Course Notes

Ausgewählte Kapitel der Mathematik 1+2
(Selected Topics in Mathematics 1+2)

Daniel Smertnig

Summer Term 2022
University of Graz

for pedagogical students in the master's program, 2+1h/week

made available online: 17.5.2026

1. Zahlmengen („Verdiefende Wiederholung")

$\mathbb{N} = \{1, 2, 3, \dots\}$ ⊂ $\mathbb{N}_0 = \{0, 1, 2, 3, \dots\}$ } $(\mathbb{N}, \cdot)$, $(\mathbb{N}_0, +)$ sind (kommutative) Monoide (Mengen mit assoziativer Verknüpfung und neutralem Element).
Distributivgesetz: $(\mathbb{N}_0, +, \cdot)$ ist (kommutativer) Halbring.

⊂

$\mathbb{Z}$ ... jedes Element hat zusätzlich ein additives Inverses, $(\mathbb{Z}, +)$ ist Gruppe, $(\mathbb{Z}, +, \cdot)$ Ring

⊂

$\mathbb{Q}$ ... jede Zahl $\neq 0$ hat zusätzlich ein multiplikatives Inverses, $(\mathbb{Q}\setminus\{0\}, \cdot)$ ist Gruppe, $(\mathbb{Q}, +, \cdot)$ Körper

⊂

$\mathbb{R}$ ... Vervollständigung von $\mathbb{Q}$: keine „Lücken" ($\sqrt{2} \notin \mathbb{Q}$), bzw. jede Cauchy-Folge konvergiert (→ Analysis)

⊂

$\mathbb{C}$ ... Jedes nicht-konstante Polynom besitzt eine Nullstelle, und zerfällt deshalb in Linearfaktoren (algebraischer Abschluss)

1.1 Die nicht-negativen ganzen Zahlen

Anschaulich: – Zählen endlich vieler Objekte unserer Anschauung
– Addition & Ordnung spiegeln das wieder.

Um diese Zahlen einer rigorosen math. Argumentation zugänglich zu machen, müssen wir uns darauf einigen welche grundlegenden Eigenschaften sie haben, und alles andere daraus ableiten (→ PEANO Axiome; 1889; Dedekind 1888)

Def: Ein Tripel $(N, 0, S)$ bestehend aus einer Menge N, einem Element $0 \in N$ und einer Abbildung $S: N \to N$ heißt Peano-System, wenn gilt:

(P1) $0 \notin S(N)$

(P2) S ist injektiv $[\Leftrightarrow \forall m, n \in N: S(m) = S(n) \Rightarrow m = n]$

(P3) Ist $A \subseteq N$ und gilt
(i) $0 \in A$ und
(ii) $\forall n \in A: S(n) \in A$ $[\Leftrightarrow S(A) \subseteq A]$, (Induktionsaxiom)
dann ist $A = N$.

Idee: $0 = \emptyset$, $1 := S(0)$, $2 = S(1) = S(S(0))$, $3 = S(2) = S(S(S(0)))$

Peanosysteme $(N, 0, S)$ und $(N', 0', S')$ heißen isomorph, wenn es eine bijektive Abbildung $f: N \to N'$ gibt, so dass gilt:

(i) $f(0) = 0'$, und

(ii) $\forall n \in S: \quad f(S(n)) = S'(f(n))$.

D.h. $0 \leftrightarrow 0'$, $1 = S(0) \leftrightarrow S(0') = 1'$, $2 = S(1) = S'(1') = 2'$, ...

Satz 1.1 Je zwei Peanosysteme sind eindeutig isomorph. (d.h., es gibt genau einen Isomorphismus)
(ohne Beweis)

Wir konstruieren nun ein Peanosystem, weil je zwei Peanosysteme ein eindeutiger Weise isomorph sind, können wir dieses als DIE nicht-negativen ganzen Zahlen $\mathbb{N}_0$ betrachten.

Setze $0_{\mathbb{N}} := \emptyset$

$1_{\mathbb{N}} := \{\emptyset\} = \{0_{\mathbb{N}}\}$

$2_{\mathbb{N}} := \{\emptyset\} \cup \{\{\emptyset\}\} = \{\emptyset, \{\emptyset\}\} = \{0_{\mathbb{N}}, 1_{\mathbb{N}}\}$

$3_{\mathbb{N}} := \{\emptyset, \{\emptyset\}\} \cup \{\{\emptyset, \{\emptyset\}\}\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} = \{0_{\mathbb{N}}, 1_{\mathbb{N}}, 2_{\mathbb{N}}\}$

$\vdots$

Allgemein: $S(A) = A \cup \{A\}$, beginnend mit $A = \emptyset$

Sei nun $\mathbb{N}_0 := \{0_{\mathbb{N}}, 1_{\mathbb{N}}, 2_{\mathbb{N}}, \ldots\}$ die Menge all dieser Mengen (Auslassung!), und $S: \mathbb{N}_0 \to \mathbb{N}_0$, $A \mapsto A \cup \{A\}$, $\mathbb{N} := \mathbb{N}_0 \setminus \{0\}$

Satz 1.2 $(\mathbb{N}_0, 0_{\mathbb{N}}, S)$ ist ein Peanosystem.

Beweisskizze: Da wir nur eine naive, und keine axiomatische, Mengenlehre zugrunde legen, können wir keinen völlig zufriedenstellenden Beweis geben, aber wir können einen solchen skizzieren.

(P2): Sei $S(m_{\mathbb{N}}) = S(n_{\mathbb{N}})$ und $m_{\mathbb{N}} \neq n_{\mathbb{N}}$.

$m_{\mathbb{N}} \cup \{m_{\mathbb{N}}\} = n_{\mathbb{N}} \cup \{n_{\mathbb{N}}\} \Longrightarrow m_{\mathbb{N}} \in n_{\mathbb{N}}$ und $n_{\mathbb{N}} \in m_{\mathbb{N}}$ ↯ (Regularitätsaxiom)

(P1) Angenommen $\exists m_{\mathbb{N}} \in \mathbb{N}_0$: $S(m_{\mathbb{N}}) = 0_{\mathbb{N}} = \emptyset$

$\Rightarrow m_{\mathbb{N}} \in S(m_{\mathbb{N}}) = \emptyset$ ↯

(P3) Heuristisch ✓ (rigoroses Argument benötigt präzise Def. von $\mathbb{N}_0$) □

Wir lassen nun das Subskript „$\mathbb{N}$" wieder weg.

Prop 1.3 Für alle $n \in \mathbb{N}$ gibt es genau ein $m \in \mathbb{N}_0$ mit $S(m) = n$, d.h. $\mathbb{N}_0 = S(\mathbb{N}_0) \cup \{0\}$.
(m heißt Vorgänger von n.)

Bew: Existenz: Benutzen (P3). Sei $A := \{0\} \cup \{n \in \mathbb{N} : \exists m \in \mathbb{N}_0 : S(m) = n\}$

z.z. $A = \mathbb{N}_0$

$0 \in A$ ✓ Sei $n \in A$. $\overset{z.z.}{\Rightarrow} S(n) \in A$ Dann ist n Vorgänger von $S(n)$, also $S(n) \in A$.

Eindeutigkeit: S ist injektiv (P2) □

Es gibt also eine Abbildung $P: \mathbb{N} \to \mathbb{N}_0$, so dass $P \circ S = id_{\mathbb{N}_0}$ und $S \circ P = id_{\mathbb{N}}$.

Definition: Seien $m, n \in \mathbb{N}_0$

(1) $$m + n := \begin{cases} m & \text{falls } n = 0 \\ S(m + P(n)) & \text{falls } n \neq 0 \end{cases}$$

(2) $$m \cdot n := \begin{cases} 0 & \text{falls } n = 0 \\ (m \cdot P(n)) + m & \text{falls } n \neq 0. \end{cases}$$

Auslassung: Zeigen, dass sich durch diese rekursiven Abbildungsvorschriften tatsächlich Funktionen definieren lassen.

Bsp: (1) $2+2=4$:

$$2+2 = S(2+P(2)) = S(2+1) = S(S(2+P(1))) = S(S(2+0)) = S(S(2))$$

$$= S(3) = 4.$$

(2) $2\cdot 2 = 4$: $2\cdot 2 = 2\cdot P(2)+2 = 2\cdot 1+2 = (2\cdot P(1)+2)+2$

$$= (2\cdot 0+2)+2 = (0+2)+2 = S(0+1)+2 = S(S(\underbrace{0+0}_{=0}))+2$$

$$= 2+2 \overset{(1)}{=} 4$$

Def: (1) Ein kommutatives Monoid $M=(M,*,e)$ ist eine nicht-leere Menge M mit einer Verknüpfung $*: M\times M \to M$ und einem Element $e\in M$, so dass gilt:

(i) $*$ ist assoziativ, d.h. $\forall a,b,c\in M: \; a*(b*c) = (a*b)*c$

(ii) e ist ein neutrales Element, d.h. $\forall a\in M: \; a*e = e*a$.

(iii) $*$ ist kommutativ, d.h. $\forall a,b\in M: \; a*b = b*a$.

(2) Ein (kommutativer) Halbring $H=(H,+,0,\cdot,1)$ ist eine Menge H mit Verknüpfungen $+,\cdot$ und Elementen $0,1\in H$, so dass gilt:

(i) $(H,+,0)$ und $(H,\cdot,1)$ sind kommutative Monoide

(ii) $\forall a,b,c\in H: \; (a+b)\cdot c = ac+bc$

(3) Ein (kommutativer) Ring ist ein Halbring R, so dass $(R,+,0)$ eine Gruppe ist. ($\forall a\in R \; \exists a'\in R: \; a+a'=0$)

(4) Ein Körper ist ein kommutativer Ring K, so dass $(K\setminus\{0\},\cdot,1)$ eine Gruppe ist. (insb. $K\neq 0$)

(d.h. $\forall a\in K\setminus\{0\} \; \exists a': \; aa'=1$ und $K\neq\{0\}$)

Satz 1.4 $\mathbb{N}_0$ ist ein Halbring.

Für $a, b, c \in \mathbb{N}_0$ mit $c \neq 0$ gilt $ac = bc \Rightarrow a = b$.

