Brückenkurs – Gesammelte Mitschriften

Tag 3, 06.10.2016 – Tag 9, 14.10.2016

1 Die natürlichen Zahlen und das Induktionsprinzip

1.1 Beispiel

Von Tag 2:

Satz

$$\Sigma_{k=1}^{n} k = \frac{1}{2} \cdot n \cdot (n+1)$$

Folgerung (*Korollar*)

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

Beweis

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

Mit Formel aus Satz auf die Formel angewendet:

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

Es wird zuerst die Summe aller Zahlen von 1 bis $2n$ addiert, danach die Summe aller geraden Zahlen abgezogen Hier auch implizite Verwendung der Assoziativität und Kommutivität der Addition.

1.2 Weiteres Beispiel

Satz Sei $x \neq 1$. Dann gilt: $\Sigma_{k=0}^{n} x^k = \frac{1-x^{n+1}}{1-x}$ („Geometrische Summe“)

Beispiel

$$1 + 2 + 4 + \ldots 2^{63} = \frac{1 - 2^{64}}{1-2} = 2^{64} - 1 = 18.446.744.073.709.551.615$$

Beweis 1 Ansatz der vollständigen Induktion:

$n = 0 \quad x^0 = 1; \frac{1-x^2}{1-x} = 1$ Formel stimmt also für $n = 0$

$n \implies n+1$

$$\Sigma_{k=0}^{n+1} x^k = x^{n+1} + \Sigma_{k=0}^{n} x^k = (I.V) x^{n+1} + \frac{1-x^{n+1}}{1-x} = \frac{x^{n+1}(1-x) + 1 - x^{n+1}}{1-x} = \frac{1-x^{n+2}}{1-x}$$

Beweis 2

$\Sigma_{k=0}^{n} x^k = \frac{1-x^{n+1}}{1-x} \Leftrightarrow (1-x)\Sigma_{k=0}^{n} x^k = 1 - x^{n+1} = \Sigma_{k=0}^{n} x^k - \Sigma_{k=0}^{n} x^{k+1} = \Sigma_{k=0}^{n} x^k - \Sigma_{k=1}^{n+1} x^k = x^0 - x^{n+1} = 1 - x^{n+1}$

Für $x \neq 1$. q.e.d.

1.3 Äquivalenz- und Induktionsprinzip

Satz Jede nicht-leere Teilmenge von $\mathbb{N}_0$ besitzt ein kleinstes Element. („ $\mathbb{N}_0$ ist *wohlgeordnet* “)

Beweis Sei $M \subseteq \mathbb{N}_0$ ohne kleinstes Element. Wir wollen zeigen dass: $M = \emptyset$, d.h. $P = \{n \in \mathbb{N}_0 | 0, 1, \ldots, n \notin M\} = \mathbb{N}_0$ Hierbei Anwendung des *Peano-Axioms*:

$0 \in P$ Wäre $0 \notin P$, so wäre $0 \in M$, insbesondere kleinstes Element von M. Dies ist ein Widerspruch, also $0 \in P$.

$n \in P \implies n+1 \in P$ Wäre $n+1 \notin P$. Dann wäre eine der Zahlen $0, \ldots, n+1 \in M$. Da aber nach Voraussetzung $n \in P$, ist $0, \ldots, n \notin M$. Also $n+1 \in M$. Insbesondere ist $n+1$ kleinstes Element. Widerspruch, also ist $n+1 \in P$.

2 Die ganzen und die rationalen Zahlen

2.1 Relation

Eine **Relation** auf einer Menge M ist eine Teilmenge $R \subseteq M \times M$ Wir schreiben $x \sim y :\Leftrightarrow .(x,y) \in R$ für $x, y \in M$.

Beispiel $x \leq y$ auf $\mathbb{N}_0$:
[Skizze: Punkte auf Gitter, $x, y \leq 4 \in \mathbb{N}_0$. Oberhalb und auf der Diagonale blaue Menge.]

	0	1	2	3	y
0	x				
1	x	x	x	x	
2	x		x		
3	x			x	
x					

Definition Eine Relation auf M heißt **Äquivalenzrelation**, falls sie:

1. **reflexiv** ist, d.h. $x \sim x$ für alle $x \in M$.
2. **symmetrisch** ist, d.h. $x \sim y \implies y \sim x$ für alle $x, y \in M$.
3. **transitiv** ist, d.h. $x \sim y \wedge y \sim z \implies x \sim z$ für alle $x, y, z \in M$.

Beispiel Die Gleichheitsrelation auf einer Menge ist eine Äquivalenzrelation

Beispiel Sei M eine Menge von Menschen. Die Relation „ist verwand mit“ (im Sinne von „gehört zur gleichen Familie“) ist eine Äquivalenzrelation.

Beispiel Sei M eine Menge von Menschen. Die Relation „hat im gleichen Monat Geburtstag“ ist eine Äquivalenzrelation.
Dabei ist $M = M_1 \cup M_2 \cup \ldots \cup M_{12}$. Die M_1 heißen die **Äquivalenzklassen** der Relation und stehen hier für die Monate.

Beispiel Relation $\sim$ auf Z mit $x \sim y :\Leftrightarrow x - y$ gerade. Ist reflexiv und symmetrisch. ist transitiv? $x \sim y, y \sim z \implies x - y$ gerade, $y - z$ gerade. $\implies (x-y)+(y-z) = x - z$ gerade $\implies x \sim z$ Ist also Äquivalenzrelation.

Äquivalenzklassen In diesem Beispiel: $Z = \{GeradeZahlen\} \cup \{UngeradeZahlen\}$

Definition Sei $\sim$ eine Relation auf einer Menge M. Für $x \in M$ heißt dann $[x]_{(\sim)} := \{y \in M | x \sim y\}$ die **Äquivalenzklasse** zu x.

Beispiel $[Peter]_{verwandt} = PetersFamilie$

Satz Es gilt für alle Äquivalenzrelationen auf eine Menge M mit $x, y \in M$:

1. $x \in [x]$
2. $x \sim y \implies [x] = [y]$
3. $[x] \neq [y] \implies [x] \cap [y] = \emptyset$

Beweis

1. $x \in [x] \Leftrightarrow x \sim x$ ok
2. Sei $x \sim y$ Zu **zeigen**: $[x] = [y]$.
   $z \in [x] \Leftrightarrow x \sim z \implies \overset{x\sim y}{y\sim x} y \sim z \Leftrightarrow z \in [y]$
3. Wir zeigen: $[x] \cap [y] \neq \emptyset \implies [x] = [y]$
   Es existiert also $z \in [x] \cap [y]$, d.h. $z \in [x]$ und $z \in [y]$, d.h. $x \sim z$, $y \sim z \implies x \sim y \implies x] = [y]$.

q.e.d.

Definition x heißt **Repräsentant** seiner Äquivalenzklasse $[x]$:
$M = \cup[x]$. $\{x$ Repräsentantensystem$\}$

Definition Sei R eine Äquivalenzrelation auf einer Menge M. Dann heißt ${}^{M}/_{R} := \{[x]_R | x \in R\}$ der **Quotioent von M nach R**.

2.2 Konstruktion der ganzen Zahlen

Erklärung ganzer Zahlen als Paar zweier natürlicher Zahlen. Dabei Subtraktion der Zahlen. Beispiel: Kontostand zusammengesetzt aus Einzahlungen und Abhebungen.

$(Einzahlungen, Abhebungen) \sim (Einzahlungen', Abhebungen') \Leftrightarrow E + A' = E' + A$ Auf der Menge der Paare (n, m) natürlicher Zahlen definieren wir die Relation $(n, m) \sim (a, b) :\Leftrightarrow n + b = m + a$
Es ist $\sim$ eine Äquivalenzrelation: Ist reflexiv und symmetrisch. Transitivität:

$(n, m) \sim (a, b) \wedge (a, b) \sim (u, v) \implies n+b = m+a \wedge a+v = b+u \implies u+b+a+v = m+a+b+u \implies n+v = m+u \implies (n, m) \sim$

Die Äquivalenzklasse zum Paar (n, m) heißt $[n, m]$

Beispiel $[3, 2] \sim [5, 4]$

Definition

$$Z = {}^{\mathbb{N}_0 \times \mathbb{N}_0}/_{\sim} = \{[n, m] \mid n, m \in \mathbb{N}_0\}$$

Jeder natürlichen Zahl n entspricht eine ganze Zahl $[n, 0]$. $\to \mathbb{N}_0 \subseteq Z$
$n \mapsto [n, 0]$.

Negative Zahlen $-[n, m] = [m, n]$

Beispiel $n \in \mathbb{N}_0$; $-n = -[n, 0] = [0, n]$ Ist diese Relation wohldefiniert? $-[7, 2] = [2, 7]$

Zu zeigen $[n, m] \sim [a, b] \implies [m, n] \sim [b, a]$
Begründung: Wenn $[n, m] \sim [a, b] \Leftrightarrow n + b = m + a \Leftrightarrow m + a = n + b \Leftrightarrow [m, n] \sim [b, a]$

Addition $[n, m] + [a, b] := [n + a, m + b]$

Multiplikation $[m, n] \cdot [a, b] := [ma + nb,\ na + mb]$

2.3 Rationale Zahlen

Auf der Menge $Z \times N_{>0}$ betrachten wir die Relation $(a, s) \sim (b, t) \Leftrightarrow a \cdot t = b \cdot s$

Rechnung $\sim$ ist Äquivalenzrelation. Die Äquivalenzklasse zu (a, s) bezeichnen wir mit $\frac{a}{s}$.
$\mathbb{Q} := {}^{\mathbb{Z}\times\mathbb{N}_0}/_{N}$

Addition

$$\frac{a}{s} + \frac{b}{t} := \frac{at + bs}{st}$$

$$\frac{b'}{t'} = \frac{b}{t} \Leftrightarrow tb' = t'b \implies \frac{at + bs}{st} = \frac{at' + b's}{st'} \Leftrightarrow t'b = tb'$$

2.4 Binomialkoeffizienten

Sei x eine (reelle) Zahl, $k \geq 0$ natürliche Zahl. Dann heißt $\left(\begin{array}{c} x \\ k \end{array} \right) := \frac{x \cdot (x-1) \cdot \dots \cdot (x-k+1)}{k!}$ der **Binomialkoeffizient** „x über k“.

