteq K$, bei denen $+$ und \cdot von K Erweiterungen von $+$ bzw. \cdot auf F sind, so nennt man den Körper K eine Erweiterung des Körpers F .

10.15 Bsp. \mathbb{R} ist Erweiterung von \mathbb{Q} . Es gibt aber viele Körper dazwischen. Zum Beispiel ist

$$\mathbb{Q}[\sqrt{2}] := \left\{ a + \sqrt{2}b : a, b \in \mathbb{Q} \right\}$$

ebenfalls ein Körper. Es gilt $\mathbb{Q} \subsetneq \mathbb{Q}[\sqrt{2}] \subsetneq \mathbb{R}$. Wie sieht das inverse eines Elements aus $\mathbb{Q}[\sqrt{2}] \setminus \{0\}$ aus?

10.16 Thm. *Jeder Körper besitzt eine algebraisch abgeschlossene Körpererweiterung.*

10.17. Es gilt sogar eine stärkere Aussage: jeder Körper eine (im einem bestimmten Sinn) minimale algebraisch abgeschlossene Körpererweiterung.

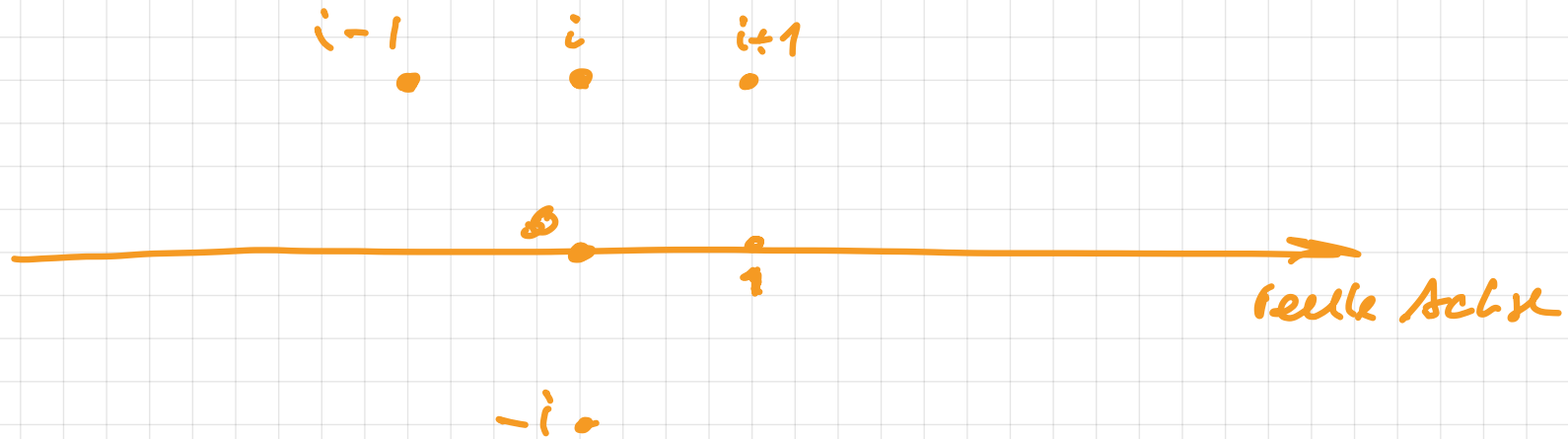
10.4 Der Körper der komplexen Zahlen

10.18 Def. Die Menge \mathbb{C} der komplexen Zahlen kann man als die Menge der formalen Ausdrücke der Form $x + iy$ mit $x, y \in \mathbb{R}$ einführen. Hierbei ist i ein formales Element, für welches man $i^2 := -1$ festlegt. Das Element i nennt man die imaginäre Einheit oder die Wurzel aus -1 . Die Menge der reellen Zahlen \mathbb{R} wird als eine Teilmenge von \mathbb{C} aufgefasst, indem man $x \in \mathbb{R}$ als $x + yi$ mit $y = 0$ schreibt.