Ohne Beweis, nur exemplarisch, z.B.

$(a+b)+c = a+(b+c)$: a, b fest, Induktion nach c (PS)

$c = 0$: $(a+b)+0 = a+b = a+(b+0)$ ✓

$c \to S(c)$: $(a+b)+S(c) = S((a+b)+c) \underset{IV}{=} S(a+(b+c)) =$

$= a + S(b+c) = a + (b+S(c))$.

$a \cdot (b+c) = a \cdot b + a \cdot c$: Induktion nach c (a, b fest)

$c = 0$: $a \cdot (b+0) = a \cdot b = a \cdot b + 0 = a \cdot b + a \cdot 0$ ✓

$c \to S(c)$: $a \cdot (b+S(c)) = a \cdot S(b+c) = a \cdot (b+c) + a$

$\underset{IV}{=} (a \cdot b + a \cdot c) + a \underset{\uparrow \text{Assoz}}{=} a \cdot b + (a \cdot c + a) = a \cdot b + a \cdot S(c)$.

...

Weiters gibt es auf $\mathbb{N}_0$ eine Totalordnung $\leq$, definiert durch

$$a \leq b \iff \exists n \in \mathbb{N}_0 : a + n = b,$$

Es gilt $a \leq b \Rightarrow a + c \leq b + c$, $a \cdot c \leq b \cdot c$.

1.2 Die ganzen Zahlen

Ansatz. Ganze Zahl x soll in der Form $m-n$ mit $m,n \in \mathbb{N}_0$ dargestellt werden

Für $(m,n), (\bar{m},\bar{n}) \in \mathbb{N}_0^2$ sei

$$(m,n) \sim (\bar{m},\bar{n}) :\Leftrightarrow m+\bar{n} = \bar{m}+n$$

Lemma 1.5: $\sim$ ist eine Äquivalenzrelation auf $\mathbb{N}_0^2$.

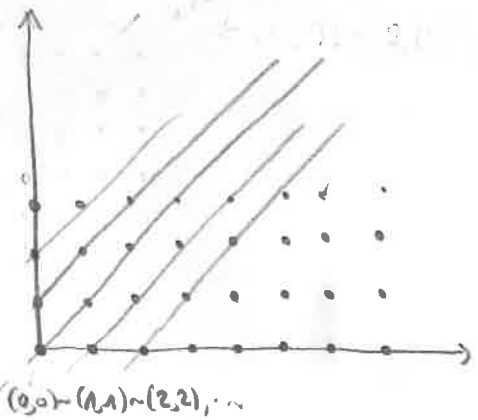
Beweis: $\sim$ ist reflexiv & symmetrisch,

Transitivität: Sei $(m,n)\sim(\bar{m},\bar{n})$, $(\bar{m},\bar{n})\sim(\bar{\bar{m}},\bar{\bar{n}})$. zz $(m,n)\sim(\bar{\bar{m}},\bar{\bar{n}})$.

$$m+\bar{n} = \bar{m}+n \;\wedge\; \bar{m}+\bar{\bar{n}} = \bar{\bar{m}}+\bar{n}$$

$$\Rightarrow m+\bar{\bar{n}}+\bar{n}+\bar{m} = \bar{m}+n+\bar{\bar{m}}+\bar{n} = \bar{\bar{m}}+n+(\bar{m}+\bar{n}) \overset{\text{Kürzen}}{\Longrightarrow} m+\bar{\bar{n}} = \bar{\bar{m}}+n. \qquad \square$$

Bezeichne $[(m,n)]$ die Äquivalenzklasse von (m,n) und $\mathbb{Z} := \mathbb{N}_0 \times \mathbb{N}_0 / \sim$ die Menge aller Äquivalenzklassen



Prop 1.6 Es gibt Abbildungen

$$+ : \begin{cases} \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \\ ([(a,b)],[(c,d)]) \mapsto [(a+c, b+d)] \end{cases}$$

und

$$\cdot : \begin{cases} \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z} \\ ([(a,b)],[(c,d)]) \longmapsto [(ac+bd,\ ad+bc)] \end{cases}$$

Beweis: Müssen zeigen, dass die Abbildungsvorschriften unabhängig von den Repräsentanten sind!

Sei $[(a,b)] = [(\bar{a},\bar{b})]$, $[(c,d)] = [(\bar{c},\bar{d})]$

"+": zz: $[(a+c, b+d)] = [(\bar{a}+\bar{c}, \bar{b}+\bar{d})]$

Es gilt $a+\bar{b} = \bar{a}+b$ und $c+\bar{d} = \bar{c}+d$.

$\Rightarrow a+c+\bar{b}+\bar{d} = (a+\bar{b})+(c+\bar{d}) = (\bar{a}+b)+(\bar{c}+d) = \bar{a}+\bar{c}+b+d$

$\Rightarrow (a+c, b+d) \sim (\bar{a}+\bar{c}, \bar{b}+\bar{d})$

"·": zz: $[(ac+bd, ad+bc)] = [(\bar{a}\bar{c}+\bar{b}\bar{d}, \bar{a}\bar{d}+\bar{b}\bar{c})]$

Es gilt
$a\bar{c}+\bar{b}c = \bar{a}c+bc$ $(\cdot c)$
$\wedge\ \bar{a}d+bd = ad+\bar{b}d$ $(\cdot d)$
$\wedge\ \bar{a}c+\bar{a}\bar{d} = \bar{a}\bar{c}+\bar{a}d$ $(\cdot \bar{a})$
$\wedge\ \bar{b}\bar{c}+\bar{b}d = \bar{b}c+\bar{b}\bar{d}$ $(\cdot \bar{b})$

$\Rightarrow ac+\cancel{\bar{b}c}+\cancel{\bar{a}d}+bd+\cancel{\bar{a}c}+\bar{a}\bar{d}+\bar{b}\bar{c}+\cancel{\bar{b}d}$
$= \cancel{\bar{a}c}+bc+ad+\cancel{\bar{b}d}+\bar{a}\bar{c}+\cancel{\bar{a}d}+\cancel{\bar{b}c}+\bar{b}\bar{d}$ (Kürzbarkeit!)

$\Rightarrow (ac+bd)+(\bar{a}\bar{d}+\bar{b}\bar{c}) = (ad+bc)+(\bar{a}\bar{c}+\bar{b}\bar{d})$

$\Rightarrow (ac+bd, ad+bc) \sim (\bar{a}\bar{d}+\bar{b}\bar{c}, \bar{a}\bar{c}+\bar{b}\bar{d})$. □

Satz 1.7 $\mathbb{Z}$ ist ein kommutativer Ring (mit $0 = [(0,0)]$, $1 = [(1,0)]$).

~~Für $x,y \in \mathbb{Z}$ gilt $xy = 0 \Rightarrow x = 0 \vee y = 0$~~

Beweis (Teil): Die Rechenregeln (Ringaxiome) lassen sich aus jenen für $\mathbb{N}_0$ herleiten.

Wir zeigen nur $\forall [(a,b)] \in \mathbb{Z}: [(a,b)] + [(b,a)] = [(0,0)]$,
insb. ist $(\mathbb{Z}, +)$ eine Gruppe.

$[(a,b)] + [(b,a)] = [(a+b, b+a)] \Rightarrow a+b = b+a \Rightarrow a+b+0 = b+a+0$
$\Leftrightarrow (a+b, a+b) \sim (0,0)$ □

Die Abbildung $c: \mathbb{N}_0 \to \mathbb{Z}$, $n \mapsto [(n,0)]$ ist ein injektiver Homomorphismus von Halbringen. Wir identifizieren $\mathbb{N}_0$ mit $c(\mathbb{N}_0)$ und können damit $\mathbb{N}_0$ als Teilmenge von $\mathbb{Z}$ auffassen.

Def: Für $[(a,b)], [(c,d)] \in \mathbb{Z}$ sei

$$[(a,b)] \leq_{\mathbb{Z}} [(c,d)] \iff a+d \leq_{\mathbb{N}_0} b+c$$

Prop 1.8: $\leq = \leq_{\mathbb{Z}}$ ist wohldefiniert und $(\mathbb{Z}, \leq)$ ist eine total geordnete Menge. Weiters gilt für alle $x,y,z \in \mathbb{Z}$:

(i) $x<y \Rightarrow x+z<y+z$

(ii) $x<y \wedge z>0 \Rightarrow xz<yz$

(iii) $0<x \iff -x<0$.

(ohne Beweis, nur Transitivität ist nicht-trivial.)

Korollar: Für $x,y \in \mathbb{Z}$ gilt $xy=0 \iff x=0 \vee y=0$,
d.h. $\mathbb{Z}$ ist nullteilerfrei (ein Integritätsbereich!)

Beweis: Indirekt. Seien $x,y \neq 0$.

zz: $xy \neq 0$.

O.E $x,y>0$, denn $(\pm x)(\pm y) = 0 \iff xy = 0$

$\overset{(ii)}{\Rightarrow}$ $xy > 0 \cdot y = 0$. □

Lemma 1.9: $\{(m,0) : m \in \mathbb{N}_0\} \cup \{(0,m) : m \in \mathbb{N}\}$ ist ein vollständiges Repräsentantensystem für $\sim$.

(„$+\mathbb{N}_0$“ ↙ „$-\mathbb{N}$“ ↙)

Beweis: $\exists$: Sei $[(a,b)] \in \mathbb{Z}$.