Spezialfall Sei $0 \leq k \leq n$ eine natürliiche Zahl. Dann ist $\left(\begin{array}{c} n \\ k \end{array} \right) = \frac{n!}{k!(n-k)!}$

3 Binomialkoeffizienten

$k \in \mathbb{N}_0 : \binom{x}{k} = \frac{x \cdot (x-1) \cdot (x-2) \dots (x-k+1)}{k!}$

Dabei gilt:

$$\binom{n}{0} = 1, \quad \binom{0}{0} = 1, \quad \binom{0}{k} = 0$$

Spezialfall $0 \leq k \leq n \in \mathbb{N}_0$

$$\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!} \in \mathbb{Q}$$

Durch Experiment: $\in \mathbb{N}_0$

Aufgabe $\binom{x}{k} = \binom{x-1}{k-1} + \binom{x-1}{k}$ für $k \geq 1$

[Beispiel für rekursive Berechnung von $\binom{5}{3}$]

$$\binom{5}{3} = \binom{4}{2} + \binom{4}{3} = \binom{3}{1} + \binom{3}{2} + \binom{3}{2} + \binom{3}{3} = \dots = \binom{0}{\dots} + \dots + \binom{0}{\dots}$$

Satz Seien $k, n \in \mathbb{N}_0$. Dann ist die Anzahl der k-elementigen Teilmengen einer n-elementigen Menge M durch $\binom{n}{k}$ gegeben.

Beweis mit Induktion über n $n = 0$: $M = \emptyset$. Anzahl der k-elementigen Teilmengen von $M = \begin{cases} 1 & \text{für } k = 0 \\ 0 & \text{für } k > 0 \end{cases} \overset{stimmt}{=} \binom{0}{k}$ $n \Rightarrow n+1$: Sei $M = \{a_0, a_1, \dots, a_n\}$ $(n+1)$-elementig. Dann ist $M' := a_1, \dots, a_n$ n-elementig.

Sei $L \subseteq M$ eine k-elementige Teilmenge. Dann ist entweder $L = a_0 \cup L'$ mit $L' \subseteq (k-1)$-elementig oder $L \subseteq M'$, k-elementig. und alle k-elementigen Teilmengen $L \subseteq M$ entstehen eindeutig auf diese Weise.
Damit ist die Anzahl der k-elementigen Teilmengen von $M \overset{IV}{=} \binom{n}{k-1} + \binom{n}{k} \overset{Aufg.}{=} \binom{n+1}{k}$

Fall $k = 0$ trivial, daher $k > 0$.

q.e.d.

3.1 Anwendung

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

Beispiel

$$(x+y)^2 = \binom{2}{0} x^2 y^0 + \binom{2}{1} x^1 y^1 + \binom{2}{2} x^0 y^2 = x^2 + 2xy + y^2$$

$$(x+y)^3 = \binom{3}{0} x^3 y^0 + \binom{3}{1} x^2 y^1 + \binom{3}{2} x^1 y^2 + \binom{3}{3} x^0 y^3 = x^3 + 3x^2 y + 3xy^2 + y^3$$

Begründung

$$(x+y)^n = (x+y)(x+y)\dots(x+y) = \Sigma n\text{-fache Produkte} = \Sigma_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$$

Verständnisfrage: Was ist $\Sigma_{k=0}^{n} \binom{n}{k}$? $= |P(M)| = 2^n =$ Anzahl der Teilmengen einer n-elementigen Menge

4 Der euklidische Algorithmus

Im Folgenden: $d, n \in \mathbb{N}_0$

4.1 Definition

Die Zahl d **teilt** n, geschrieben $d|n$, falls $n = b \cdot d$ für ein $b \in \mathbb{Z}$.

Beispiele $2|100$, $11|165$, $-13|169$, 5X21.

4.2 Regeln

1. $1|n,\ n|n,\ d|0$
2. $0|d \implies d = 0,\ d|1 \implies d = \pm 1$
3. $d|n, n|m \implies d|m$
4. $d|a, d|b \implies d|(ax + bx)$ für alle $x, y \in \mathbb{Z}$
5. $bd|bn,\ b \neq 0 \implies d|n$
6. $d|n,\ n \neq 0 \implies |d| \leq |n|$ Jedes $n \neq 0$ hat nur endlich viele Teiler; insbesondere 1.
7. $d|n,\ n|d \implies d = \pm n$

Beweis von 4. Es gelte also $d|a, d|b$ d.h. $a = sd, b = td$ für $s, t \in \mathbb{Z}$ Damit ist $ax+by = sdx+tdy = (sx+ty)\cdot d$, also $d|ax + by$

Konsequenz Aus diesen Regeln ergibt sich, dass jede Zahl endlich viele Teiler hat, also haben je zwei $a, b \in \mathbb{Z}$ einen größten gemeinsamen Teiler, $ggT(a, b)$, wobei $ggT(0, 0) := 0$.

Es gilt

- $ggT(a, b)|a,\ \ ggT(a, b)|b.$
- $d|a,\ \ d|b \implies d|ggT(a, b).$

Beispiel $ggT(11, 14) = 1,\ ggT(21, 14) = 7,\ ggT(110, 140) = 10,\ ggT(210, 140) = 70.$

4.3 Satz: Division mit Rest

$a, b \in \mathbb{Z}$, $b \neq 0$. Dann existieren eindeutige $q, r \in \mathbb{Z}$ mit $a = bq + r$ mit $0 \leq r < |b|$.

Beweis $R = \{a - bq \mid q \in \mathbb{Z}\} \cap \mathbb{N}_0$ ist nicht leer. Diese besitzt ein kleinstes Element, welches das gesuchte $r = a - bq$ für das gewünschte q ist.
Bleibt zu zeigen: $r < |b|$. Dies folgt aus der Minimalität von $r \in R$.
q.e.d.

Folgerung Seien $a, b \in \mathbb{Z}$, $d = ggT(a, b)$. Dann $(d) := \{d \cdot n \in \mathbb{Z}\} = \{ax + by | x, y \in \mathbb{Z}\} =: (a, b)$.
Insbesondere läßt sich d in der Form $d = ax + by$ für gewisse $x, y \in \mathbb{Z}$ schreiben. (Beispiel: $ggT(9, 6) = 3 = 9 \cdot 1 + 6 \cdot (-1)$)

Beweis „$\supseteq$“ $ax + by \in (d) \Leftrightarrow d|(ax + by)$ (wg. 4. und $d|a$, $d|b$)
„$\subseteq$“ Es reicht zu zeigen, dass $d \in (a, b)$. Der Fall $a = 0$ ist einfach: Also sei $a \neq 0$.
Die Menge $M := ax + by | x, y \in \mathbb{Z} \cap \mathbb{N}_{\geq 1}$ ist nicht leer; damit besitzt sie ein kleinstes Element $m \geq 1$. Wir wissen schon (4.), dass $d|m$. Division mit Rest liefert $a = mq + r,\ 0 \leq r < m$.

Annahme $r > 0$. Dann ist $r = a - mq \in M$ **! Widerspruch !** Also $r = 0$, also $a = mq$, daher $m|a$.
Analog (mit b anstelle von a) erhalten wir $m|b$, also ist m gemeinsamer Teiler von a und b. Damit $m \leq d$. Zusammen mit $d \leq m$ folgt $d = m$. Somit $d \in (a, b)$.
$m \mid a, m \mid b \overset{iv}{\implies} m \mid ggT(a, b)$ $\square$

4.4 Praktische Bestimmung des ggT

$$\begin{array}{rcrcrcr} 117 & = & 3 & \cdot & 33 & + & 18 \\ 33 & = & 1 & \cdot & 18 & + & 15 \\ 18 & = & 1 & \cdot & 15 & + & 3 \\ 15 & = & 5 & \cdot & 3 & + & 0 \end{array}$$

Verbleibende Zahl $3 = ggT(117, 33)$.

4.5 Satz über den euklidischen Algorithmus

Seien $a, b \in \mathbb{N}_0$, $a \geq b \neq 0$.

$$\begin{array}{rcrcrcrl} a & = & q_1 & \cdot & b & + & r_1 & 0 \leq r_1 < b \\ b & = & q_2 & \cdot & r_1 & + & r_1 & 0 \leq r_2 < r_1 \\ r_1 & = & q_3 & \cdot & r_2 & + & r_1 & 0 \leq r_3 < r_2 \\ & & & & \vdots & & & \\ r_{n-2} & = & q_n & \cdot & r_{n-1} & + & r_1 & 0 \leq r_1 < b \\ r_{n-1} & = & q_{n+1} & \cdot & r_n & + & 0 & \end{array}$$

5 Primzahlen

5.1 Definition

Ein $p \in \mathbb{N}_0$ heißt **Primzahl**, wenn sie genau zwei positive Teiler besitzt.

5.2 Lemma von Euklid

Seien p eine Primzahl, $a, b \in \mathbb{Z}$. Dann: $p \,|\, (a \cdot b) \implies p \,|\, a \wedge p \,|\, b$

5.2.1 Beweis

Sei $d = ggT(p, a)$. Dann $d|p$. Nach Voraussetzung ist dann $d = 1$ oder $d = p$.

Fall 1: $d = p$ Dann $p|a$, da $p = ggT(p, a)$.