Nach diesen Festlegungen lassen sich die Operationen $+$ und \cdot vom Körper \mathbb{R} der reellen Zahlen auf \mathbb{C} auf eine eindeutige Weise erweitern, wenn man fordert, dass \mathbb{C} mit Operationen $+$ und \cdot ein kommutativer Ring sein soll, vgl. dazu die Gesetze für einen kommutativen Ring. (Wie wir in Kürze sehen werden, ist $(\mathbb{C}, +, \cdot)$ sogar ein Körper.) Die Addition und



Ein Außerirdischer kommt
selten allein (eine Invasion!)



Multiplikation führen wir also auf die folgende Weise eingeführt:

$$(x_1 + y_1 \mathbf{i}) + (x_2 + y_2 \mathbf{i}) := (x_1 + x_2) + (y_1 + y_2) \mathbf{i}$$

$$(x_1 + y_1 \mathbf{i}) \cdot (x_2 + y_2 \mathbf{i}) := (x_1 x_2 - y_1 y_2) + (x_1 y_2 + x_2 y_1) \mathbf{i},$$

kompatibel mit
den Gesetzen,
die wir
uns
wünschen

für $x_1, x_2, y_1, y_2 \in \mathbb{R}$.

Ist $z = x + y \mathbf{i}$ mit $x, y \in \mathbb{R}$ so führen wir den Realteil von z als $\operatorname{Re}(z) := x$ und den Imaginärteil von z als $\operatorname{Im}(z) := y$ ein; die Zahl $\bar{z} = x - y \mathbf{i}$ nennen wir komplex konjugiert zu z ; den Wert $|z| = \sqrt{x^2 + y^2}$ nennen wir den Betrag von z .

Bsp.

$$(2 + 3i) \cdot (-1 + i) = ?? + ??i$$

i die imaginäre Einheit,
d.h. $i^2 = -1$.

10.19. In Algebra werden oft Strukturen formal nach "eigenen Vorgaben" eingeführt. Bei der Definition von komplexen Zahlen sieht man ein Beispiel dafür. $i^2 = -1$ ist

eine Vorgabe von uns.

In $\mathbb{Q}[\sqrt{2}]$ ist $(\sqrt{2})^2 = 2$ ebenfalls eine Vorgabe von uns (so können wir ~~den~~ innerhalb von \mathbb{Q} auffassen, denn innerhalb von \mathbb{Q} gibt es keine Zahl, die zum Quadrat gleich 2 ist)

$\sqrt{2}$ in Bezug auf \mathbb{Q} ist ebenfalls "ein Außerordlicher".

10.20 Thm. \mathbb{C} ist ein algebraisch abgeschlossener Körper.

Beweis. Dass $(\mathbb{C}, +, \cdot)$ ein kommutativer Ring ist, lässt sich direkt verifizieren (Aufgabe).

Um zu zeigen, dass $(\mathbb{C}, +, \cdot)$ sogar ein Körper ist, muss man verifizieren, dass jedes $z = x + y\mathbf{i}$ mit $x, y \in \mathbb{R}$ mit $|z| \neq 0$ ein inverses Element in \mathbb{C} besitzt. Es stellt sich heraus, dass man das inverse Element z^{-1} als $z^{-1} = \frac{1}{|z|^2} \bar{z}$ beschreiben kann. Mit der Verwendung der dritten binomischen Formel erhalten wir

$$zz^{-1} = \frac{z\bar{z}}{|z|^2} = \frac{(x + y\mathbf{i})(x - y\mathbf{i})}{x^2 + y^2} = \frac{x^2 - (y\mathbf{i})^2}{x^2 + y^2} = \frac{x^2 - y^2\mathbf{i}^2}{x^2 + y^2} = \frac{x^2 + y^2}{x^2 + y^2} = 1.$$

Dass der Körper $(\mathbb{C}, +, \cdot)$ algebraisch abgeschlossen ist, ist ziemlich bemerkenswert. Bedenken Sie, dass wir nur die imaginäre Einheit \mathbf{i} eine formale Lösung der Polynomgleichung $z^2 + 1 = 0$ in einem unbekannten z eingeführt haben. Die Behauptung über die algebraische

Abgeschlossenheit ist, dass wird durch diese Ergänzung für eine beliebige Polynomgleichung von einem positiven Grad (und mit Koeffizienten in \mathbb{C}) eine Lösung in \mathbb{C} finden. Um diese Behauptung herzuleiten braucht man wissen aus der Analysis (wir geben also an dieser Stelle keinen Beweis). □