Fall 1: $a \geq b$: $\exists! c \in \mathbb{N}_0$: $a = b+c \Rightarrow (a,b) \sim (c,0)$

Fall 2: $a<b$: $\exists! c \in \mathbb{N}$: $b = a+c \rightsquigarrow (a,b) \sim (0,c)$

Eindeutigkeit: $(0,m) \sim (0,\bar{m}) \iff m+0 = \bar{m}+0 \iff m=\bar{m}$ $(m,\bar{m} \in \mathbb{N})$

$\forall m,\bar{m} \in \mathbb{N}_0$: $(m,0) \sim (\bar{m},0) \iff m = \bar{m}$

Sei $m \in \mathbb{N}_0$, $\bar{m} \in \mathbb{N}$: $(m,0) \sim (0,\bar{m}) \Longrightarrow m+\bar{m} = 0+0 = 0 \Longrightarrow m=\bar{m}=0$ ↯

□

1.3 Die rationalen Zahlen

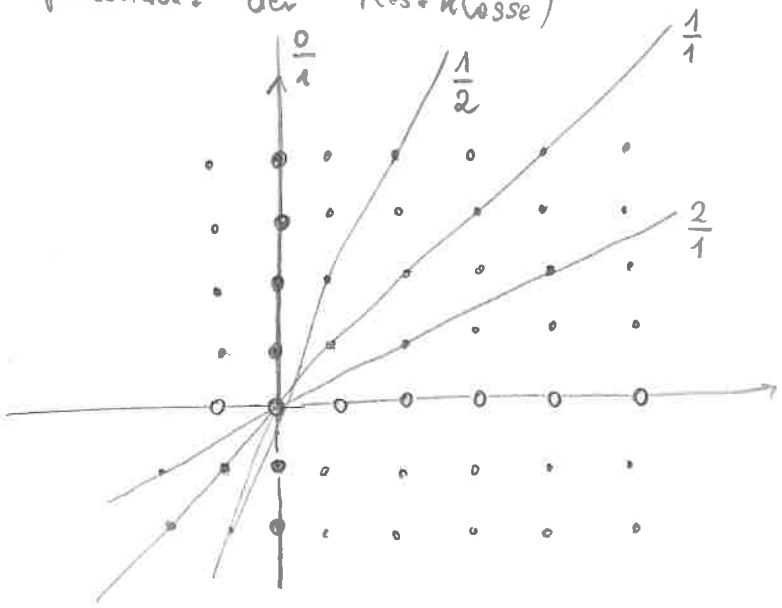
Darstellung als Brüche, aber verschiedene Brüche repräsentieren die gleiche Zahl, z.B. $\frac{2}{3} = \frac{4}{6}$.

Konstruktion Für $(a,m), (c,n) \in \mathbb{Z} \times \mathbb{Z}^*$, $\mathbb{Z}^* := \mathbb{Z} \setminus \{0\}$, sei

$$(a,m) \sim (c,n) :\iff an = cm.$$

$\sim$ ist eine Äquivalenzrelation auf $\mathbb{Z} \times \mathbb{Z}^*$ (Ausnahme!). Wir schreiben $\frac{a}{m}$ für die Äquivalenzklasse von (a,m), und definieren $\mathbb{Q} := \mathbb{Z} \times \mathbb{Z}^* / \sim$ als die Menge aller Äquivalenzklassen.

(D.h. rationale Zahl ≙ Äquivalenzklasse; Bruchdarstellung der Zahl ≙ Repräsentant der Restklasse)



Zahl q ≙ Gerade mit Steigung $\frac{1}{q}$

Bruch ≙ ganzzahlige Punkte auf der Geraden

Durch $\frac{a}{m} + \frac{b}{n} := \frac{an+bm}{mn}$ und $\frac{a}{m} \cdot \frac{b}{n} := \frac{ab}{mn}$ werden Verknüpfungen $\mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ definiert. (Unabhängigkeit von der Wahl der Repräsentanten muss überprüft werden!)

[„+": Sei $\frac{a}{m} = \frac{a'}{m'}$, $\frac{b}{n} = \frac{b'}{n'}$ zz: $\frac{an+bm}{mn} = \frac{a'n'+b'm'}{m'n'}$

$(an+bm)m'n' = anm'n' + bmm'n' = \underline{am'}nn' + \underline{bn'}mm'$

$= a'mnn' + b'nmm' = (a'n' + b'm')mn$ ✓]

Satz 1.10 $\mathbb{Q}$ ist ein Körper (mit $0 := \frac{0}{1}$, $1 := \frac{1}{1}$)

Teilbeweis: Die Körperaxiome rechnet man direkt nach.

Inverse: Sei $\frac{a}{b} \in \mathbb{Q} \setminus \{0\}$. Dann ist $a \neq 0$ (denn $a = 0 \Rightarrow a \cdot 1 = 0 \cdot b \Rightarrow \frac{a}{b} = \frac{a}{1} = 0$ ↯)

$\Rightarrow \frac{b}{a} \in \mathbb{Q} \Rightarrow \frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ab} = \frac{1}{1}$ (denn $ab \cdot 1 = 1 \cdot ab$) □~

Weiters ist $\mathbb{Q}$ ein geordneter Körper, d.h., es gibt eine Totalordnung $\leq$ auf $\mathbb{Q}$, so dass für alle $a, b, c \in \mathbb{Q}$ gilt:

(i) $a < b \Rightarrow a + c < b + c$

(ii) $0 < a \wedge 0 < b \Rightarrow 0 < a \cdot b$

Diese ist wie folgt definiert: Seien $x, y \in \mathbb{Q}$

$\Rightarrow \exists a, b \in \mathbb{Z}, m, n \in \mathbb{N}: x = \frac{a}{m}, y = \frac{b}{n}$

$x \leq_{\mathbb{Q}} y :\Leftrightarrow an \leq_{\mathbb{Z}} bm$

Darstellung: Jedes $x \in \mathbb{Q}$ lässt sich darstellen als $x = \frac{a}{m}$ mit $a \in \mathbb{Z}$, $m \in \mathbb{N}$. Man kann weiters $ggT(a, m) = 1$ wählen; dann ist die Darstellung eindeutig (reduzierte Bruchdarstellung → Elementare Zahlentheorie)

1.4 Die reellen Zahlen

Details: Schichl-Steinbauer, Einf. in die math. Arbeiten, 6.4.1, oder (2. Aufl. 2012)
Bojnok, An Invitation to Abstract Mathematics, Ch. 23, 2013

Def: Sei $(X, \leq)$ partiell geordnet, $M \subseteq X$.
$x \in X$ heißt

(1) untere Schranke für M, falls $\forall m \in M: x \leq m$

(2) obere Schranke für M, falls $\forall m \in M: m \leq x$.

(3) Infimum von M in X, falls x eine untere Schranke für M ist, und für jede weitere untere Schranke x' gilt $x' \leq x$

(4) Supremum von M in X, falls x eine obere Schranke für M ist, und für jede weitere obere Schranke x' gilt: $x' \geq x$.

(Diese sind eindeutig)

Bsp: $M = \{x \in \mathbb{Q} : x^2 < 2\}$ besitzt in $\mathbb{Q}$ kein Supremum / Infimum

untere Schranken: $\{y \in \mathbb{Q}_{<0} : y^2 > 2\} = L$

obere Schranken: $\{y \in \mathbb{Q}_{>0} : y^2 > 2\} = U$

U besitzt kein Minimum: Sei $y \in U$.

$$2 < (y-\varepsilon)^2 = y^2 - 2\varepsilon y + \varepsilon^2$$

Durch geeignete (kleine Wahl) von ε lässt sich $\varepsilon^2 - 2\varepsilon y < y^2 - 2$ erreichen $\Rightarrow y - \varepsilon \in U$.

Ein partiell geordnete Menge

Def: $(X, \leq)$ heißt (ordnungs)vollständig, wenn jede beschränkte, nicht-leere Menge ein Supremum und ein Infimum besitzt

Machen $\mathbb{Q}$ in einen ordnungsvollständigen Körper einbetten.
Wir wissen schon $|\mathbb{R}| > |\mathbb{Q}|$, d.h. $\mathbb{R}$ lässt sich nicht als Quotient von $\mathbb{Q}^2$ konstruieren!

Idee: $\sqrt{2} = 1{,}4142\ldots \notin \mathbb{Q}$,

können uns von unten und oben ohne beliebig nähern:

$1 < 1{,}4 < 1{,}41 < 1{,}414 < \ldots < \sqrt{2} < \ldots < 1{,}42 < 1{,}5$

Stelle $\sqrt{2}$ durch $A = \{x \in \mathbb{Q} : x^2 < \sqrt{2}\}$, $B = \{x \in \mathbb{Q} : x^2 > \sqrt{2}\}$

dar: (A,B) repräsentiert $\sqrt{2}$

Eigenschaften: $A \cup B = \mathbb{Q}$, $\forall a \in A, b \in B: a < b$, $A, B \neq \emptyset$

Stellen wir ohne $q \in \mathbb{Q}$ derart dar, ergeben sich zwei Möglichkeiten:

$(-\infty, q] \cup (q, \infty)$ oder $(-\infty, q) \cup [q, \infty)$

Wählen stets ersteres, d.h. ein Dedekindscher Schnitt von $\mathbb{Q}$ ist ein Paar (A,B), $A, B \subseteq \mathbb{Q}$, so dass gilt:

(i) $\mathbb{Q} = A \cup B$, $A, B \neq \emptyset$

(ii) $\forall a \in A \, \forall b \in B: a < b$

(iii) B besitzt kein Minimum.

Beobachtung: $A = \mathbb{Q} \setminus B$, also ist A redundant.

Def. Eine nicht-leere Menge $B \subseteq \mathbb{Q}$ heißt Oberklasse, falls $\emptyset \neq B \subsetneq \mathbb{Q}$ und

(i) $\forall b \in B \, \forall q \in \mathbb{Q}: q \geq b \Rightarrow q \in B$

(ii) B besitzt kein Minimum, d.h., $\forall b \in B \, \exists b' \in B: b' < b$.

Man definiert nun $\mathbb{R} = \{B \subseteq \mathbb{Q} : B \text{ ist Oberklasse}\}$.

Einbettung von $\mathbb{Q}$: For $q \in \mathbb{Q}$ sei $q_{\mathbb{R}} := \{x \in \mathbb{Q} : q < x\} \in \mathbb{R}$.

Damit ergibt sich eine injektive Abb.

$$i \begin{cases} \mathbb{Q} \longrightarrow \mathbb{R} \\ q \longmapsto q_{\mathbb{R}} \end{cases}$$

Zahlen in $i(\mathbb{Q})$ heißen rational, jene in $\mathbb{R} \setminus i(\mathbb{Q})$ irrational.