Fall 2: $d = 1$ Damit ist $1 = px + ay$ mit $x, y \in \mathbb{Z}$.
$\overset{b}{\implies} b = bpx + aby \overset{p|ab}{\implies} p|b$
□

5.3 Fundamentalsatz der Arithmetik

Satz Jede natürliche Zahl $n \geq 1$ besitzt eine eindeutige Primfaktorzerlegung („PFZ“), d.h. es existieren eindeutig bestimmte Zahlen $\nu_p(n) \in \mathbb{N}_0$ mit

$$n = \prod_{p \in \mathbb{P}} p^{\nu_p(n)}$$

Beispiel $60 = 2^2 \cdot 3^1 \cdot 5^1 \cdot 7^0 \ldots$ hier bspw.: $\nu_3(60) = 1$

Beweis

Existenz Sei $M = \{n \in \mathbb{N} \text{ mit } n \geq 1 \text{ ohne } PFZ\}$. Zu zeigen: $M = \emptyset$. Sei $n \in M$.
Dann ist jedenfalls n keine Primzahl, also existieren $2 \leq a, b < n$ mit $n = ab$. Damit muss $a \in M \vee b \in M$. Insbesondere ist n in M nicht kleinstes Element.
Also hat M kein kleinstes Element und $M = \emptyset$.

Eindeutigkeit Sei $n = p_1 \cdot p_2 \ldots p_r = q_1 \cdot q_2 \ldots q_s$ mit p_i, q_j Primzahlen.
$p_1 \,|\, p_1 \ldots p_r \implies p_1 \,|\, q_1 \ldots q_s \overset{Euklid}{\implies} p_1 \,|\, q_j$ für ein j. Da p_1, q_j Primzahlen $\implies p_1 = q_j$. Dann kürze mit $p_1 (= q_j)$ und mache mit p_2 weiter, ...

6 Primzahlen

Satz (Euklid) Es gibt undendlich viele Primzahlen.

Beweis Seien $p_0, \dots p_{n-1}$ Primzahlen.
Dann können wir eine Primzahl p_n konstruieren mit $p_n \notin \{p_0, \dots, p_{n-1}\}$: Dazu betrachte: $e := p_0 \dots p_{n-1} + 1 = q_1 \dots q_s$ mit Primzahlen $q_1, \dots, q_s$ (PFZ)
Da die $P - i$ jeweils e nicht teilen (Rest 1!), die q_j aber e teilen, sind die q_j von p_i verschieden. Damit ist $p_n := q_i$ die gesuchte Primzahl.

Beispiel

$$\begin{array}{rcccl} \emptyset & \rightsquigarrow & 1+1 & = & 2 = 2^1 \\ 2 & \rightsquigarrow & 2+1 & = & 3 = 3^1 \\ 2,3 & \rightsquigarrow & 2\cdot 3+1 & = & 7 = 7^1 \\ 2,3,7 & \rightsquigarrow & 2\cdot 3\cdot 7+1 & = & 43 = 43^1 \\ 2,3,7,43 & \rightsquigarrow & 2\cdot 3\cdot 7\cdot 43+1 & = & 1807 = 13\cdot 139 \end{array}$$

Primzahlsatz Sei $\pi(x)$ die Anzahl der Primzahlen $\leq x$. Dann gilt: $\pi(x) \approx \frac{x}{\ln x}$, d.h.

$$\lim_{x\to\infty} {}^{\pi(x)}/_{{}^{x}/_{\log x}} = 1$$

$$\pi(1) = 0, \pi(2) = 1, \pi(3) = 2, \pi(4) = 2, \pi(5) = 3, \pi(7,5) = 4, \cdots$$

Riemannsche Vermutung: $\Sigma_{n=1}^{\infty} \frac{1}{n^s} = \zeta(s)$
Sei p_n die n-te Primzahl ($p_0 = 2, p_1 = 3, \cdots$).

Behauptung $p_n < e^{2^n}$ (Konvention [1])

Beweis per Induktion über n **n=0**
$p_0 = 2; e^{2^0} = e^1 = e > 2$
$n \implies n+1$

$$p_{n+1} \overset{\text{Euklid}}{\leq} p_0 \dots p_n + 1 = e^{2^0+2^1+\cdots+2^n} + 1 = e^{2^{n+1}-1} + 1 = e^{2^{n+1}}(\frac{1}{e} + \frac{1}{e^{2^{n+1}}}) < e^{2^{n+1}} \quad \square$$

7 Algebraische Strukturen

7.1 Definition: Gruppe

Eine Gruppe ist eine Menge G zusammen mit einem ausgezeichneten Element $e \in G$ und einer Verknüpfung $\circ : G \times G \to G, (g,h) \mapsto g \circ h$, so dass folgende Axiome gelten:

(G1) Die Verknüpfung ist assoziativ: $g \circ (h \circ k) = (g \circ h) \circ k$ für $g, h, k \in G$

(G2) Das Element e ist neutrales Element: $e \circ g = g = g \circ e$ für $g \in G$

(G3) Jedes Element besitzt ein Inverses: Für alle $g \in G$ existiert ein $h \in G$ mit $g \circ h = e = h \circ g$

Die Gruppe heißt kommutativ (oder *abelsch*), falls zusätzlich gilt:

(G4) Die Verknüpfung ist kommutativ: $g \circ h = h \circ g$ für alle $g, h \in G$.

7.1.1 Beispiele

Beispiel $G = \mathbb{Z}, e = 0 \in \mathbb{Z}, \circ = + : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$

(G1) $g + (h + k) = (g + h) + k$ für alle $g, h, k \in \mathbb{Z}$

(G2) $0 + g = g = g + 0$ für alle $g \in \mathbb{Z}$

(G3) $g + (-g) = 0 = (-g) + g$ für alle $g \in \mathbb{Z}$

(G4) $g + h = h + g$

[1] $(a^b)^c = a^{b\cdot c}$, $a^{b^c} =: a^{b^c}$

Beispiel $(\mathbb{Q}, 0, +)$ ist genauso eine abelsche Gruppe.

Beispiel $(\mathbb{N}_0, 0, +)$ ist **keine Gruppe**.

Beispiel $(\mathbb{Z}, 1, \cdot)$ ist **keine Gruppe**, da G3 nicht erfüllt (z.B. existiert kein $n \in \mathbb{Z} mit 2 \cdot n = 1$).

Beispiel $(\mathbb{Q}, 1, \cdot)$ ist keine Gruppe, da G3 nicht erfüllt (Es existiert kein $x \in \mathbb{Q} mit 0 \cdot x = 1$)

Beispiel $(\mathbb{Q}*, 1, \cdot)$, wobei $\mathbb{Q}* := \mathbb{Q} \setminus 0$ ist eine Gruppe

Beispiel $(\mathbb{Q} \setminus \mathbb{Z}, 1, \cdot)$ ist alles, aber keine Gruppe

7.1.2 Aussage

Sei G eine Gruppe mit zwei neutralen Elementen e, e'. Dann gilt $e = e'$.

Beweis $e = e \circ e' = e'$, da e neutral und e' neutral. $\square$

Bemerkung Analog zeigt sich, dass das Inverse zu einem Element eindeutig bestimmt ist.

7.1.3 Aussage

Sei G eine Gruppe. Seien $a, b \in G$ mit Inversen a^{-1} bzw. $b^{-1} \in G$. Dann ist $b^{-1} \cdot a^{-1}$ invers zu $(a \circ b)$
$=: (a \circ b)^{-1}$

Beweis

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

Analog

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

Schreibweise Auch in abstrakten Gruppen schreiben wir häufig $\cdot$ statt $\circ$ für die Verknüpfung und 1 für das neutrale Element. **Abkürzung** $ab := a \cdot b, a^{-1} :=$ Inverses zu a.

Aussage Sei G eine (multiplikativ geschriebene) Gruppe. Für $a \in G$ gilt dann $(a^{-1})^{-1} = a$

Beweis $a \cdot a^{-1} = 1 = a^{-1} \cdot a \quad \square$

Beispiel [Gleichseitiges Dreieck mit gegen den Urzeigersinn nummerierten Ecken 1 - 3]
Symmetrien in der Ebene: $\left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\} =: G$
mit e, τ, σ.
Seien $g, h \in G$. Dann sei $g \cdot h$ die Hintereinanderausführung von h und danach g.

Beispiel

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

$\tau \circ \sigma = e$

Gruppentafel:

a \ b	e	σ	τ
e	e	σ	τ
σ	σ	τ	e
τ	τ	e	σ

Beispiel [Gleichseitiges Dreieck mit gegen den Urzeigersinn nummerierten Ecken 1 - 3]
Symmetrien im Raum:

$$\left\{\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\right\}$$

mit e, τ, σ, α_1, α_2, α_3.

$\alpha_1 \circ \sigma = \alpha_2$, $\sigma \circ \alpha_1 = \alpha 3 \neq \alpha_2 = \alpha 1 \circ \sigma$ Also nicht abelsch / kommutativ.

$$\alpha_1^2 = \alpha_1 \circ \alpha_1 = e \implies \alpha_1^{-1} = \alpha_1$$

Definition: symmetrische Gruppe Die **symmetrische Gruppe in n Buchstaben** ist die Gruppe der Permutationen von $1, \ldots, n$, geschrieben S_n, d.h. $S_n = \left\{\begin{pmatrix}1&2&\cdots&n\\\sigma_1&\sigma_2&\cdots&\sigma_n\end{pmatrix} | (\sigma_1, \cdots, \sigma_n) \text{ Permutationen von } (1, \cdots, n)\right\}$

Beispiel {Dreiecks-Symmetrie im Raum} $= S_3$

7.1.4 Definition: Untergruppe

Eine Teilmenge $U \subseteq G$ einer Gruppe G heißt **Untergruppe**, falls (U1) $e \in U$, (U2) $g, h \in U \implies g \circ h \in U$, (U3) $g \in U \implies g^{-1} \in U$

Beispiel {Dreiecks-Symmetrien in der Ebene} $\subseteq \{Dreiecks - SymmetrienimRaum\}$

Beispiel $\mathbb{Z} \subseteq (\mathbb{Q}, 0, +)$ ist Untergruppe

Beispiel $\mathbb{N}_0 \subseteq (\mathbb{Z}, 0, +)$ ist keine Untergruppe.