10.21 Aufgabe. Zeigen Sie $|uv| = |u| \cdot |v|$ für alle $u, v \in \mathbb{C}$.

10.22 (Der Satz von Pythagoras, Radianten und Grade, Kosinus und Sinus, und der Taschenrechner). Für das nachfolgende Thema soll man zuerst an das folgende Wissen aus der Schule erinnern.

zu C

- *Der Satz des Pythagoras.* Der Abstand zwischen dem Punkt $(0, 0) \in \mathbb{R}^2$ und dem Punkt $(x, y) \in \mathbb{R}^2$ ist gleich $\sqrt{x^2 + y^2}$. Wenn man diese Behauptung in einer koordinaten-freien Form mit Hilfe von rechtwinkligen Dreiecken formuliert, so nennt man sie den Satz des Pythagoras.
- *Der Wirrwarr um Radianten und Grade.* Im alten Babylonien dachte man, das Jahr wäre 360 Jahre lang (das stimmt nicht, wie wir jetzt wissen). Daher teilte man den Jahreskreis in 360 Teile auf, die den Tagen entsprechen. Ein Grad steht daher für einen Tag im babylonischen Jahreskreis. Das zeigt, dass die Herkunft der Messung der Winkel in Graden nicht mathematisch ist. Sie ist anthropologisch *und* hängt mit dem Planeten Erde zusammen.

men, auf dem wir uns befinden, und mit den Babylonier:innen, die bei der Bestimmung der Anzahl der Tage im Jahr sich ein Wenig verschätzten. Dennoch hat sich die Messung mit 360 Graden für den vollen Winkeln bis jetzt erhalten. Das liegt vielleicht daran, dass einige für uns interessante Winkel mit Graden durch eine ganze Zahl darstellbar sind (90° , 60° , 30°). Die Messung mit Radianten ist eine dimensionslose Messung und sie ist intrinsisch mathematisch. Man nimmt einen Kreis mit dem Radius 1 und misst Winkel durch die Längen der Bögen dieses Kreises. Dabei bezeichnet man die Länge einer Hälfte des Einheitskreises als π und nennt die Zahl π die Kreiszahl. Diese Zahl π ist etwas größer als 3 (das sieht man, wenn man in den Einheitskreis ein reguläres Sechseck einschreibt).

Ein Grad ist nichts Anderes als $1^\circ := \frac{\pi}{180} = \frac{2\pi}{360}$. Wenn man Winkel in Radianten misst, kann man etwa 1.2 Radianten aber auch einfach nur 1.2 sagen, denn die Einheit Radiant ist dimensionslos.

im Gegensatz zur Messung mit Graden

An sich gibt es an der Messung der Winkel mit Graden nichts Falsches. Dieser Kommentar dient einfach nur dazu, darauf hinzuweisen, dass die Zahlen wie 360 und 180 in Bezug auf die Winkelmessung keine mathematische sondern eine anthropologische Natur haben.

- *Kosinus und Sinus.* Man betrachte eine kreisförmige Radrennbahn mit Zentrum im Punkt $(0, 0)$ vom Radius 1. Diese Bahn ist nach dem Satz des Pythagoras durch die Gleichung $x^2 + y^2 = 1$ beschrieben. Nun legen wir den Punkt $(1, 0)$ dieser Bahn als den Startpunkt fest. Von diesem Punkt aus kann man nun Strecken einer beliebigen Länge zurücklegen. Wie lang die Strecke ist und ob man sich im Gegenuhrzeiger oder im Uhrzeigersinn bewegt wird durch eine Zahl $\alpha \in \mathbb{R}$ notiert. Der Betrag von α gibt die Länge der Strecke an, die man zurücklegen will. Das Vorzeichen von α gibt an, ob man sich im Gegenuhrzeigersinn oder im Uhrzeigersinn bewegt. Bei einem positiven Vorzeichen - im Gegenuhrzeigersinn und bei einem negativen Vorzeichen - im Uhrzeigersinn. Für jedes $\alpha \in \mathbb{R}$ erhält man

einen Punkt (x, y) , in dem man sich nach dem Zurücklegen der vorgegebenen Strecke in die vorgegebene Richtung landet. Die x -Komponente dieses Punkts nennt man den Kosinus von α (Bezeichnung: $x = \cos \alpha$) und die y -Komponente dieses Punkts nennt man den Sinus von α (Bezeichnung: $y = \sin \alpha$).