Bemerke: $\inf(q_{\mathbb{R}}) = q \in \mathbb{Q}$, $B \subseteq \mathbb{R} \setminus \mathbb{Q}$ besitzt in $\mathbb{Q}$ kein Infimum.

~~Addition: $A+B := \{a+b : a \in A, b \in B\}$, $0_{\mathbb{R}} = \{q \in \mathbb{Q} : q > 0\}$~~

Inverse: Für $A \subseteq \mathbb{R}$ sei $A^{\downarrow} := \{q \in \mathbb{Q} : \forall a \in A : q < a\}$ die Menge der echten unteren Schranken von A, und

$$\hat{A} := \begin{cases} A^{\downarrow} \setminus \{\inf A\} & \text{falls } A \text{ rational;} \\ A^{\downarrow} & \text{falls } A \text{ irrational.} \end{cases}$$

Bsp: $A = \{x \in \mathbb{Q} : x^2 > 2\} \cap \{x > 0\}$
$= (\sqrt{2}, \infty)$ "

$A^{\downarrow} = \{x \in \mathbb{Q} : x^2 < 2\} \cup \mathbb{Q}_{<0}$
$= (-\infty, \sqrt{2})$ "

oder $(2,\infty)^{\downarrow} = (-\infty, 2]$
$\overline{(2,\infty)} = (-\infty, 2)$

Sei $-A := \{-q : q \in \hat{A}\}$

Prop: $-A$ ist eine Oberklasse und $A + (-A) = 0_{\mathbb{R}}$

Beweis: $A \neq \emptyset$: $A \neq \mathbb{Q} \Rightarrow A$ besitzt untere Schranke $\rightarrow A^{\downarrow} \neq \emptyset \Rightarrow \hat{A} \neq \emptyset$
$\Rightarrow -A \neq \emptyset$

($a \in A^{\downarrow} \Rightarrow a - 1 \in A^{\downarrow}$)

$-A \neq \mathbb{Q}$: Sei $a \in A \Rightarrow a \notin A^{\downarrow} \Rightarrow -a \notin -A$.

$-A$ ist nach oben abgeschlossen: Sei $a \in -A$ und $b \in \mathbb{Q}$ mit $a < b$.

zz: $b \in -A$.

$-a \in A^{\downarrow} \wedge -b < -a \Rightarrow -b \in A^{\downarrow}$

Wegen $-b < -a$ ist $-b$ jedenfalls kein Infimum von A

$\Rightarrow -b \in \hat{A} \Rightarrow b \in A$

$-A$ besitzt kein Minimum: Sei $a \in -A \Rightarrow -a \in \hat{A}$,

also $-a \in A^{\downarrow}$ und $-a$ ist kein Infimum von a.

$\Rightarrow \exists b \in A^{\downarrow} : -a < b$ & b ist kein Infimum
[wäre $b = \inf A$, wähle $-a < b' < b$]

$\Rightarrow b \in \hat{A} \Rightarrow -b \in -A$ und $-b < a$.

$A + (-A) = 0_{\mathbb{R}}$

„$\subseteq$" Sei $a \in A$, $b \in -A$

$b \in -A \Rightarrow -b < a \Rightarrow 0 < a+b \Rightarrow A + (-A) \subseteq 0_{\mathbb{R}} = \{q \in \mathbb{Q} : q > 0\}$.

„$\supseteq$" Sei $x \in \mathbb{Q}_{>0}$. Seien $a \in A$, $b \in \mathbb{Q} \setminus A$: $a - b < x$ (!).

$\forall a \in A: a > b \Rightarrow b \in A^{\downarrow}$, wlog $b \in \hat{A}$

$\Rightarrow -b \in -A$

$d := a - b$, $d < x \Rightarrow x - d > 0$.

$\Rightarrow \underbrace{(x-d)+a}_{=a'} \in A$ (A Oberhalbmenge)

$\Rightarrow a' + (-b) = x - a + b + a - b = x$. □

Ordnung: $A \leq B :\Leftrightarrow A \supseteq B$

Multiplikation:

Achtung, die Idee „$A \cdot B = \{ab : a \in A, b \in B\}$" funktioniert i.A. nicht. z.B.,

$A = -2_{\mathbb{R}} = \{q \in \mathbb{Q} : q > -2\}$, $B = -3_{\mathbb{R}} = \{q \in \mathbb{Q} : q \geq -3\}$

Erwartung: $(-2_{\mathbb{R}})(-3_{\mathbb{R}}) = 6_{\mathbb{R}} = \{q \in \mathbb{Q} : q > 6\}$

aber: $(-1) \cdot B \supseteq -1 \cdot \mathbb{Q}_{\geq 0} \supseteq \mathbb{Q}_{<0}$

und $1 \cdot B \supseteq \mathbb{Q}_{\geq 0}$

$\Rightarrow \{a \cdot b : a \in A, b \in B\} = \mathbb{Q}$!

Man definiert für $A, B \in \mathbb{R}$ mit $A, B \geq 0$:

$$A \cdot B := \{ab : a \in A, b \in B\}$$

und

$$A \cdot B := \begin{cases} -((-A)\cdot B) & \text{falls } A<0, B \geq 0 \\ -(A(-B)) & \text{falls } A \geq 0, B<0 \\ (-A)(-B) & \text{falls } A, B<0. \end{cases}$$

(Ähnlich analog zu Addition, aber wieder zuerst für $A \geq 0$!)

Satz 1.11 $\mathbb{R}$ ist ein ordnungsvollständiger, geordneter Körper & enthält $\mathbb{Q}$ als (geordneten) Unterkörper. (nach Identifikation $\mathbb{Q} \cong i(\mathbb{Q})$)

Teilbeweis: Zeigen nur, dass jede nicht-leere, beschränkte Menge $M \subseteq \mathbb{R}$ ein Supremum & Infimum besitzt.

Sei $A = \bigcup_{X \in M} X$

Beh.: $A = \inf \mathcal{P}(M)$

(i) A ist Oberklasse: $M \neq \emptyset \Rightarrow A \neq \emptyset$

Sei $C \in \mathbb{R}$ eine untere Schranke für $M \Rightarrow \forall X \in M: C \leq X$

$\Rightarrow \forall X \in M: C \geq X \Rightarrow C \geq \bigcup_{X \in M} X \Rightarrow C \leq A.$

Sei $a \in A, q \in \mathbb{Q}: a \leq q$

$\Rightarrow \exists X \in M: a \in X \overset{X \text{ ok.}}{\Rightarrow} q \in X \Rightarrow q \in A$

A besitzt kein Minimum: Sei $a \in A \Rightarrow \exists X \in M: a \in X$

$\Rightarrow \exists b \in X: b < a \Rightarrow b \in A$

A ist untere Schranke für M:

$$\forall x \in M: \; X \subseteq A \Rightarrow A \leq X$$

$A = \inf(M)$: Sei $C \in \mathbb{R}$ untere Schranke für M

$$\Rightarrow \forall x \in M: \; C \leq X \Rightarrow X \subseteq C \Rightarrow \bigcup_{X \in C} X \subseteq C \Rightarrow C \leq A.$$

Supremum: Sei $B = -\inf(-M)$ Beh. $B = \sup(M)$.

[Sofern hier voraus, dass $\mathbb{R}$ geordneter Körper ist]

Sei $X \in M \Rightarrow -X \in -M \Rightarrow -X \geq \inf(-M) \Rightarrow X \leq -\inf(-M)$.

Sei $C \in \mathbb{R}$ eine weitere obere Schranke für M.

$$\Rightarrow \forall x \in M: \; X \leq C \Rightarrow -X \geq -C \Rightarrow -C \leq \inf(-M)$$
$$\Rightarrow +C \geq -\inf(-M).$$

□~

Satz 1.12 Ist R' ein weiterer ordnungs-vollständiger Körper, so gibt es einen eindeutig bestimmten Körperisomorphismus $R' \cong \mathbb{R}$, der die Ordnung erhält.

Beweis siehe [Menini & van Oystaeyen, Abstract Algebra, Marcel-Dekker Verl, 2004 — Kapitel 33, insb. Satz 33.52.

Andere Konstruktion für $\mathbb{R}$:

$$\mathcal{C} := \{ (a_n)_{n \geq 0} \in \mathbb{Q}^{\mathbb{N}_0} : \; (a_n)_{n \geq 0} \text{ ist Cauchy-Folge} \}$$

$\mathcal{C}$ ist ein kommutativer Ring mit $(a_n)_{n \geq 0} + (b_n)_{n \geq 0} = (a_n + b_n)_{n \geq 0}$ und

$(a_n)_{n \geq 0} \cdot (b_n)_{n \geq 0} := (a_n b_n)_{n \geq 0}$

Sei $\mathcal{N} \subseteq \mathcal{C}$ die Menge der Nullfolgen. Dann ist $\mathcal{N}$ ein Ideal von $\mathcal{C}$ (d.h. $\mathcal{N} \neq \emptyset$, $\mathcal{N} + \mathcal{N} \subseteq \mathcal{N}$, $\mathcal{C}\mathcal{N} \subseteq \mathcal{N}$)

$(a_n)_{n\geq 0} \sim (b_n)_{n\geq 0} :\Leftrightarrow (a_n - b_n)_{n\geq 0} \in \mathcal{N}$ ist eine Äquivalenzrelation auf $\mathcal{C}$. Die Menge der Äquivalenzklassen $\mathcal{C}/\mathcal{N}$ ist ein Ring, mit induzierten Verknüpfungen (weil $\mathcal{N}$ ein Ideal ist $\rightarrow$ Algebra), und sogar ein Körper,

$\mathbb{Q} \hookrightarrow \mathcal{C}/\mathcal{N}$, $q \mapsto [(q,q,q,\dots)_{n\geq 0}]_{\mathcal{N}}$.

Man kann nun zeigen, dass $\mathcal{C}/\mathcal{N}$ vollständig bzw. ordnungsvollständig ist. Eindeutigkeit $\rightarrow \mathbb{R} \cong \mathcal{C}/\mathcal{N}$.

1.5 Die komplexen Zahlen

Auf $\mathbb{R}^2$ definiert man

$(a,b) + (a',b') := (a+a',\ b+b')$ und

$(a,b)\cdot(a',b') := (aa' - bb',\ ab' + ba')$.