7.1.5 Definition: Kommutative Ringe

Ein **kommutativer Ring** ist eine Menge R zusammen mit zwei ausgezeichneten Elementen 0 und $1 \in R$ und zwei Verknüpfungen $+ : R \times R \mapsto R$ und $\cdot : R \times R \mapsto R$ so dass gilt:

(R1) $\forall x, y, z \in R : x + (y + z) = (x + y) + z$

(R2) $\forall x \in R : x + 0 = x = 0 + x$

(R3) $\forall x \in R \; \exists \, y \in R : x + y = 0 = y + x$

(R4) $\forall x, y \in R : x + y = y + x$

(R5) $\forall x, y, z \in R : x \cdot (y \cdot z) = (x \cdot y) \cdot z$

(R6) $\forall x \in R : x \cdot 1 = x = 1 \cdot x$

(R7) $\forall x, y \in R : x \cdot y = y \cdot x$

(R8) $\forall x, y, z \in R : x \cdot (y + z) = x \cdot y + x \cdot z \wedge (y + z) \cdot x = y \cdot x + u \cdot x$

Beispiel $(\mathbb{Z}, 0, 1, +, \cdot)$

Beispiel $(\mathbb{Q}, 0, 1, +, \cdot)$

Beispiel

Menge der Polynome bis X aus $\mathbb{Z}$ $\mathbb{Z}[X] = \{a_n X^n + \cdots + a_1 X + a_0 \mid a_0, \cdots, a_n \in \mathbb{Z}\}$

Beispiel $(\mathbb{Z}[X], 0, 1, +, \cdot)$
$(R[X], 0, 1, +, \cdot)$ falls R kommutativer Ring.

Bemerkung Ist $(R, 0, 1, +, \cdot)$ ein kommutativer Ring, so ist $(R, 0, +)$ eine abelsche Gruppe.

Definition Ist R ein kommutativer Ring, so $R* := \{x \in R \mid \exists\, y \in R : x \cdot y = 1 = y \cdot x\}$ Es ist $(R*, 1, \cdot)$ eine kommutative Gruppe, die **Einheitengruppe von** R.

Beispiel $\mathbb{Z}* = \{\pm 1\}, \mathbb{Q}* = \mathbb{Q} \setminus \{0\}$

Definition: Körper Ein **Körper** K der Menge ist ein kommutativer Ring für den Multiplikation und Addition abelsch definiert sind. Somit gelten für ihn die Axiome der abelschen Gruppen $(K, +, 0)$ und $(K, \cdot, 1)$ und das Distributivgesetz. Außerdem ist definiert: $K* = K \setminus \{0\}$

Beispiel $\mathbb{Q}$ und $\mathbb{R}$ sind Körper.

Beispiel $\mathbb{Q}(\sqrt{2}) := \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{R}$ ist ein Unterkörper.

$$0 = 0 + 0\sqrt{2}\ ,\ 1 = 1 + 0\sqrt{2}$$

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} -$$

7.4 Beispiele für Ringe

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}\mathbb{Z}[X], \mathbb{Q}[X], \mathbb{R}[X]$ (alle nullteilerfrei)

Beispiel Sei M eine Menge. Sei $R := P(M) = \{N \mid N \subseteq M\}$.
Wir definieren: $A + B := (A \cup B) \setminus (A \cap B)$, $A \cdot B = A \cap B$
[Venn-Diagramm aus Menge M mit $A + B$ und $A \cdot B$ markiert]
Sei $0 := \emptyset$, $1 := M$. Dann ist $(R = P(M), 0, 1, +, \cdot)$ ein kommutativer Ring.
Es gilt dann: $-A = A$, insbesondere $A + A = 2 \cdot A = 0$

Bemerkung Dieser Ring ist für $|M| \geq 2$ nicht **nullteilerfrei**:
Seien $A, B \in R; A \neq \emptyset; B \neq \emptyset; A \cap B = \emptyset$. Dann gilt: $A\dot{B} = 0$, aber $A \neq 0, B \neq 0$.

Anmerkung Im Ring $\mathbb{Z}$ gibt es immer eine eindeutige Primfaktorzerlegung. Für $\mathbb{Q}[X]$ gibt es irreduzible Polynome, die sich nicht als Produkt anderer Polynome schreiben lassen:
$x^2 - 1 = (x - 1)(x + 1)$ ist reduzibel.
$X^2 + 1$ hingegen ist irreduzibel.
$x^3 - 1 = (x - 1)(x^2 + x + 1)$ wurde in zwei irreduzible Polynome zerlegt.

8 Rechnen mit Restklassen

8.1 Satz („9er Probe“)

$9 \mid \sum_{j=0}^{n} a_j \cdot 10^j \Leftrightarrow 9 \mid \sum_{j=0}^{n} a_j$, wobei $a_j \in \mathbb{Z}$.

Beispiel $9|123456789 \Leftrightarrow 9|(1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9) \Leftrightarrow 9|45$

8.2 Definition: Kongruenz

Sei $n \in \mathbb{Z}$. Sind dann $a, b \in \mathbb{Z}$, so heißen a und b **kongruent modulo m**, falls $m|(a - b)$, d.h. der Rest der Division von a beziehungsweise b durch m ist gleich soweit $m \neq 0$. Wir schreiben dann $a \equiv b(m)$.

Beispiel $5 \equiv 7(2), 8 \equiv 3(5), 9 \equiv -1(10), 4 \equiv 14(1), -3 \equiv -3(0)$

Proposition $\equiv (m)$ ist eine Äquivalenzrelation.

Beweis

$$a \equiv a(m); a \equiv b(m) \Rightarrow b \equiv a(m)$$

$$a \equiv b(m), b \equiv c(m) \Rightarrow a \equiv c(m) : m|(a - b), m|(c - b) \Rightarrow \exists\, d, e \in \mathbb{Z} : a - b = dm, c - b = e, \Rightarrow m|(c - a)$$

8.3 Definition: Restklassen

Die Äquivalenzklassen modulo m heißen **Restklassen modulo m**.

Beispiel $m = 3$
$[0]_3 = \{\cdots, -3, 0, 3, 6, \cdots\}$
$[1]_3 = \{\cdots, -2, 1, 4, 7, \cdots\} = [4]_3$

Proposition $a \equiv a'(m), b \equiv b'(m)$. Dann gilt:

1. $a + b \equiv a' + b'(m)$
2. $a \cdot b \equiv a' \cdot b'(m)$

Beweis

- $(a + b) - (a' + b') = (a - a') + (b - b')$ ist durch m teilbar, also 1.
- $a \cdot b - a' \cdot b' = a \cdot b - a' \cdot b + a' \cdot b - a' \cdot b' = (a - a') \cdot b + a'(b - b')$ ist durch m teilbar, also 2.

8.4 Der Körper $\mathbb{F}_3$

Damit können wir definieren: $[a]_m + [b]_m := [a + b]_m$ und $[a]_m \cdot [b]_m := [a \cdot b]_m$.
Die Mege der Restklassen modulo m ${}^{\mathbb{Z}}/_{\equiv(m)}$ bezeichnen wir auch mit ${}^{\mathbb{Z}}/_{(m)}$
Es ist $\left({}^{\mathbb{Z}}/_{(m)}, [0]_m, [1]_m, +, \cdot\right)$ ein kommutativer Ring, der **Restklassenring modulo m**.

Beispiel $m = 3$

$+$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[1]$	$[2]$
$[1]$	$[1]$	$[2]$	$[0]$
$[2]$	$[2]$	$[0]$	$[1]$

$\cdot$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$
$[2]$	$[0]$	$[2]$	$[1]$

Dieser Körper wird $\mathbb{F}_3$ genannt.

8.5 Beweis (9er Probe)

$$9 | \sum_{j=0}^{n} a_j \cdot 10^j \Leftrightarrow \sum_{j=0}^{n} a_j \cdot 10^j \equiv 0(9) \Leftrightarrow \sum_{j=0}^{n} a_j \cdot 1^j \equiv 0(9) \Leftrightarrow 9 | \sum_{j=0}^{n} a_j$$

9 Konvergente und divergente Folgen

Beispiele für Folgen

- $1, 3, 5, 7, 9, 11, 13, \cdots$
- $1, 4, 9, 16, 25, \cdots$
- $1, 3, 2, 4, 3, 5, 4, 6, 5, 7, 6, 8, \cdots$

Definition Eine **Folge** a (reeller Zahlen) ist eine Abbildung $a : \mathbb{N}_0 \to \mathbb{R}, n \mapsto a_n$
Für diese Abbildung schreiben wir auch $(a_n)_n \in \mathbb{N}_0$.

Beispiele

- $a_n = n : (a_n)_{n \in \mathbb{N}_0} = (0, 1, 2, 3, \cdots)$
- $b_n = \frac{1}{n} : (b_n)_{n \in \mathbb{N}_{\geq 1}} = (1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4} \cdots)$
- $c_n = \frac{(-1)^n}{n} : (c_n)_{n \in \mathbb{N}_{\geq 1}} = (-1, \frac{1}{2}, -\frac{1}{3}, \frac{1}{2}, \cdots)$

Beispiel: Fibonacci-Folge

$$(F_n)_{n\geq 0} \text{ , wobei } F_0 = 0, F_1 = 1, F_n + 2 = F_n + F_{n+1}$$

$$\rightsquigarrow (F_n)_{n\geq 0} = (0, 1, 1, 2, 3, 5, 8, 13, 21, 34, \cdots)$$

$$x^2 = 2y^2 + 1 : (3, 2); (17, 12); (99, 70), \cdots$$

$$\rightarrow \text{ Folge: } \frac{3}{2}, \frac{17}{12}, \frac{99}{70}, \cdots \rightsquigarrow \sqrt{2}$$

Definition Eine Folge $(a_n)_{n\geq 0}$ heißt **konvergent mit Grenzwert** a, falls $\forall \varepsilon > 0\, \exists\, n_0 : \forall n \geq n_0 : |a_n - a| < \varepsilon$
Wir schreiben dann: $\lim_{n\to\infty} a_n = a$

Beispiel $(b_n) = (\frac{1}{n})$. $\lim_{n\to\infty} \frac{1}{n} = 0$.
Zu untersuchen: $|\frac{1}{n} - 0| = \frac{1}{n} < \varepsilon$.
Sei $\varepsilon > 0$ vorgegeben. Dann wähle $n_0 \in \mathbb{N}_{\geq 1}$ mit $\frac{1}{n_0} < \varepsilon$. Für $n \geq n_0$ gilt dann: $\frac{1}{n} \leq \frac{1}{n_0} < \varepsilon$

Definition Eine Folge (a_n), für die kein a mit $\lim_{n\to\infty} a_n = a$ existiert, heißt **divergent**.