Die Eingabe für `cos` und `sin` ist also eine reelle Zahl und die Rückgabe ist oben beschrieben.

- *Kosinus und Sinus im Taschenrechner.* Wenn die Studierenden den Kosinus und Sinus (unter anderem für sehr einfache Werte α) im Taschenrechner berechnen, so sieht man, dass es immer wieder dazu kommt, dass ihre Ergebnisse falsch sind. Das liegt daran, dass man in vielen Taschenrechnern eine Umschaltung zwischen Grad und Radianten hat. Ist der Taschenrechner auf Radianten eingestellt, so berechnet er die eigentlichen Kosinus und Sinus, wie sie in Mathematik (und in den meisten Programmiersprachen) zu finden sind. Ist der Taschenrechner auf Grade eingestellt, so berechnet er die Funktionen $t \mapsto \cos(\frac{\pi}{180}t)$

und $t \mapsto \sin\left(\frac{\pi}{180}\right)t$ an der Stelle von \cos und \sin . Übrigens: in Excel wird die Funktion $t \mapsto \frac{\pi}{180}t$, die oben in \cos und \sin eingesetzt wurde, das Bogenmaß von t genannt.

- Die vielen Formeln, die man für den Kosinus und Sinus und andere trigonometrische Funktionen hat, lassen sich im Rahmen der linearen Algebra (IT-2) viel besser verstehen.



10.23 Thm. Jede komplexe Zahl $z \in \mathbb{C}$ besitzt eine Darstellung als

$$z = \rho(\cos \phi + \mathbf{i} \sin \phi)$$

mit $\rho \in \mathbb{R}_{\geq 0}$ und $\phi \in \mathbb{R}$. Hierbei gilt $\rho = |z|$. Bei $z \neq 0$, ist ϕ eindeutig durch z bis auf das addieren eines ganzzahligen Vielfachen von 2π definiert.

Beweis. **WARNUNG:** Der nachfolgende Beweis und unsere Definition von \cos und \sin entspricht nicht ganz den mathematischen Standards, solange wir den Begriff Länge (eines Bogens) und Orientierung (einer Kurve), auf den wir uns bei der Einführung von \cos und \sin beziehen, nicht mathematisch formal definiert haben. Wir verlassen uns also auf Intuition und darauf, dass man (später) den Begriff Länge mathematisch korrekt einführen kann (solche Begriffe führt man in der Analysis ein). Es gibt auch einen formalen nicht-geometrischen Zugang zum Kosinus und Sinus (dieser Zugang ist aber nicht wirklich intuitiv, sodass man dadurch nicht wirklich versteht,

was Kosinus und Sinus eigentlich sind).

Da jede komplexe Zahl $z = x + yi$ eindeutig durch $x, y \in \mathbb{R}$ gegeben ist, kann man z als einen Punkt $(x, y) \in \mathbb{R}^2$ visualisieren. Die Visualisierung von \mathbb{C} auf diese Weise nennt man die gaußsche Zahlenebene. Dabei werden 1 und i als die zueinander senkrechte Vektoren $(1, 0)$ und $(0, 1)$ dargestellt. Man sieht, dass die Menge $K := \{z \in \mathbb{C} : |z| = 1\} = \{x + iy : x^2 + y^2 = 1\}$ als der Einheitskreis mit Zentrum in $0 \in \mathbb{C}$ und dem Radius 1 in der gaußschen Zahlenebene darstellbar ist.

Existenz: Ist $z \neq 0$, so ist $z/|z|$ ein Punkt im Kreis K und so hat z die Darstellung $z/|z| = \cos \phi + i \sin \phi$ für ein $\phi \in \mathbb{R}$ nach unserer Beschreibung von \cos und \sin . Es folgt also, dass $z = \rho(\cos \phi + i \sin \phi)$ mit $\rho = |z|$ gilt. Im Fall $z = 0 \in \mathbb{C}$ kann man $\rho = 0$ und ein beliebiges ϕ fixieren.