Damit wird $\mathbb{C} := (\mathbb{R}^2, +, \cdot)$ zum Körper mit $1 = (1,0)$, $0 = (0,0)$.

$\mathbb{R} \hookrightarrow \mathbb{C}$, $a \mapsto (a,0)$

Nimmt man als Basis $1 = (1,0)$ und $i = (0,1)$, so ergibt sich die übliche Darstellung $a+bi$, $a,b \in \mathbb{R}$.

Für $z = a+bi \in \mathbb{C}$ sei $\bar{z} := a - bi$ die zu z komplex konjugierte Zahl, $\mathrm{Re}(z) := \frac{z+\bar{z}}{2} = a$ und $\mathrm{Im}(z) := \frac{z-\bar{z}}{2i} = b$.

Sei weiters $|z| := \sqrt{z\bar{z}} = \sqrt{a^2+b^2}$.

Satz 1.13 Für einen Körper K sind äquivalent:

(a) Jedes $f \in K[X] \setminus K$ besitzt eine Nullstelle in K

(b) Für $f \in K[X]$ gibt es $\lambda_1, \dots, \lambda_n \in K$, $\alpha \in K$:

$$f = \alpha(X-\lambda_1)\cdot\ldots\cdot(X-\lambda_n)$$

(c) Ist $L \supseteq K$ ein Oberkörper mit $\dim_K L < \infty$, so ist $L = K$.

Man nennt dann K algebraisch abgeschlossen.

Teilbeweis: (a) $\Rightarrow$ (b) Induktion nach $\deg(f)$.

$\deg(f) = -\infty \Rightarrow f = 0$ ✓

$\deg(f) = 0 \Rightarrow f = a \in K^\times$ ✓

$\deg(f) \geq 1$: Sei $\lambda \in K$ mit $f(\lambda) = 0$.

Polynomdivision $\Rightarrow$ $\exists\, f = (X-\lambda)g + r$ mit $r, g \in K[X]$, $\deg(r) < 0$.

$\Rightarrow 0 = f(\lambda) = \underbrace{(\lambda-\lambda)g(\lambda)}_{=0} + r(\lambda) \to r(\lambda) = 0 \overset{r \in K}{\Longrightarrow} r = 0$

$\Rightarrow f = (X-\lambda)g$, $\deg(g) = \deg(f) - 1$

$\overset{IV}{\Longrightarrow} \exists\, a \in K, \lambda_2, \dots, \lambda_n \in K:\ g = a(X-\lambda_2) \cdots (X-\lambda_n)$

$\to f = a(X-\lambda)(X-\lambda_2)\cdots(X-\lambda_n)$

(b) $\Rightarrow$ (c) Sei $\alpha \in L$. zz: $\alpha \in K$

$M = \{1, \alpha, \alpha^2, \dots\} \subseteq L$

$\dim_K L < \infty \Rightarrow M$ ist K-Vektorraum

$\to \exists\, n \geq 1, a_0, a_1, \dots, a_n \in K:\ a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n = 0$.

D.h. α ist NST von $f(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n \in K[X]$

$\overset{b)}{\Longrightarrow} f = \beta(X-\lambda_1)\cdots(X-\lambda_n)$ mit $\beta, \lambda_1, \dots, \lambda_n \in K$

$0 = f(\alpha) = \beta(\alpha-\lambda_1)\cdots(\alpha-\lambda_n) \Rightarrow \exists\, i:\ \alpha = \lambda_i \Rightarrow \alpha \in K$.

(c) $\Rightarrow$ (b) [Skizze] Sei $f \in K[X] \setminus K$ von minimalem Grad, so dass f keine NST in K besitzt ($\Rightarrow \deg f > 1$)

Ist $f = gh$ mit $g, h \in K[X]$, so folgt $g \in K^\times$ oder $h \in K^\times$

[ansonst hätte g oder h, und damit f eine Nullstelle]

Man zeigt $K[X]/fK[X] = \{g + fK[X] : g \in K[X]\}$ ist ein Körper,

$K \hookrightarrow K[X]/fK[X]$, $\lambda \mapsto \lambda + fK[X]$, und $\dim_K L = \deg(f) > 1$

[siehe beliebiges Algebra-Lehrbuch – Körpertheorie]

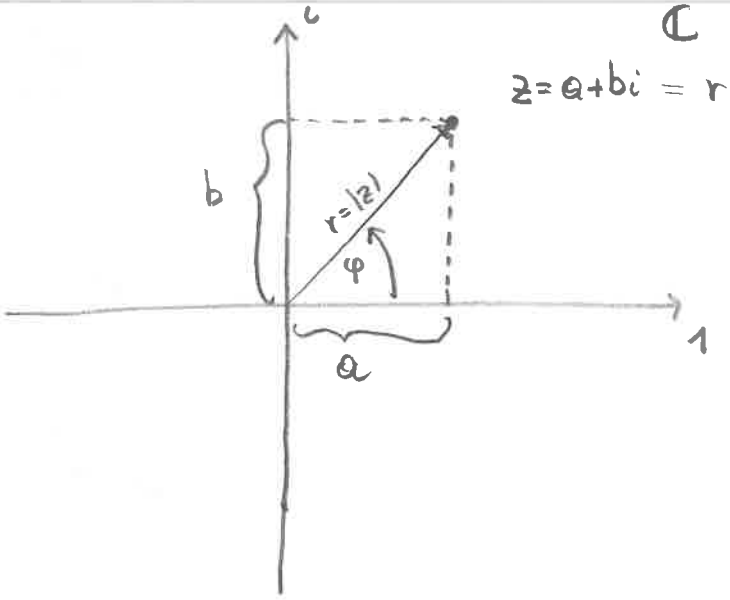
□

Satz 1.14 (Fundamentalsatz der Algebra)

$\mathbb{C}$ ist algebraisch abgeschlossen.

(ohne Beweis → Analysis / Komplexe Analysis Lehrbuch)

Polardarstellung: Jedes $z \in \mathbb{C}$ lässt sich darstellen als $z = re^{i\varphi}$ mit $r \geq 0$, $\varphi \in \mathbb{R}$. Dabei ist $r = |z|$. Ist $z \neq 0$, so ist φ eindeutig bis auf Vielfache von 2π.



$\mathbb{C}$

$z = a + bi = r\cos(\varphi) + i\, r\sin(\varphi)$

$$S^1 := \{ z \in \mathbb{C} : |z| = 1 \} = \{ e^{i\varphi} : \varphi \in \mathbb{R} \} = \{ e^{i\varphi} : \varphi \in [0, 2\pi) \}$$

ist der Einheitskreis.

Drehungen im $\mathbb{R}^2$: Drehungen um den Ursprung sind lineare Abbildungen.

Drehung um den Winkel φ in der Standardbasis des $\mathbb{R}^2$ wird repräsentiert durch die Matrix

$$A_\varphi := \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}$$

$$SO_2(\mathbb{R}) := \{ A \in M_2(\mathbb{R}) : AA^T = \mathbb{1} = A^T A \text{ und } \det(A) = 1 \}$$

$$= \left\{ \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix} : \varphi \in [0, 2\pi) \right\}$$

Prop 1.15 $f: \begin{cases} (S^1, \cdot) \longrightarrow (SO_2, \cdot) \\ z \longmapsto \begin{pmatrix} \mathrm{Re}\, z & -\mathrm{Im}\, z \\ \mathrm{Im}\, z & \mathrm{Re}\, z \end{pmatrix} \end{cases}$ ist Gruppenisomorphismus

---

Beweis Entweder mit Polarkoordinaten, $z = e^{i\varphi}$

$$\Rightarrow f(z) = \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}$$

oder direkt:

-) $f(z_1 z_2) = f(z_1) f(z_2)$:

$$f(z_1) f(z_2) = \begin{pmatrix} \mathrm{Re}\, z_1 & -\mathrm{Im}\, z_1 \\ \mathrm{Im}\, z_1 & \mathrm{Re}\, z_1 \end{pmatrix} \begin{pmatrix} \mathrm{Re}\, z_2 & -\mathrm{Im}\, z_2 \\ \mathrm{Im}\, z_2 & \mathrm{Re}\, z_2 \end{pmatrix}$$

$$= \begin{pmatrix} \mathrm{Re}\, z_1 \mathrm{Re}\, z_2 - \mathrm{Im}\, z_1 \mathrm{Im}\, z_2 & -(\mathrm{Re}\, z_1 \mathrm{Im}\, z_2 + \mathrm{Im}\, z_1 \mathrm{Re}\, z_2) \\ \mathrm{Im}\, z_1 \mathrm{Re}\, z_2 + \mathrm{Re}\, z_1 \mathrm{Im}\, z_2 & -\mathrm{Im}\, z_1 \mathrm{Im}\, z_2 + \mathrm{Re}\, z_1 \mathrm{Re}\, z_2 \end{pmatrix}$$

$$= \begin{pmatrix} \mathrm{Re}(z_1 z_2) & -\mathrm{Im}(z_1 z_2) \\ \mathrm{Im}(z_1 z_2) & \mathrm{Re}(z_1 z_2) \end{pmatrix} = f(z_1 z_2).$$

-) Injektivität: Sei $f(z) = 1 \Rightarrow \mathrm{Re}\, z = 1,\ \mathrm{Im}\, z = 0 \Rightarrow z = 1$.

-) Surjektivität: Sei $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SO_2 \Rightarrow \det(A) = 1 \wedge A^T A = 1$

$$\Rightarrow 1 = ad - bc \wedge \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a^2 + c^2 & ab + cd \\ ab + cd & b^2 + d^2 \end{pmatrix}$$

Sei $z = a + ci \overset{a^2 + c^2 = 1}{\Longrightarrow} z \in S^1$. zz. $f(z) = A$

$0 = ab + cd \Rightarrow \begin{pmatrix} a \\ c \end{pmatrix} \perp \begin{pmatrix} b \\ d \end{pmatrix} \Rightarrow b + di = \lambda(-c + ai)$ mit $\lambda \in \mathbb{R}$

$\Rightarrow b = -\lambda c,\ d = \lambda a \overset{\det(A) = 1}{\Longrightarrow} 1 = \lambda a^2 + \lambda c^2 = \lambda \underbrace{(a^2 + c^2)}_{= 1}$

$\Rightarrow \lambda = 1$ ✓

□

1.6 Die Quaternionen

Abweichend von Kapitel 1.1–1.5 behandeln wir jetzt nicht notwendigerweise kommutative Ringe (d.h. $(R,+)$ ist abelsche Gruppe, $(R,\cdot)$ ist ein – möglicherweise nicht-kommutativer – Monoid, und die Distributivgesetze gelten).