Beispiel $(a_n) = (-1)^n : 1, -1, 1, -1, \cdots$ divergiert.
Annahme: a wäre Grenzwert. Dann gäbe es insbesondere zu $\varepsilon = \frac{1}{2}$ ein n_0 mit $|a_n - a| < \frac{1}{2}$ für $n \geq n_0$.
Damit $|a_{n_0} - a| + |a_{n_0+1} - a| < 1$.

9.1 Einschub: Dreiecksungleichung

$\forall x, y \in \mathbb{R} : |x + y| \leq |x| + |y|$

Beweis

$$x \leq |x|, y \leq |y| \Rightarrow x + y \leq |x| + |y|$$
$$-x \leq |x|, -y \leq |y| \Rightarrow -(x + y) \leq |x| + |y|$$
$$\Longrightarrow |x + y| \leq |x| + |y| \quad \square$$

Fortsetzung

Nach Dreiecks-Ungleichung: $|a_{n_0} - a + (a - a_{n_0+1})| < 1$, also $|a_{n_0} - a_{n_0+1}| < 1$
Widerspruch! Die Funktion divergiert also.

9.2

Proposition Sind (a_n) und (b_n) Folgen mit $\lim_{n\to\infty} a_n = a$, $\lim_{n\to\infty} b_n = b$ so gilt:

1. $\lim_{n\to\infty}(a_n + b_n) = \lim_{n\to\infty} a_n + \lim_{n\to\infty} b_n$
2. $\lim_{n\to\infty}(a_n \cdot b_n) = (\lim_{n\to\infty} a_n \cdot \lim_{n\to\infty} b_n)$
3. $\lim_{n\to\infty} \frac{a_n}{b_n} = \frac{\lim_{n\to\infty} a_n}{\lim_{n\to\infty} b_n}$, falls $b \neq 0$

Beispiel

$$\lim_{n\to\infty} \frac{2n^2 - 3}{n^2 + n + 1} = \lim_{n\to\infty} \frac{2 - \frac{3}{n^2}}{1 + \frac{1}{n} + \frac{1}{n^2}} = \frac{\lim_{n\to\infty}(2 - \frac{3}{n^1})}{\lim_{n\to\infty}(1 + \frac{1}{n} + \frac{1}{n^2})} = \frac{\lim_{n\to\infty} 2 + \lim_{n\to\infty}(-\frac{3}{n^2})}{\lim_{n\to\infty} 1 + \lim_{n\to\infty} \frac{1}{n} + \lim_{n\to\infty} \frac{1}{n^2}} = \frac{2 + 0}{1 + 0 + 0} = 2$$

Beweis zu 1. Zu zeigen: $\forall \varepsilon > 0 \exists n_0 : \forall n \geq n_0 : |a_n + b_n - a - b| < \varepsilon$
Sei $\varepsilon > 0$ vorgegeben.
Da $\lim_{n\to\infty} a_n = a$ und $\lim_{n\to\infty} b_n = b$ existieren n_1, n_2 mit $\forall n \geq n_1 : |a_n - a| < \frac{\varepsilon}{2}$ und $\forall n \geq n_2 : |b_n - b| < \frac{\varepsilon}{2}$
Für $n \geq max(n_1, n_2) = n_0 : |a_n + b_n - a - b| \leq |a_n - a| + |b_n - b| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$

9.3 Beispiel: Fibonacci-Folge, die Zweite

$F_0 = 0, F_1 = 1, F_2 = 1, F_3 = 2, F_4 = 3, 5, 8, 13, 21, \cdots$

$$\frac{F_{n+1}}{F_n} : \frac{1}{1}, \frac{2}{1}, \frac{3}{2}, \frac{5}{3}, \frac{8}{5}, \cdots \overset{?}{\to} \phi := \frac{1}{2}(1+\sqrt{5})$$

Satz (Bichet) Es gilt: $F_n = \frac{1}{\sqrt{5}}(\varphi^n - \overline{\varphi}^n)$, wobei $\overline{\varphi} := \frac{1}{2}(1-\sqrt{5})$

Korollar

$$\lim_{n\to\infty} \frac{F_{n+1}}{F_n} = \varphi$$

Beweis

$$\lim_{n\to\infty} \frac{F_{n+1}}{F_n} = \lim_{n\to\infty} \frac{\varphi^{n+1} - \overline{\varphi}^{n+1}}{\varphi^n - \overline{\varphi}^n} = \lim_{n\to\infty} \frac{\varphi}{1} = \varphi$$

Satz Die Folge $(x^k)_{k\in\mathbb{N}_0}$ konvergiert für $|x| < 1$ gegen 0.

Beweis Zu betrachten: Abstand x^k zu 0 für große $k \to |x^k|$ Wir müssen $|x^k - 0| = |x|^k$ abschätzen. Ohne Beschränkung der Allgemeinheit sei $0 \le x < 1$.
Da $x < 1$, ist $\frac{1}{x} = 1 + y$ für $y > 0$. Damit ist $\frac{1}{x^n} = (1+y)^n = 1 + 1 + \binom{n}{2}y^2 + \ldots + \binom{n}{n}y^n \ge 1 + n \cdot y$
Also $x^n \le \frac{1}{1+n\cdot y} < \frac{1}{n\cdot y}$ Ist also $\varepsilon > 0$ vorgegeben, so wähle $n_0 \ge \frac{1}{\varepsilon y}$.
Für alle $n \ge n_0$ ist dann $|x^n| < \varepsilon_0$

Fibonacci-Satz $\varphi := \frac{1}{2}(1+\sqrt{5}), \overline{\varphi} := \frac{1}{2}(1-\sqrt{5})$. Dann gilt: $F_n = \frac{1}{\sqrt{5}}(\varphi^n - \overline{\varphi}^n)$

Beweis Es gilt: $\varphi^2 = \varphi + 1$ und $\overline{\varphi}^2 = \overline{\varphi} + 1$, also $X^2 - X - 1 = (X - \varphi)(X - \overline{\varphi})$
Dann Induktion über n:
n = 0: $F_0 = 0 \overset{\checkmark}{=} \frac{1}{\sqrt{5}}(\varphi^0 - \overline{\varphi}^0)$
n = 1: $F_1 = 1 \overset{\checkmark}{=} \frac{1}{\sqrt{5}}(\varphi^1 - \overline{\varphi}^1)$
n, n+1 → n + 2:

$$F_n + F_{n+1} \overset{IV}{=} \frac{1}{\sqrt{5}}(\varphi^n - \overline{\varphi}^n) + (\varphi^{n+1} - \overline{\varphi}^{n+1}) = \frac{1}{\sqrt{5}}\left(\varphi^n(1+\varphi) - \overline{\varphi}^n(1+\overline{\varphi})\right) = \frac{1}{\sqrt{5}}(\varphi^n\varphi^2 - \overline{\varphi}^n\overline{\varphi}^2) = \frac{1}{\sqrt{5}}(\varphi^{n+2} - \overline{\varphi}^{n+2}) \quad \square$$

9.4 Heron-Verfahren

Sei $a_0 = 1, a_{n+1} = \frac{1}{2}(a_n + \frac{2}{a_n})$
$a_0 = 1; a_1 = \frac{3}{2}; a_2 = \frac{17}{12} = 1,41\overline{6}; a_3 = \frac{577}{408} = 1,414215\ldots$

Vermutung Die Folge $(a_n)_{n\ge 0}$ konvergiert gegen $\sqrt{2} = 1,414213562\ldots$

Beweisskizze Wir zeigen unter der Annahme, dass die Folge konvergiert, dass
$a := \lim_{n\to\infty} a_n = \sqrt{2} : a = \lim_{n\to\infty} a_{n+1} = \lim_{n\to\infty} \frac{1}{2}(a_n + \frac{2}{a_n}) = \frac{1}{2}((\lim_{n\to\infty} a_n) + \frac{2}{\lim_{n\to\infty} a_n}) = \frac{1}{2}(a + \frac{2}{a})$
$\implies 2a^2 = a^+2 \implies a^2 = 2 \overset{a>0}{\implies} a = \sqrt{2}$

Aufgabe Finde ein Verfahren zur Berechnung von $\sqrt{13}$.

9.5 Unendliche Reihen und Dezimalbrüche

Sei (a_k) eine Folge. Dann heißt $s_n := \sum_{k=0}^{n} a_k = a_0 + a_1 + \ldots + a_n$ die n-te Partielsumme zur Folge (a_k).
Der Grenzwert $\lim_{n\to\infty} s_n = \lim_{n\to\infty} \sum_{k=0}^{n} a_k =: \sum_{k=0}^{\infty} a_k = a_0 + a_1 + a_2 + a_3 + \ldots$ heißt die **Reihe** zur Folge (a_k).
Im Falle, dass der Grenzwert gar nicht existiert, sagen wir, die Reihe **divergiere**.