Eindeutigkeit: Ist $z = \rho(\cos \phi + i \sin \phi)$ mit $\rho \in \mathbb{R}_{\geq 0}$ und $\phi \in \mathbb{R}$ so gilt $|z| = |\rho(\cos \phi + i \sin \phi)| = \rho |\cos \phi + i \sin \phi| = \rho \sqrt{\cos^2 \phi + \sin^2 \phi} = \rho$. Ist $z \neq 0$, so ist $z/|z|$ der Punkt

$\cos \phi + \mathbf{i} \sin \phi$ auf Einheitskreis K . Der Punkt $\cos \phi + \mathbf{i} \sin \phi$ im Kreis K ändert sich nicht, wenn man zum Wert von ϕ ein ganzzahliges Vielfaches von 2π dazu addiert, weil der Kreis K die Länge 2π hat. So besteht die Möglichkeit als ϕ einen Wert aus $[0, 2\pi)$ zu wählen.

Da K die Länge 2π hat, ist jeder Punkt eindeutig durch die Angabe eines solchen $\phi \in [0, 2\pi)$ gegeben. □

10.24 Def. Wir erweitern die Exponentialfunktion e^x auf \mathbb{R} auf den Bereich \mathbb{C} der komplexen Zahlen, in dem wir

$$e^{x+iy} := e^x (\cos y + i \sin y)$$

für alle $x, y \in \mathbb{R}$ festlegen. (Insbesondere, $e^{iy} = \cos y + i \sin y$).

$$\cos(\alpha \pm \beta) = \cos \alpha \cos \beta \mp \sin \alpha \sin \beta$$

$$\sin(\alpha \pm \beta) = \sin \alpha \cos \beta \pm \cos \alpha \sin \beta$$

In IT-2
kann man diese
Formeln herleiten.

$$(\cos \alpha + i \sin \alpha)(\cos \beta + i \sin \beta)$$

$$= (\cos \alpha \cos \beta - \sin \alpha \sin \beta) + (\cos \alpha \sin \beta + \sin \alpha \cos \beta)i$$

$$= \cos(\alpha + \beta) + i \sin(\alpha + \beta) \Rightarrow$$

Multiplikation von komplexen Zahlen entspricht:

- der Multiplikation der Beträge und
- Addition der Argumente

$$|z_1 \cdot z_2| = |z_1| \cdot |z_2| \quad \arg(z_1 \cdot z_2) = \arg z_1 + \arg z_2$$

10.25. Jede Zahl $z \in \mathbb{C}$ besitzt eine Darstellung $z = \rho e^{i\phi}$ mit $\rho = |z|$ und $\phi \in \mathbb{R}$.

\cup
 ϕ
 das ist eine Kurzschreibweise
 für $\cos \phi + i \sin \phi$

Sei volle Bezeichnung, denn die bekannten
 Rechenregeln für die Exponentialfunktion
 bleiben in \mathbb{C} gelten:

$$e^{i\varphi} \cdot e^{i\psi} = e^{i(\varphi+\psi)}$$

Die Euler-Formel reduziert Trigonometrie
 zur Algebra (oft sehr praktisch!)

11 Asymptotische Notation

11.1 O , Ω und Θ

11.1. Bei der Analyse von Algorithmen und der Analysis redet man oft von der Größenordnung von Funktionen. Eine praktische Ausdrucksweise dafür ist die sogenannte asymptotische Notation *(wird auch Landau-Symbole genannt!)*

11.2 Def (*O*-Notation). Seien $f, g : \mathbb{N} \rightarrow \mathbb{R}$ Funktionen. Man schreibt $f(n) = O(g(n))$, wenn eine Konstante $c > 0$ und ein $n_0 \in \mathbb{N}$ existiert, so dass $|f(n)| \leq c|g(n)|$ für alle $n \geq n_0$ gilt.