Def: Ein Ring $(R,+,\cdot)$ heißt

- Divisionsring oder Schiefkörper, wenn $(R\setminus\{0\},\cdot,1)$ eine (möglicherweise nicht-abelsche) Gruppe ist.
- (assoziative unitäre) $\mathbb{R}$-Algebra, wenn R zusätzlich ein $\mathbb{R}$-VR ist und es gilt
$$\forall \lambda\in\mathbb{R}\ \forall r,s\in R:\ \lambda(rs)=(\lambda r)s=r(\lambda s)$$

Bsp:
- Körper sind Divisionsringe
- $\mathbb{R}$-Algebren: $\mathbb{R}$, $\mathbb{C}$, $M_n(\mathbb{R})$, $\mathbb{R}[x]$

Sei $\mathbb{H}=\mathbb{C}^2$ mit $(z_1,w_1)+(z_2,w_2):=(z_1+z_2,\ w_1+w_2)$
und $(z_1,w_1)\cdot(z_2,w_2):=(z_1z_2-w_1\overline{w_2},\ z_1w_2+w_1\overline{z_2})$

Darstellung: Sei $1=(1,0)$, $j=(0,1)\in\mathbb{C}^2$, also $(z_1,w_1)=z_1+w_1j$
Ist $z_\ell=a_\ell+b_\ell i$, $w_\ell=c_\ell+d_\ell i$, und identifizieren wir $\mathbb{R}^4=\mathbb{C}^2$,
so ist $1=(1,0)$, $i=(i,0)$, $j=(0,1)$, $k=(0,i)$ eine $\mathbb{R}$-Basis von $\mathbb{H}$.

Es gilt: $(a_1+b_1i+c_1j+d_1k)(a_2+b_2i+c_2j+d_2k)$
$=(a_1+b_1i,\ c_1+d_1i)(a_2+b_2i,\ c_2+d_2i)$
$=\big((a_1+b_1i)(a_2+b_2i)-(c_1+d_1i)(c_2-d_2)i,$
$\quad (a_1+b_1i)(c_2+d_2i)+(c_1+d_1i)(a_2-b_2i)\big)$
$=\big(a_1a_2-b_1b_2-c_1c_2-d_1d_2+(a_1b_2+b_1a_2+c_1d_2-d_1c_2)i,$
$\quad a_1c_2-b_1d_2+c_1a_2+d_1b_2+(a_1d_2+b_1c_2-c_1b_2+d_1a_2)i\big)=$

$$= (a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2) + (a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2)\,i$$
$$+ (a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2)\,j + (a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2)\,k \qquad (*)$$

Satz 1.16 $\mathbb{H}$ ist eine nichtkommutative assoziative $\mathbb{R}$-Algebra.

Beweis: $(\mathbb{H},+)$ ist VR und $\forall \lambda\in\mathbb{R}\ \forall x,y\in\mathbb{H}$: $\lambda(xy) = (\lambda x)y = x(\lambda y)$

$(\mathbb{H},\cdot)$ ist Monoid: $(z,w)\cdot(1,0) = (z,0)$ ✓ $\quad (1,0)(z,w) = (z,0)$ ✓

Assoziativität:

$$(z_1,w_1)\big((z_2,w_2)(z_3,w_3)\big) = (z_1,w_1)\left(z_2z_3 - w_2\overline{w}_3,\ z_2w_3 + w_2\overline{z}_3\right)$$
$$= \big(z_1z_2z_3 - z_1w_2\overline{w}_3 - w_1\overline{z}_2\overline{w}_3 - w_1\overline{w}_2z_3,$$
$$z_1z_2w_3 + z_1w_2\overline{z}_3 + w_1\overline{z}_2\overline{z}_3 - w_1\overline{w}_2w_3\big)$$

$$\big((z_1,w_1)(z_2,w_2)\big)(z_3,w_3) = \left(z_1z_2 - w_1\overline{w}_2,\ z_1w_2 + w_1\overline{z}_2\right)(z_3,w_3)$$
$$= \big(z_1z_2z_3 - w_1\overline{w}_2z_3 - z_1w_2\overline{w}_3 - w_1\overline{z}_2\overline{w}_3,$$
$$z_1z_2w_3 - w_1\overline{w}_2w_3 + z_1w_2\overline{z}_3 + w_1\overline{z}_2\overline{z}_3\big)$$

Distributivität:

$$(z_1,w_1)\big((z_2,w_2) + (z_3,w_3)\big) = (z_1,w_1)(z_2+z_3,\ w_2+w_3)$$
$$= \big(\underline{z_1z_2} + z_1z_3 - \underline{w_1\overline{w}_2} - w_1\overline{w}_3,\ \underline{z_1w_2} + z_1w_3 + \underline{w_1\overline{z}_2} + w_1\overline{z}_3\big)$$
$$= (z_1,w_1)(z_2,w_2) + (z_1,w_1)(z_3,w_3)$$

$$\big((z_1,w_1) + (z_2,w_2)\big)(z_3,w_3) = (z_1+z_2,\ w_1+w_2)(z_3,w_3)$$
$$= \big(\underline{z_1z_3} + z_2z_3 - \underline{w_1w_3} - w_2w_3,\ \underline{z_1w_3} + z_2w_3 + \underline{w_1\overline{z}_3} + w_2\overline{z}_3\big)$$
$$= (z_1,w_1)(z_3,w_3) + (z_2,w_2)(z_3,w_3)$$

□

Die Multiplikation beliebiger Elemente ergibt sich aus der Multiplikation der Basiselemente $1, i, j, k$

~~$\mathbb{C}\subset\mathbb{H}$, aber keine $\mathbb{C}$-Algebra~~

$\cdot$	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

$ij = k = -ji$
$ki = j = -ik$
$jk = i = -kj$
$i^2 = j^2 = k^2 = -1$

Bem: •) Alle Relationen lassen sich aus $\boxed{i^2 = j^2 = k^2 = -1,\ ijk = -1}$ herleiten.

•) $\{\pm 1, \pm i, \pm j, \pm k\}$ bildet eine 8-elementige Gruppe, die Quaternionengruppe Q_8.

•) $\mathbb{C} \hookrightarrow \mathbb{H}$ via $i \mapsto i$, aber auch $i \mapsto j$!
$\mathbb{H}$ ist kein $\mathbb{C}$-Algebra, denn $ij \neq ji$.

Def: Für $x = a + bi + cj + dk = z + wj \in \mathbb{H}$ $(a,b,c,d \in \mathbb{R},\ z,w \in \mathbb{C})$ sei $\bar{x} = a - bi - cj - dk = \bar{z} - wj$ das zu x konjugierte Quaternion.

Lemma 1.17 (1) $\mathbb{H} \to \mathbb{H}, x \mapsto \bar{x}$ ist $\mathbb{R}$-linear, $\overline{xy} = \bar{y}\bar{x}$, und $\bar{\bar{x}} = x$ (die Abbildung ist eine Involution)

(2) Sei $x = a + bi + cj + dk \in \mathbb{H}$. $x \in \mathbb{R} \Leftrightarrow x = \bar{x}$
$x\bar{x} = \bar{x}x = a^2 + b^2 + c^2 + d^2 \in \mathbb{R}_{\geq 0}$,
$x + \bar{x} = \bar{x} + x = 2a \in \mathbb{R}$.

(3) $x\bar{x} = 0 \Leftrightarrow x = 0$.

Beweis: (1) $\mathbb{R}$-Linearität und $\bar{\bar{x}} = x$ sind klar.

Sei $x = z_1 + w_1 j$, $y = z_2 + w_2 j$ mit $z_\ell, w_\ell \in \mathbb{C}$

$\Rightarrow \bar{y}\bar{x} = (\bar{z}_2 - w_2 j)(\bar{z}_1 - w_1 j) = (\bar{z}_1\bar{z}_2 - \bar{w}_1 w_2) + (-w_1\bar{z}_2 - z_1 w_2)\, j$

$\overline{xy} = \overline{(z_1 z_2 - w_1\bar{w}_2) + (z_1 w_2 + w_1 \bar{z}_2)\, j} = (\bar{z}_1\bar{z}_2 - \bar{w}_1 w_2) - (z_1 w_2 + w_1 \bar{z}_2)\, j$

(*) **Lemma 1.18** For $\lambda \in \mathbb{R}$, $x, y \in \mathbb{H}$ gilt

(1) $\mathrm{trd}(x+y) = \mathrm{tr}(x) + \mathrm{tr}(y)$, $\mathrm{tr}(\lambda x) = \lambda\, \mathrm{tr}(x)$

(2) $\mathrm{nr}(xy) = \mathrm{nr}(x)\,\mathrm{nr}(y)$ und $\mathrm{nr}(\lambda x) = \lambda^2 \mathrm{nr}(x)$ sowie $\mathrm{nr}(\bar{x}) = \mathrm{nr}(x)$

Beweis: (1) ✓

(2) $\mathrm{nr}(xy) = \overline{xy}\, xy = \bar{y}\bar{x}xy = \bar{y}\underbrace{\mathrm{nr}(x)}_{\in \mathbb{R}} y = \mathrm{nr}(x)\,\bar{y}y = \mathrm{nr}(x)\,\mathrm{nr}(y)$

$\mathrm{nr}(\lambda x) = \overline{\lambda x} \cdot \lambda x = \lambda^2 \bar{x}x$

$\mathrm{nr}(\bar{x}) = \bar{\bar{x}}\,\bar{x} = x\bar{x} = \bar{x}x = \mathrm{nr}(x)$ □

Bem nr/tr hängen nicht von Basis 1, i, j, k ab.