Satz Für $|x| < 1$ gilt: $\sum_{n=0}^{\infty} x^n = \frac{1}{1-x}$ („Geometrische Reihe“)

Beispiel $x = {}^1/_2$
$\sum_{n=0}^{\infty}(\frac{1}{2})^n = 1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \ldots \overset{\text{Satz}}{=} \frac{1}{1-{}^1/_2} = 2$

Beweis Schon bekannt: $\sum_{k=0}^{n} x^k = \frac{1-x^{n+1}}{1-x}$.
Damit ist $\sum_{k=0}^{\infty} x^k = \lim_{n\to\infty} \frac{1-x^{n+1}}{1-x} = \frac{1-\lim_{n\to\infty} x^{n+1}}{1-x} = \frac{1-0}{1-x} = \frac{1}{1-x}$ $\square$

Beispiel $\sum_{n=1}^{\infty} \frac{1}{n} = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \ldots$ („*harmonische Reihe*“) konvergiert nicht (in $\mathbb{R}$):

$$\frac{1}{3} + \frac{1}{4} \geq \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$$
$$\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} \geq \frac{4}{8} = \frac{1}{2}$$
$$\frac{1}{9} + \ldots + \frac{1}{16} \geq \frac{8}{16} = \frac{1}{2}$$

Wir sehen: Die Folge der Partialsummen ist unbeschränkt.

Warnung $\lim_{k\to\infty} a_k = 0 \overset{\text{i. allg.}}{\Rightarrow} \sum_{k=0}^{\infty} a_k$ konvergiert.

Satz $\sum_{k=0}^{\infty} a_k$ konvergiert in $\mathbb{R} \implies \lim_{k\to\infty} a_k = 0$

Beweis Sei $a := \sum_{k=0}^{\infty} a_k$. Sei $\varepsilon > 0$ vorgegeben. Dann existiert ein n_0, so dass $|\sum_{k=0}^{n-1} a_k - a| < \frac{\varepsilon}{2}$ für alle $n \geq n_0$.
Damit gilt:
$|a_n| = |\sum_{k=0}^{n} a_k - \sum_{k=0}^{n-1} a_k| = |(\sum_{k=0}^{n} a_k - a) - (\sum_{k=0}^{n-1} a_k - a)| \leq |\sum_{k=0}^{n} a_k - a| + |\sum_{k=0}^{n-1} a_k - a| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$ für $n \geq n_0$.

10 Zahlen als konvergente Reihen

Jede reelle Zahl α ist konvergente Reihe: $\alpha = \sum_{k=0}^{\infty} a_k \cdot 10^{-k}$, wobei $a_0 \in \mathbb{Z}; a_k = \{0, \ldots, 9\}$ für $k > 0$.

Beispiel $\pi = 3 + 1 \cdot 10^{-1} + 4 \cdot 10^{-2} + 1 \cdot 10^{-3} + \ldots = 3,141\ldots$

Warnung $1,00000\ldots = 0,99999\ldots$ Die Dezimaldarstellung ist im Zweifelsfall nicht eindeutig.

Satz Die Reie α beschreibt genau dann eine rationale Zahl, wenn die Folge der a_k (also die Dezimalbruchdarstellung) periodisch ist.

Beispiel $0,142857142857\ldots = 0,\overline{142857}$ ist rational $(= \frac{1}{7})$
$0,5 = 0,5\overline{0}$ ist rational $(= \frac{1}{2})$
$0,123456789101112131415\ldots$ ist irrational (da nicht periodisch)

Beweis $\implies$: Sei $\alpha = \frac{u}{v}$ eine rationale Zahl: $u \in \mathbb{Z}; v \in \mathbb{N}_{>0}$
Bsp: $\frac{3}{7} = 0,\overline{428571}$ (Beispiel mit schriftlicher Division an der Tafel)
Bei der schriftlichen Division tauchen höchstens v viele Reste auf, das heißt die Dezimalbruchdarstellung von α hat ist periodisch mit der Periodelänge höchstens v.
$\impliedby$: Sei α periodisch, etwa $\alpha = a_0,\ a_1\, a_2\, \overline{a_3\, a_4\, a_5}$
Dann ist $\alpha = a + a_1 10^{-1} + a_2 10^{-2} + (100a_3 + 10a_4 + a_5) \cdot (10^{-5} + 10^{-8} + 10^{-11} + \ldots)$ [2]

Beispiel $0,121212\ldots = \frac{12}{100} \cdot \frac{100}{99} = \frac{12}{99} = \frac{4}{33}$

10.0.1 Die Eulersche Zahl

Sei $x \in \mathbb{R}$. Dann sei $exp(x) := \sum_{n=0}^{\infty} = \frac{x^n}{n!} = 1 + x + \frac{x^2}{2} + \frac{x^3}{6} + \ldots$

[2] $(10^{-5} + 10^{-8} + 10^{-11} + \ldots) = 10^{-5}(1 + 10^{-3} + 10^{-6} + \ldots)$

Bemerkungen

- In der Analysis wird die Konvergenz für alle x gezeigt.
- Ebenfalls wird dort $exp(x) = e^x$)

Die Zahl $e := exp(1) = \sum_{n=0}^{\infty} \frac{1}{n!} = 1 + 1 + \frac{1}{2} + \frac{1}{6} + \ldots = 2,7182818284\ldots$ heißt **eulersche Zahl**.

Satz e ist irrational.

Beweis **Annahme**: $e = \frac{a}{b}; a, b \in \mathbb{Z}; b > 0$. Sei $m \geq b$ eine ganze Zahl. Dann $b|m!$.
Also $\alpha := m!(e - \sum_{n_0}^{m} \frac{1}{n!}) = a\frac{m!}{b} - \sum_{n=0}^{m} \frac{m!}{n!} \in \mathbb{Z}$.
Aber:

$$\alpha = \sum_{n=m+1}^{\infty} \frac{m!}{n!} \leq \sum_{n=m+1}^{\infty} \frac{m!}{m! \cdot (m+1)^{n-m}} = \frac{1}{m+1} \cdot \sum_{k=0}^{\infty} \frac{1}{(m+1)^k} = \frac{1}{m+1} \cdot \frac{1}{1 - \frac{1}{m+1}} = \frac{1}{m}$$

Widerspruch! $\overset{0 \leq \alpha < 1}{\Longrightarrow}$ α kann nicht als ganze Zahl geschrieben werden.

11 Abzählbarkeit und Überabzählbarkeit

Sei $f : M \to N$ eine Abbildung[3].

Definition f heißt

1. **injektiv**, falls $\forall x, y \in M : (f(x) = f(y) \Rightarrow x = y)$
2. **surjektiv**, falls $\forall z \in N \, \exists \, x \in M : f(x) = z$
3. **bijektiv**, falls f *injektiv* und *surjektiv* ist.

Definition Zwei Mengen M und N heißen **gleichmächtig**, falls eine Bijektion $f : M \Rightarrow N$ existiert.
Eine Menge M heißt **abzählbar**, wenn sie gleichmächtig zu $\mathbb{N}_0$ ist.
Eine unendliche, nicht abzählbare Menge heißt **überabzählbar**.

Beispiel $\mathbb{N}_0$ ist abzählbar. $(0 \mapsto 0, 1 \mapsto 1, 2 \mapsto 2, 3 \mapsto 3, \ldots)$

Beispiel $\mathbb{Z}$ ist abzählbar. $(0 \mapsto 0, 1 \mapsto 1, -1 \mapsto 2, 2 \mapsto 3, -2 \mapsto 4, \ldots)$

Exkurs: Gedankenexperiment – Hilberts Hotel Hotel mit unendlich vielen Zimmern, alle Zimmer sind belegt. Ein Gast kommt hinzu. Kann dieser ein Zimmer bekommen? Ja: Der Portier fordert alle Gäste auf, in das nächste Zimmer zu ziehen.

Beispiel $\mathbb{Q}$ ist abzählbar: $0, \frac{1}{1}, -\frac{1}{1}, \frac{2}{1}, -\frac{2}{1}, \frac{1}{2}, -\frac{1}{2}, \ldots$

Satz (Cantor) $\mathbb{R}$ ist überabzählbar.

Beweis Annahme: $\mathbb{R}$ ist abzählbar. Dann gibt es eine Liste aller reeller Zahlen.
$\alpha^{(0)} = a_0^{(0)}\,,\, a_1^{(0)}\, a_2^{(0)}\, a_3^{(0)}\, a_4^{(0)} \ldots$

$\alpha^{(1)} = a_0^{(1)}\,,\, a_1^{(1)}\, a_2^{(1)}\, a_3^{(1)}\, a_4^{(1)} \ldots$

$\alpha^{(2)} = a_0^{(2)}\,,\, a_1^{(2)}\, a_2^{(2)}\, a_3^{(2)}\, a_4^{(2)} \ldots$

$\vdots$

In Dezimaldarstellung ohne Neunerperiode.
Dann betrachte die reelle Zahl $\beta = b_0\,,\, b_1 b_2 b_3 \ldots$, wobei wir die b_is so wählen, dass $b_i \neq a_i^{(i)}$
Dann taucht β in der Liste gar nicht auf.
Somit **Widerspruch!**: $\mathbb{R}$ ist überabzählbar.
Dieses Vorgehen heißt Cantorsches Diagonalargument.