11.3. Die Bezeichnung $f(n) = O(g(n))$ steht für “ $f(n)$ hat die Größenordnung höchstens $g(n)$ bis auf eine multiplikative Konstante” und man sagt „ $f(n)$ ist in Groß-O von $g(n)$ “. Die Schreibweise $f(n) = O(g(n))$ ist streng genommen nicht ganz korrekt, in der Literatur aber sehr verbreitet. Die korrekte Schreibweise wäre $f(n) \in O(g(n))$, d.h., $f(n)$ liegt in der Menge aller Funktionen der Größenordnung höchstens $g(n)$. In der Literatur verwendet man oft $O(g(n))$ als eine Schreibweise für eine anonyme Funktion der Größenordnung höchstens $g(n)$. In diesem Kurs spielen die Beträge in der Definition von $O(g(n))$ in der Regel keine Rolle, weil wir beim Anwenden der asymptotischen Notationen fast ausschließlich nichtnegative Funktionen benutzen.

in dieser Form wird $= O$ am Stück
als eine
Relation zwischen f und g aufgeführt.

11.4 Def (Ω -Notation). Man schreibt $f(n) = \Omega(g(n))$, wenn eine Konstante $c > 0$ und ein $n_0 \in \mathbb{N}$ existieren, so dass $|f(n)| \geq c|g(n)|$ für alle $n \geq n_0$ gilt. In diesem Fall: Die Größenordnung von $f(n)$ ist mindestens $g(n)$, bis auf eine multiplikative Konstante und man sagt „ $f(n)$ ist in Groß-Omega von $g(n)$ “.

11.5 Def. Man schreibt $f(n) = \Theta(g(n))$, wenn sowohl $f(n) = O(g(n))$ als auch $f(n) = \Omega(g(n))$ gelten.

11.6. In diesem Fall: Die Größenordnung von $f(n)$ ist genau $g(n)$ bis auf eine multiplikative Konstante, und man sagt „ $f(n)$ ist in Groß-Theta von $g(n)$ “.

11.7. Die asymptotischen Notationen $O(g(n))$, $\Omega(g(n))$ und $\Theta(g(n))$ (und ihre weiteren Varianten) werden oft auch Landau-Symbole genannt.

11.8 Bsp. Sei $f : \mathbb{N} \rightarrow \mathbb{R}$ definiert durch $f(n) := \sqrt{2n+5} - 10$. Es gilt $f(n) = \Theta(\sqrt{n})$, denn einerseits ist $\sqrt{2n+5} - 10 \leq \sqrt{2n+5} \leq \sqrt{7n} = \sqrt{7}\sqrt{n}$ für alle $n \in \mathbb{N}$, woraus $f(n) = O(\sqrt{n})$ folgt. Andererseits ist $\sqrt{2n+5} - 10 \geq \sqrt{n} - 10 \geq \frac{1}{2}\sqrt{n}$ für alle $n \geq 400$, woraus $f(n) = \Omega(\sqrt{n})$ folgt.

11.9 Aufgabe. Sind die folgenden asymptotischen Abschätzungen richtig?

- $n! = O(n^n)$
- $n^n = \Omega(n!)$
- $n! = O(2^n)$
- $n^n = O(n!)$

11.10. Seien $f_1, f_2, g_1, g_2 : \mathbb{N} \rightarrow \mathbb{R}$ Funktionen, wobei g_1, g_2 nicht-negativ sind und $f_i(n) = O(g_i(n))$, für $i = 1, 2$, vorausgesetzt wird. Dann gilt

$$f_1(n) + f_2(n) = O(g_1(n) + g_2(n)) = O(\max\{g_1(n), g_2(n)\}),$$

und

$$f_1(n) \cdot f_2(n) = O(g_1(n) \cdot g_2(n)).$$

11.2 o und ω

11.11 Def. Bei $g : \mathbb{N} \rightarrow \mathbb{R}$ steht $o(g(n))$ für die Menge aller Funktionen $f : \mathbb{N} \rightarrow \mathbb{R}$ mit der Eigenschaft, dass für jedes $c > 0$ ein $n_0 \in \mathbb{N}$ existiert derart, dass $|f(n)| \leq c|g(n)|$ für alle $n \in \mathbb{N}$ mit $n \geq n_0$ erfüllt ist. In der Literatur schreibt man oft $f(n) = o(g(n))$ an der Stelle von $f(n) \in o(g(n))$.