(2) $x \in \mathbb{R} \Leftrightarrow x = \bar{x}$ ✓

$\overline{x\bar{x}} \overset{(1)}{=} \bar{\bar{x}}\,\bar{x} = x\bar{x} \Rightarrow x\bar{x} \in \mathbb{R}$, analog $\bar{x}x \in \mathbb{R}$.

$\Rightarrow x\bar{x} = a^2 + b^2 i^2 - c^2 j^2 - d^2 j^2$ (*) (Conclave Terme verschwinden)

$= a^2 + b^2 + c^2 + d^2$

und analog für $\bar{x}x$.

Rest klar.

(3) $x\bar{x} = 0 \Leftrightarrow a^2 + b^2 + c^2 + d^2 = 0 \Leftrightarrow a^2 = b = c^2 = d^2 = 0 \Leftrightarrow a = b = c = d = 0$.

($a^2, \dots, d^2 \geq 0$) □

Def: $nr: \mathbb{H} \to \mathbb{R}_{\geq 0}$, $x \mapsto x\bar{x} = \bar{x}x$ heißt (reduzierte) Norm von $\mathbb{H}$, und $tr: \mathbb{H} \to \mathbb{R}$, $x \mapsto x + \bar{x} = \bar{x} + x$ heißt (reduzierte) Spur von $\mathbb{H}$ ($\|\cdot\|: x \mapsto \sqrt{nr(x)}$ ist die euklidische Norm auf $\mathbb{R}^4$)

(*)

Satz 1.19 $\mathbb{H}$ ist ein Divisionsring (bzw. $\mathbb{R}$-Divisionsalgebra)

Beweis: Sei $x \in \mathbb{H} \setminus \{0\}$. Zz: $\exists x' \in \mathbb{H}: xx' = 1 = x'x$.

$x \neq 0 \Rightarrow nr(x) \in \mathbb{R}_{>0}$. Setze $x' := (nr(x))^{-1} \bar{x}$

$\Rightarrow x'x = \frac{1}{nr(x)} \bar{x}x = \frac{nr(x)}{nr(x)} = 1$ und $xx' = x\frac{1}{nr(x)}\bar{x} \overset{\mathbb{R}\text{-Algebra}}{=} \frac{1}{nr(x)} x\bar{x} = \frac{nr(x)}{nr(x)} = 1$. □

Sei A eine $\mathbb{R}$-Algebra, und seien $x_1, \dots, x_n \in A$. Dann wird A erzeugt durch $x_1, \dots, x_n$ bzw. $x_1, \dots, x_n$ ist ein Erzeugendensystem für A, wenn sich jedes $a \in A$ als $\mathbb{R}$-Linearkombination von Produkten der Form $x_{i_1} \cdots x_{i_k}$, $i_1, \dots, i_k \in \{1, \dots, n\}$, $k \geq 0$, schreiben lässt ($k = 0$ entspricht dem leeren Produkt mit Wert 1)

Satz 1.20 Sei A eine $\mathbb{R}$-Algebra, welche durch $i_0, j_0 \in A \setminus \{0\}$ erzeugt wird und so dass gilt

$$i_0^2 = -1, \quad j_0^2 = -1, \quad i_0 j_0 = -j_0 i_0.$$

Dann gibt es einen $\mathbb{R}$-Algebrenisomorphismus $\mathbb{H} \cong A$.

Beweis: Sei $k_0 := i_0 j_0$. Aus den gegebenen Relationen lässt sich herleiten:

$$i_0 j_0 = -j_0 i_0 = k$$
$$k_0 i_0 = j_0 = -i_0 k_0$$
$$j_0 k_0 = i_0 = -k_0 j_0$$
$$i_0^2 = j_0^2 = k_0^2 = -1$$

(z.B. $k_0 i_0 = i_0 j_0 i_0 = -i_0^2 j_0 = -(-1) j_0 = j_0$)

Damit folgt, dass die $\mathbb{R}$-lineare Abbildung

$\varphi : \mathbb{H} \to A$, $1 \mapsto 1$, $i \mapsto i_0$, $j \mapsto j_0$, $k \mapsto k_0$ ein $\mathbb{R}$-Algebrenhomomorphismus ist (d.h. $\varphi(1) = 1$, $\varphi(xy) = \varphi(x)\varphi(y)$ für x, y).

Zeigen: $1, i_0, j_0, k_0$ ist $\mathbb{R}$-Basis von A. Dann ist φ bijektiv.

zz: $1, i_0, j_0, k_0$ sind linear unabhängig (ESV)

Sei $x = a + b i_0 + c j_0 + d k_0 = 0$ mit $a, b, c, d \in \mathbb{R}$. **zz:** $a = b = c = d$.

$$0 = i_0(a i_0 + i_0 x) = i_0(2a i_0 - 2b) = -2a - 2b i_0 = -2(a + b i_0)$$
$$\overset{2 \neq 0}{\Longrightarrow} \quad \underline{a + b i_0 = 0}$$

$$0 = j_0(a j_0 + j_0 x) = j_0(2a j_0 - 2c) = -2a - 2c j_0 = -2(a + c j_0)$$
$$\Longrightarrow \quad \underline{a + c j_0 = 0}$$

$$0 = k_0(a k_0 + k_0 x) = k_0(2a k_0 - 2d) = -2a - 2d k_0 = -2(a + d k_0)$$
$$\Longrightarrow \quad \underline{a + d k_0 = 0}$$

$$\Longrightarrow 0 \overset{(*)}{=} x - (a + b i_0) - (a + c j_0) - (a + d k_0) = -2a \Longrightarrow 1 \cdot a = 0.$$
$$\overset{1 \neq 0}{\Longrightarrow} \underline{a = 0}. \quad \overset{(*)}{\Longrightarrow} \quad b i_0 = c j_0 = d k_0 = 0.$$

$2 \neq 0 \Rightarrow 2x = 0 \Rightarrow 1 \cdot x = 0 \Rightarrow x = 0$

$i_0 \neq 0 \Rightarrow b = 0$, $j_0 \neq 0 \Rightarrow c = 0$, $k_0 \neq 0 \Rightarrow d = 0$ □

Sei $\mathbb{H}^\circ := \{ bi + cj + dk \in \mathbb{H} : b, c, d \in \mathbb{R} \}$

$= \{ x \in \mathbb{H} : \mathrm{tr}(x) = 0 \} = \{ x \in \mathbb{H} : \bar{x} = -x \} = \mathbb{R}^3$

der $\mathbb{R}$-VR der reinen Quaternionen, und

$\mathbb{H}^1 := \{ a + bi + cj + dk \in \mathbb{H} : a^2 + b^2 + c^2 + d^2 = 1 \}$

$= \{ x \in \mathbb{H} : \mathrm{nr}(x) = 1 \}$

die multiplikative Gruppe der Norm-Eins-Quaternionen

(Da $x \in \mathbb{H}^1$ ist $x^{-1} = \bar{x}$)

$\mathbb{H}^1$ ist ein 3-Sphäre im $\mathbb{R}^4$. (S^3)

Lemma 1.21 Für $x, y \in \mathbb{H}^\circ$ gilt

(1) $xy = -\langle x, y \rangle + x \times y$

(2) $xy \in \mathbb{H}^\circ \Leftrightarrow x \perp y \Leftrightarrow xy = -yx$

(3) $x^2 = -\mathrm{nr}(x) = -\|x\|^2 \in \mathbb{R}_{\leq 0}$.

Beweis: ☺ (Aufgabe 17)

Sei $x = a + bi + cj + dk \in \mathbb{H}^1 \Rightarrow |a|, |b|, |c|, |d| \leq 1$.

$\Rightarrow \exists \alpha \in [0, \pi] : a = \cos(\alpha)$, und $\alpha \in (0, \pi)$ falls $\alpha \neq \pm 1$

$\Rightarrow \boxed{x = \cos(\alpha) + \sin(\alpha)\, I(x)}$ mit

$$I(x) := \begin{cases} 0 & \text{falls } x \in \{\pm 1\} \\ \dfrac{bi + cj + dk}{\sin(\alpha)} & \text{falls } x \notin \{\pm 1\} \end{cases}$$

$1 = \mathrm{nr}(x) = \cos^2(\alpha) + \sin^2(\alpha) \underbrace{\left(\dfrac{b^2 + c^2 + d^2}{\sin^2(\alpha)} \right)}_{=1}$ $\overset{\cos^2(\alpha) + \sin^2(\alpha) = 1}{\Rightarrow}$ $\mathrm{nr}(I(x)) = 1$

und wegen $I(\alpha) \in \mathbb{H}^\circ$, $\boxed{I(\alpha)^2 = -1}$

Satz 1.22 Sei $x = \cos(\alpha) + \sin(\alpha)\, I(x) \in \mathbb{H}^1$. Die $\mathbb{R}$-lineare Abb. $D_x : \begin{cases} \mathbb{H}^\circ \longrightarrow \mathbb{H}^\circ \\ v \longmapsto xvx^{-1} = xv\bar{x} \end{cases}$

stellt eine Drehung um den Winkel 2α um die Drehachse $I(x)$ dar.

Beweis: Sei $i' := I(x)$ und $j' \in \mathbb{H}^\circ$ ein Einheitsvektor mit $i' \perp j'$.

$\overset{L1.21}{\Longrightarrow}$ $(i')^2 = (j')^2 = -1$ und $i'j' = -j'i' \in \mathbb{H}^\circ$

Nach Satz 1.20 ist $i', j', i'j' =: k'$ eine Basis von $\mathbb{H}^\circ$, wir bestimmen die Matrix von D_x bzgl. dieser Basis.