[3] Widerspricht nicht, dass ein Element aus N nicht oder mehrfach zugeordnet wird

12 Die komplexen Zahlen

$\mathbb{N}_0 \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

Beispiel $X^2 + 10X - 144 = 0$

Lösungsansatz Quadratische Ergänzung
$X^2 + 2 \cdot 5 \cdot X + 5^2 - 5^2 - 144 = 0 \Leftrightarrow (X+5)^2 = 169 \Leftrightarrow X + 5 = \pm\sqrt{169} = \pm 13 \Leftrightarrow X = -5 \pm 13 = -18, 8$

Allgemein $X^2 + pX + q = 0$

Lösung $\Leftrightarrow X^2 + pX + (\frac{p}{2})^2 - (\frac{p}{2})^2 + q = 0 \Leftrightarrow (X + \frac{p}{2})^2 - (\frac{p}{2})^2 + q = 0 \Leftrightarrow (X + \frac{p}{2})^2 = (\frac{p}{2})^2 - q \Leftrightarrow$
$\Leftrightarrow X + \frac{p}{2} = \pm\frac{1}{2}\sqrt{p^2 - 4q} \Leftrightarrow X = -\frac{p}{2} \pm \frac{1}{2}\sqrt{p^2 - 4q}$

Definition $\Delta := p^2 - 4q$ heißt die **Diskriminante** der Gleichung / des quadratischen Polynoms.
Drei Fälle, jeweils in $\mathbb{R}$:

1. **Fall:** $\Delta > 0$: 2 (verschiedene) Lösungen
2. **Fall:** $\Delta = 0$: 1 Lösungen
3. **Fall:** $\Delta < 0$: Keine Lösungen

[Darstellung: Funktion $X^2 + pX + q$ in Koordinatensystem für $\Delta = 0$, $\Delta < 0$ und $\Delta > 0$]

Vergleiche $X^2 - 2 = 0$ hat in $\mathbb{Q}$ keine Lösung, da 8 kein Quadrat in $\mathbb{Q}$ ist.
$X^2 + 1 = 0$ hat in $\mathbb{R}$ keine Lösung, da -4 kein Quadrat in $\mathbb{R}$.

12.1 Die Imaginäre Einheit

Wir suchen einen Körper $\mathbb{C}$, in dem wir $X^2 + 1 = 0$ lösen können. Damit muss ein $i \in \mathbb{C}$ existieren mit $i^2 = -1$, die sogenannte **imaginäre Einheit**.
Angenommen, ein solches $\mathbb{C}$ existiert. Sind dann $a, b \in \mathbb{R}$, so ist $a + b \cdot i \in \mathbb{C}$.

12.2 Rechnen in $\mathbb{C}$

Addition $(a + b \cdot i) + (c + d \cdot i) = (a + c) + (b + d)i$

Multiplikation $(a + bi) \cdot (c + di) = ac + adi + cbi + bd \cdot i^2 = (ac - bd) + (ad + bc)i$ [4]
Die Menge der Ausdrücke der Form $a + bi; a, b \in \mathbb{R}$, wobei $i^2 = -1$ bildet einen kommutativen Ring, der $\mathbb{R}$ umfasst.

Multiplikative Inversen $\frac{1}{a+bi} = \frac{a-bi}{(a+bi)(a-bi)} = \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i$, wobei $a \neq 0 b \neq 0$
Die Rechnung zeigt, dass $(a + bi)^{-1}$ existiert, nämlich $(a + bi)^{-1} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i$

Satz Die Menge $\mathbb{C} := \{a + bi | a, b \in \mathbb{R}\}$, wobei $i^2 = -1$, bildet einen Oberkörper von $\mathbb{R}$ den **Körper der komplexen Zahlen**.

Warnung $\mathbb{C}$ ist kein angeordneter Körper[5]: Angenommen, es gibt eine Anordnung, die mit den arithmetischen Operationen verträglich ist.
Fall $i > 0$: $\implies i^2 > 0 \implies -1 > 0 \implies 1 < 0$ **Widerspruch zu „Quadrate sind nicht negativ“**
Fall $i < 0$: $\implies (-i)^2 > 0 \implies$ **Ebenfalls Widerspruch**

12.3 Komplexe Zahlenebene

[Darstellung: Ebene komplexer Zahlen statt Zahlenstrahl. Betrag der komplexen Zahl ist Abstand vom Ursprung]

[4] $bdi^2 = -bd$, da qua Definition $i^2 = -1$
[5] Das heißt: In $\mathbb{C}$: Wenn $a < b, c < d$ gilt **nicht** $a + c < b + d$

Definition Ist $z = a + bi \in \mathbb{C}; a, b \in \mathbb{R}$, so heißt $|z| := \sqrt{a^2 + b^2}$ der **Betrag von** z.

Proposition

1. $|z| \geq 0$
2. $|z| = 0 \Leftrightarrow z = 0$

Aufgabe $|z + w| \leq |z| + |w|$ für alle $z, w \in \mathbb{C}$.

Proposition $|z \cdot w| = |z| \cdot |w|$ für alle $z, w \in \mathbb{C}$.

Beweis $(a + bi) \cdot (c + di) = ac - bd + (ad + bc)i \implies |(a + bi)(c + di)|^2 = (ac - bd)^2 + (ad + bc)^2 =$
$= |a + bi|^2 \cdot |c + di|^2 = (a^2 + b^2) \cdot (c^2 + d^2)$

12.4 Alternative Darstellung

Eine komplexe Zahl $z = a + bi$ lässt sich auch in der Form $z = r(\cos\varphi + i \sin\varphi)$ schreiben. Hierbei ist $r \in \mathbb{R}_{\geq 0}$ der **Betrag** $|z|$ von z und $\varphi \in \mathbb{R}$ heißt das **Argument**.

Multiplikation

$$r(\cos\varphi + i\sin\varphi) \cdot r'(\cos\varphi' + \sin\varphi') = r \cdot r'((\cos\varphi \cdot \cos\varphi' - \sin\varphi\sin\varphi') + i(\cos\varphi\sin\varphi' + \sin\varphi\cos fgft\varphi')) =$$

$$= rr'(\cos(\varphi + \varphi') + i\sin(\varphi + \varphi'))$$

Erfolg In $\mathbb{C}$ hat jede quadratische Gleichung $X^2 + pX + q = 0$ (mindestens) eine Lösung, nämlich $X = -\frac{p}{2} \pm \frac{1}{2}\sqrt{\Delta}$, $\Delta = p^2 - 4q$.
$\sqrt{-5} = \sqrt{-1} \cdot \sqrt{5} = \pm i\sqrt{5}$
$\sqrt{r(\cos\varphi + i\sin\varphi)} = \pm\sqrt{r} \cdot (\cos{}^{\varphi}/_{2} + i\sin{}^{\varphi}/_{2})$

12.5 Kubische Gleichungen

$X^3 + aX^2 + bX + c = 0$

Ansatz $X^3 + aX^2\frac{1}{3}a^2X + \frac{1}{27}a^3 + (b - \frac{1}{3}a^2)X + (c - \frac{1}{27}a^3) = (X + \frac{a}{3})^3 + (b - \frac{1}{3}a^2)X + (c - \frac{1}{27}a^3)$ Setze $Y := X + \frac{a}{3}$

$Y^3 + (b - \frac{1}{3}a^2)(Y - \frac{a}{3}) + (c - \frac{1}{27}a^3)$
$= Y^3 + (b - \frac{1}{3}a^2)Y + (c - \frac{ab}{3} + \frac{2a^3}{27})$ Setze $p := b - \frac{1}{3}a^2, q := c - \frac{ab}{3} + \frac{2a^3}{27}$
$= Y^3 + pY + q$ (*Kubik in reduzierter Form*)
Es reicht damit, Gleichungen der Form $Y^3 + pY + q = 0$ zu lösen.

Ansatz $Y = U + V$. Dann $(U + V)^3 + p(U + V) + q = U^3 + 3U^2V + 3UV^2 + V^3 + pU + pV + q$

Ansatz $U^3 + V^3 = -q$. Dann $3U^2V + 3UV^2 + pU + pV = 0 = (3 \cdot UV + p) \cdot U + (3 \cdot UV + p) \cdot V$.

Ansatz $U \cdot V = -\frac{p}{3}$, daraus $U^3 \cdot V^3 = -\frac{p}{27}$

Lösung $V^3 = -q - U^3$. Also: $U^3(-q - U^3) = -\frac{p^3}{27} \Leftrightarrow (U^3)^2 + qU^3 - \frac{p^3}{27} = 0 \Leftrightarrow U^3 = -\frac{q}{2} \pm \frac{1}{2}\sqrt{q^2 + \frac{4p^3}{27}} \Leftrightarrow$
$\Leftrightarrow U = \sqrt[3]{-\frac{q}{2} \pm \frac{1}{2}\sqrt{q^2 + \frac{4p^3}{27}}}, \quad V = -\frac{p}{3U}, \quad Y = U + V, X = Y - \frac{a}{3}$

12.6 Gaussscher Fundamentalsatz der Algebra

$\mathbb{C}$ ist **algebraisch abgeschlossen**, das heißt: Jedes nicht konstante Polynom hat in $\mathbb{C}$ eine Nullstelle.
$P(X) \in \mathbb{C}[X]$, deg. $P(X) = n > 0$. Nach dem FdA[6] existiert $z_1 \in \mathbb{C}$ mit $P(z_1) = 0$.
Polynomdivision: $P(X) = (X - z_1) \cdot Q(X) + R$, deg. $Q(X) = n - 1$, $\quad \mathbb{R} \in \mathbb{C}$. Wegen $P(z_1) = 0$ sogar $R = 0$.
Dann machen wir mit $Q(X)$ anstelle $P(X)$ weiter, usw.
$\rightsquigarrow P(X) = (X - z_1) \cdot Q(X) = (X - z_1)(X - z_2) \cdot \overline{Q}(X) = \ldots = c \cdot (X - z_1)/cdot(X - z_2) \cdots (X - Z_n)$.
Insbesondere lässt sich jedes Polynom über $\mathbb{C}$ als Produkt linearer Polynome schreiben.