11.12 Def. Die Bezeichnung $\omega(g(n))$ steht für die Menge aller Funktionen $f : \mathbb{N} \rightarrow \mathbb{R}$, für welche für alle $c > 0$ ein $n_0 \in \mathbb{N}$ existiert derart, dass $|f(n)| \geq c|g(n)|$ für alle $n \in \mathbb{N}$ mit $n \geq n_0$ erfüllt ist.

Kapitel III

Kombinatorik

1 Basics

1.1 Lemma. Seien A, B endliche disjunkte Mengen. Dann ist $|A \cup B| = |A| + |B|$.

1.2 Lemma. Seien A_1, \dots, A_n endliche paarweise disjunkte Mengen. Dann ist

$$\left| \bigcup_{i=1}^n A_i \right| = \sum_{i=1}^n |A_i|.$$

1.3 Lemma. Seien A und B endliche Mengen. Dann gilt

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

1.4 Lemma. Seien A und B endliche Menge. Dann gilt:

$$|A \times B| = |A| \cdot |B|.$$

2. X^K UND B^A

177

2 X^k **und** B^A

2.1 Thm. *Sei X eine endliche Menge und sei $k \in \mathbb{N}_0$. Dann ist $|X^k| = |X|^k$. (In dieser und den nachfolgenden kombinatorischen Formeln interpretieren wir 0^0 als 1.)*

Beweis. Die Formel ist trivial für in den entarteten Fällen $|X| = 0$ und $k = 0$. (für $k > 0$ und $X = \emptyset$ ist X^k ebenfalls die leere Menge und für $k = 0$ besteht X^k aus dem einzigen 0-Tupel). Wir nehmen also $|X| > 0$ und $k > 0$ an und beweisen die Gleichung $|X^k| = |X|^k$ in diesem Fall durch Induktion über k .

Die Formel ist trivial für $k = 1$: es gilt $|X^1| = |X|$ wegen $X^1 = X$. Sei $k \geq 2$ und sei die Formel $|X^{k-1}| = |X|^{k-1}$ bereits verifiziert.

Sei $n := |X|$. Dann ist X^k die disjunkte Vereinigung

$$X^k = \bigcup_{a \in X} X^{k-1} \times \{a\}.$$

der n Mengen $X^{k-1} \times \{a\}$. Mit anderen Worten zerlegen wir X^k in n paarweise disjunkte

Mengen, indem wir n verschiedene Möglichkeiten für die Wahl der letzten Komponente eines k -Tupels aus X^k unterscheiden. Nach Lemma 1.2 gilt dann

$$|X^k| = \sum_{a \in X} |X^{k-1} \times \{a\}|.$$

Es bleibt, für jedes feste $a \in X$, die Anzahl der Elemente in $X^{k-1} \times \{a\}$ zu bestimmen. Die Abbildung $f_a : X^{k-1} \times \{a\} \rightarrow X^k$ mit $f_a(x_1, \dots, x_{k-1}, a) = (x_1, \dots, x_{k-1}, a)$, welche die letzte Komponente des Tupels (x_1, \dots, x_{k-1}, a) weglässt ist eine Bijektion (begründen Sie kurz, warum). Daher hat $X^{k-1} \times \{a\}$ für jede Wahl von a genauso viele Elemente wie X^{k-1} . Es folgt

$$|X^k| = \sum_{a \in X} |X^{k-1} \times \{a\}| = \sum_{a \in X} |X^{k-1}|.$$

Nach der Induktionsvoraussetzung erhalten wir $|X^{k-1}| = |X|^{k-1}$. Da die Summe über die $|X|$ -elementige Menge geht, erhalten wir

$$|X^k| = |X| \cdot |X^{k-1}| = |X|^k.$$



2.2 Thm. Seien A, B endliche Mengen. Dann gilt $|B^A| = |B|^{|A|}$.

Beweis. Die Formel ist trivial, wenn A oder B leer ist. Seien A und B nicht leer. Sei $|A| = k$ und $A = \{a_1, \dots, a_k\}$. Dann ist die Abbildung $B^A \rightarrow B^k$, die jedem $f : A \rightarrow B$ das Tupel $(f(a_1), \dots, f(a_k))$ eine Bijektion. Somit gilt $|B^A| = |B^k| = |B|^k = |B|^{|A|}$. \square

3 $\binom{X}{k}$

4 Zählen der bijektiven und injektiven Abbildungen