Beweis $\quad P(Z) = Z^d + a_1 Z^{d-1} + \ldots + a_{d-1} Z + a_d; \quad a_i \in \mathbb{C}$

$$\lim_{|Z| \to \infty} |P(X)| = \lim_{|Z| \to \infty} |Z^d (1 + a_1 Z^{-1} + \ldots + a_d Z^{-d})| \leq \lim_{|z| \to \infty} |z|^d (1 + |a_1| \cdot |z|^{-1} + \ldots + |a_d| \cdot |z^{-d}|) = \infty$$

Damit nimmt $|P(Z)|$ an einer Stelle $z_0 \in \mathbb{C}$ ihr Minimum an. Das heißt: $\forall a \in \mathbb{C} : |P(a)| \geq |P(z_0)|$

Annahme $\quad |P(z_0)| > 0$ (sonst $|P(z_0)| = 0$, also $P(z_0) = 0$, also hätten wir Nullstellen)
$W = Z - z_0 \Leftrightarrow Z = W + z_0; \quad P(Z) = a + bW^n + W^{n+1} \cdot Q(W)$, $a, b \in \mathbb{C}$, $Q(W) \in \mathbb{C}[W]$
Bei $W = 0$ nimmt $P(Z)$ betraglich sein Minimum an.
Wähle $\omega \in \mathbb{C}$ mit $\omega^n = -\frac{a}{b}$. Dann ist $\delta |\omega^{n+1} \cdot Q(\delta \cdot \omega)| < |a|$ für geeignetes $\delta > 0$.
$P(\delta \cdot \omega) = a + b \cdot \delta^n \cdot \omega^n + \delta^{n+1} \cdot \omega^{n+1} \cdot Q(\delta \cdot \omega) = a(1 - \delta^n) + \delta^{n+1} \cdot \omega^{n+1} \cdot Q(\delta \cdot \omega)$
$\implies |P(\delta\omega)| \leq |a| \cdot |1 - \delta^n| + \delta^{n+1} |\omega^{n+1} Q(\delta\omega)| < |a| \cdot |1 - \delta^n| + |a| \cdot \delta^n \leq |a| = |P(z_0)|$

13 Auswahlaxiom, Zornsches Lemma und Ultrafilter

13.1 Auswahlaxiom

Definition Ist M eine Menge nicht-leerer Mengen, so existiert dazu eine Auswahlmenge, das heißt: eine Menge X, so dass $\forall U \in M \exists ! \, a \in U.$ mit $a \in X$[7].
Sei Z eine Menge, $\mathscr{X} \subseteq P(Z)$, also ist $\mathscr{X}$ eine Menge von Teilmengen von Z.

Definition Eine **Kette in** $\mathscr{X}$ ist eine Teilmenge $\mathscr{Y} \subseteq \mathscr{X}$ mit $\forall Y_1, Y_2 \in \mathscr{Y} : Y_1 \subseteq Y_2 \wedge Y_2 \subseteq Y_1$

13.2 Zornsches Lemma

Sei $Z, \mathscr{X}$ wie eben. Zusätzlich gelte:

1. Ist $X' \subseteq X \in \mathscr{X}$, so auch $X' \in \mathscr{X}$
2. Ist $\mathscr{Y} \subseteq \mathscr{X}$ eine Kette, so ist $\cup \mathscr{Y} = \cup Y \in \mathscr{X}$.

Dann besitzt $\mathscr{X}$ ein **maximales Element** $X_0 \in \mathscr{X}$ bzgl. „$\subseteq$“, d.h. $\forall X \in \mathscr{X} : X \supseteq X_0 \implies X = X_0$

Beweisidee

- Wegen 2. (Wähle $\mathscr{Y} = \emptyset \subseteq \mathscr{X}$ (Kette)) ist $\emptyset = \cup \emptyset \in \mathscr{X}$.
- Falls $\emptyset$ maximal in $\mathscr{X}$, sind wir fertig.
- Ansonsten gibt es $X_1 \in \mathscr{X}$ mit $X_0 \subsetneqq X_1$.
- Entweder ist X_1 maximal oder wir machen weiter …
  $X_0 \subsetneqq X_1 \subsetneqq X_2 \subsetneqq X_3 \subsetneqq \ldots \subsetneqq X_\omega$

Breche der Prozess nicht ab (ansonsten wären wir nach $n \in \mathbb{N}_0$ Schritten fertig.)
Wegen 2. ist $X_\omega = \cup_{i=0}^{\infty} X_i \in \mathscr{X}$.
Ist X_ω immer noch nicht maximal, so finden wir $X_\omega \subsetneqq X_{\omega+1} \subsetneqq \ldots \subsetneqq X_{\omega+n} \subsetneqq \ldots$
Bricht dies immer noch nicht ab, so ist $X_{\omega \cdot 2} = \cup_{n=0}^{\infty} X_{\omega+n}$ der nächste Kandidat.
$X_0 \subsetneqq X_1 \subsetneqq X_2 \subsetneqq \ldots X_\omega$
$X_\omega \subsetneqq X_{\omega+1} \subsetneqq X_{\omega+2} \subsetneqq X_{\omega+3} \subsetneqq \ldots \subsetneqq X_{\omega \cdot 2}$
$X_{\omega \cdot 2} \subsetneqq X_{\omega \cdot 2+1} \subsetneqq X_{\omega \cdot 2+2} \subsetneqq X_{\omega \cdot 2+3} \subsetneqq \ldots \subsetneqq X_{\omega \cdot 3}$

[6] Fundamentalsatz der Algebra
[7] $\exists !$ bedeutet: „es existiert genau ein Element“

Korollar Sei $(Z, \leq)$ eine **teilweise geordnete** Menge, das heißt es gilt:

1. $\forall z \in Z : z \leq z$.
2. $\forall x, y \in Z : x \leq y \wedge y \leq x \implies x = y$
3. $\forall x, y, z \in Z : x \leq y \wedge y \leq z \implies x \leq z$

Besitzt dann jede **Kette** Y in Z (d.h. jede vollständig geordnete Teilmenge von $Y \subseteq Z$) eine **obere Schranke** in Z, das heißt $\exists z \in Z \forall y \in Y : y \leq z$, dann besitzt Z ein maximales Element $z_0 \in Z$, das heißt $\forall z \in Z : z \geq z_0 \implies z = z_0$.

Beweis Sei $\mathscr{X} \subseteq P(Z)$ die Menge der Ketten von $(Z, \leq)$. Dann sind 1. und 2. vom Zornschen Lemma erfüllt. Damit existiert eine maximale Kette $X_0 \in \mathscr{X}$.
Nach Voraussetzung des Korollars besitzt X_0 eine obere Schranke $z_0 \in Z$.

Annahme z_0 ist nicht maximal, das heißt es existiert $z_1 \in Z$ mit $z_1 \geq z_0, z_1 \neq z_0$. Dann wäre aber $X_0 \cup \{z_1\}$ eine echt größere Kette als X_0. Dies wäre aber ein **Widerspruch** zur Maximalität von X_0.

13.3 Ultrafilter

Definition Sei X eine Menge. Ein **Filter** F auf X ist eine Teilmenge $F \subseteq P(X)$ mit

1. $X \in F$
2. $\emptyset \notin F$
3. $\forall A \in F : B \supseteq A \Rightarrow B \in F$
4. $\forall A, B \in F \Rightarrow A \cap B \in F$

Beispiel Sei $x_0 \in X$ ein Element einer Menge. Dann ist $F := \{A \subseteq X | x_0 \in A\}$ ein Filter, der von x_0 erzeugte Filter.
Filter, die nicht von einem Element erzeugt werden, heißen **frei**.

Beispiel Sei S eine unendlich große Menge. Dann ist $F := \{A \subseteq X | X \backslash A \text{ endlich}\}$ ein Filter, der sogenannte **Fréchet-Filter** auf X.

Definition Ein **Ultrafilter** auf X ist ein Filter mit 5. $\forall A \subseteq X : A \in F \vee X \setminus A \in F$.

Beispiel Nicht freie Filter[8] sind Ultrafilter.

Frage Gibt es freie Ultrafilter?

Satz Ist F ein Filter auf X, so gibt es einen Ultrafilter $\hat{X}$ auf X mit $F \subseteq \hat{F}$.

Folgerung Auf jeder unendlichen Menge gibt es einen freien Ultrafilter.

Beweis (Folgerung) Wähle einen Ultrafilter, der den Fréchet-Filter umfasst. □

Beweis (Satz) Sei Z die Menge der Filter $\widetilde{F}$ mit $\widetilde{F} \supseteq F$. Es ist Z bezüglich „$\subseteq$“ teilweise geordnet. Jede Kette $\mathbb{F}$ in Z, also jede Kette von Filtern besitzt eine obere Schranke in Z, nämlich $\cup_{\widetilde{F} \in F} \widetilde{F}$.
Zu überprüfen, dass dies ein Filter ist, also in Z liegt.
z.B. Filgereigenschaft 4. : $A, B \in \cup_{\widetilde{F} \in \mathbb{F}} \widetilde{F} \stackrel{?}{\Rightarrow} A \cap B \in \cup_{\tilde{F} \in \mathbb{F}} \mathbb{F}$
$\rightsquigarrow$ Da $\mathbb{F}$ Kette, $\tilde{F}_1 \subseteq \tilde{F}_2$ oder $\tilde{F}_2 \subseteq \tilde{F}_1$. Ohne Beschränkung der Allgemeinheit: $\tilde{F}_1 \subseteq \tilde{F}_2$.
Also $A, B \in \tilde{F}_2 \Rightarrow A \cap B \in \tilde{F}_2 \in \mathbb{F} \Rightarrow A \cap B \in \cup\mathbb{F}$.
Nach Zorn besitzt Z ein maximales Element $\hat{F}$.
Behauptung: $\hat{F}$ ist Ultrafilter.
Begründung Unter der Annahme, dass $\hat{F}$ ein Ultrafilter ist, gibt es ein $A \subseteq X$ mit $A \notin \hat{F}$ und $X \setminus A \notin \hat{F}$.
Definition: $\mathscr{G} := \{G \subseteq X | \exists F \in \hat{F} : G \supseteq F \cap A\}$
Damit ist $\mathscr{G}$ ein Filter; wegen $A \in \mathscr{G}$, aber $A \notin \hat{F}$ ist $\hat{F} \neq \mathscr{G}$. Aber $\hat{F} \subseteq \mathscr{G}$.
Damit $\hat{F}$ nicht maximal. **Widerspruch!** □

[8] Bspw. Fréchet-Filter