Wegen $\overline{i'} = -i'$ gilt $x^{-1} = \bar{x} = \cos(\alpha) - \sin(\alpha) i'$

$$D_x(i') = x i' x^{-1} = (\cos(\alpha) + \sin(\alpha) i')(\cos(\alpha) - \sin(\alpha) i')\, i'$$
$$= (\cos(\alpha)^2 + \sin(\alpha)^2) i' - \sin(\alpha)\cos(\alpha) + \sin(\alpha)\cos(\alpha) = i'.$$

$$D_x(j') = x j' x^{-1} = (\cos(\alpha) + \sin(\alpha) i')(\cos(\alpha) + \sin(\alpha) i')\, j'$$
$$= (\cos(\alpha)^2 - \sin(\alpha)^2) j' + (\cos(\alpha)\sin(\alpha) + \sin(\alpha)\cos(\alpha))\, \underbrace{i'j'}_{=k'}$$
$$= \cos(2\alpha) j' + \sin(2\alpha) k'$$

$$D_x(k') = x k' x^{-1} = x i' j' x^{-1} = x i' x^{-1} x j' x^{-1} = i'(x j' x^{-1})$$
$$= \cos(2\alpha) k' - \sin(2\alpha) j'.$$

D.h. die Matrix von D_x bzgl. i', j', k' ist

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(2\alpha) & -\sin(2\alpha) \\ 0 & \sin(2\alpha) & \cos(2\alpha) \end{pmatrix}.$$

□

Beobachtung: $D_x = D_{-x}$!

Für $x,y \in \mathbb{H}^1$ ist $D_x = D_y \Leftrightarrow x = \pm y$.

Die Abbildung $\varphi: \mathbb{H}^1 \longrightarrow SO_3(\mathbb{R})$, $x \longmapsto D_x$ ist ein (schiefer, ...) Gruppenepimorphismus mit $\ker \varphi = \{\pm 1\}$. Man sagt $\mathbb{H}^1$ ist eine doppelte Überdeckung der $SO_3(\mathbb{R})$. (Durch eine Einbettung $\mathbb{H} \hookrightarrow M_2(\mathbb{C})$ sieht man $\mathbb{H}^1 \cong SU_2(\mathbb{C})$.)

Anwendungen z.B. in Computergrafik (Simulatoren, Animationen), Kinematik (Interpolation von Drehungen).

Vorteile gegenüber Matrizen:
- Kompakt (4 Zahlen vs. 9)
- numerisch stabiler
- SLERP (Interpolation)

1.7 Satz von Frobenius

Bem: (1) Jedes Polynom $P \in \mathbb{R}[X]$ zerfällt über $\mathbb{R}$ in ein Produkt von Linearfaktoren (reelle Nullstellen) und quadratischen Faktoren (Paare konjugiert komplexer Nullstellen). ($\Leftarrow$ Fundamentalsatz der Algebra)

(2) Jedes reelle Polynom ungeraden Grades besitzt zumindest eine reelle Nullstelle ($\Leftarrow$ Zwischenwertsatz)

(3) Ist V ein $\mathbb{R}$-VR ungerader Dimension und $\varphi: V \to V$ ein Endomorphismus, so besitzt φ zumindest einen reellen Eigenwert.

Satz 1.23 (Frobenius, 1878 [43]) Jede endlich-dimensionale $\mathbb{R}$-Divisionsalgebra ist isomorph zu $\mathbb{R}$, $\mathbb{C}$ oder $\mathbb{H}$.

Beweis (Brešar & Shulmann 2019) Sei D eine endlich-dim. $\mathbb{R}$-Divisonsalgebra. Für $a,b \in D$ sei $a \circ b := ab + ba$ ($a \circ b = 0 \Leftrightarrow ab = -ba$)

(A) $\forall a \in D \; \exists \alpha, \beta \in \mathbb{R}: \; a^2 = \alpha a + \beta$.
Ist $\alpha = 0$ und $a \notin \mathbb{R}$, so ist $\beta < 0$ und $\left(\frac{a}{\sqrt{-\beta}}\right)^2 = -1$

Bew. von A: $\{1, a, a^2, \dots\}$ ist l.abh. $/\mathbb{R}$.
$\Rightarrow \exists P \in \mathbb{R}[X] \setminus \mathbb{R} : P(a) = 0$,
$P = \lambda(X - \gamma_1) \cdots (X - \gamma_n)(X^2 - \alpha_1 X - \beta_1) \cdots (X^2 - \alpha_e X - \beta_e)$
$\Rightarrow 0 = \lambda(a - \gamma_1) \cdots (a - \gamma_n)(a^2 - \alpha_1 a - \beta_1) \cdots (a^2 - \alpha_e a - \beta_e) \in D$
Weil D ein Divisionsring ist, muss einer der Faktoren 0 sein.
Sei $\alpha = 0$. Ist $\beta \geq 0$, so ist $0 = a^2 - \beta = (a - \sqrt{\beta})(a + \sqrt{\beta})$, also $a \in \{\pm\sqrt{\beta}\} \subseteq \mathbb{R}$. D.h. $a \notin \mathbb{R} \Rightarrow \beta < 0$.

(B) Sei $a \in D$ mit $a^2 = -1$. Dann gibt es für alle $b \in D \setminus \langle 1, a \rangle$ ein $c \in \langle 1, a, b \rangle \setminus \langle 1, a \rangle$ so dass gilt $a \circ c = 0$ und $c^2 = -1$.

Nach (a) ist $(a+b)^2, a^2, b^2 \in \langle 1, a, b \rangle =: V$ und deshalb
$a \circ b = (a+b)^2 - a^2 - b^2 \in V$.
$\Rightarrow$ Die Lin. Abb. $x \mapsto a \circ x$ bildet V auf V ab.
Wegen $\dim V = 3$ gibt es ein $\lambda \in \mathbb{R}$ und ein $v \in V \setminus \{0\}$ mit
$a \circ v = \lambda v$.
Also: $av + va = \lambda v \Rightarrow va = (\lambda - a)v \Rightarrow \underline{\lambda - a = vav^{-1}}$
$\Rightarrow (\lambda - a)^2 = v \underbrace{a^2}_{=-1} v^{-1} = -1$.
Andererseits: $(\lambda - a)^2 = \lambda^2 - 2\lambda a + a^2 = \lambda^2 - 2\lambda a - 1$ $\Big\}\ominus$
$\Rightarrow 0 = \lambda^2 - 2\lambda a = \lambda(\lambda - 2a) \underset{a \notin \mathbb{R}}{\Longrightarrow} \lambda = 0$.
$\Rightarrow \boxed{a \circ v = 0}$
D.h. $av \neq va$ aber $av^2 = v^2 a$. (*)
Sei $v^2 = \alpha v + \beta$ (nach (A)). Wegen (*) ist $\alpha = 0$, also

$v^2 \in \mathbb{R} \Rightarrow c := \frac{v}{\sqrt{-b}}$ erfüllt $c^2 = -1$ und $a \circ c = 0$.

$[\Rightarrow c \notin \langle 1, a \rangle.]$

(C) $D \cong \mathbb{R}, \mathbb{C}$ oder $\mathbb{H}$

Ist $\dim_{\mathbb{R}} D = 1$, so ist $D \cong \mathbb{R}$. Sei o.E. $\dim_{\mathbb{R}} D > 1$ und $a \in D \setminus \mathbb{R}$.

(A) $\Rightarrow \exists \alpha: \; a^2 - \alpha a \in \mathbb{R}$

$\Rightarrow \underbrace{a^2 - \alpha a}_{\in \mathbb{R}} + \underbrace{\frac{\alpha^2}{4}}_{\in \mathbb{R}} = (a - \frac{\alpha}{2})^2 \in \mathbb{R}$

$\overset{(A)}{\Rightarrow} \exists i \in D: \; i^2 = -1$ (und $i \notin \mathbb{R}$)

Ist $\dim_{\mathbb{R}} D = 2$ so folgt damit $D \cong \mathbb{C}$. Sei also $\dim_{\mathbb{R}} D > 2$.

$\overset{(B)}{\Rightarrow} \exists j \in D \setminus \langle 1, i \rangle: \; ij = -ji$ und $j^2 = -1$.

Sei $k := ij$.

$\Rightarrow \langle 1, i, j, k \rangle$ ist ein $\mathbb{R}$-Unterschiefkörper von D und isomorph zu $\mathbb{H}$ (Satz 1.20)

zz. $\langle 1, i, j, k \rangle = D$

Angenommen $\langle 1, i, j, k \rangle \subsetneq D$.

(B) $\Rightarrow \exists c \in D \setminus \langle 1, i, j, k \rangle: \; ic = 0$.

$\Rightarrow (jc)i = i(jc)$, d.h. i und jc kommutieren

Ist $b \notin \langle 1, i \rangle$, so gibt es nach (B) ein Element $b' \in \langle 1, i, b \rangle$ mit $b'i \neq ib'$. Dann ist auch $bi \neq ib$.

Es folgt also $jc \in \langle 1, i \rangle$, also $jc = \gamma i + \delta$ mit $\gamma, \delta \in \mathbb{R}$

$\overset{(-j)}{\Rightarrow} c = \gamma k - \delta j \in \langle k, j \rangle$ $\lightning$ $c \notin \langle 1, i, j, k \rangle$.

□

2. g-adische Ziffernderstellung reeller Zahlen

(Stellenwertsysteme) → [Bundschuh, – Einführung in. Zahlen Theorie]
[Remmert, Ullrich – Elemendare Zahlen Theorie]

Sei $g \in \mathbb{N}_{\geq 2}$ und $S_g = \{0, 1, \dots, g-1\}$.

2.1 Entwicklung natürlicher Zahlen

$$8203 = \underline{8} \cdot 10^3 + \underline{2} \cdot 10^2 + \underline{0} \cdot 10^1 + \underline{3} \cdot 10^0$$

Dezimalziffern $\in \{0, 1, \dots, 9\} = S_{10}$

$$8203 = 8192 + 11 = 2^{13} + 8 + 2 + 1 = \underline{1} \cdot 2^{13} + \underline{0} \cdot 2^{12} + \dots + \underline{0} \cdot 2^4 + \underline{1} \cdot 2^3 + \underline{0} \cdot 2^2 + \underline{1} \cdot 2^1 + 0$$

Binärdarstellung, Ziffern $\in \{0, 1\} = S_2$

Satz & Def 2.1 Jedes $n \in \mathbb{N}$ hat eine eindeutige Darstellung der Form

$$n = \sum_{i=0}^{k} a_i g^i$$

mit $a_0, \dots, a_k \in S_g$ und $a_k \neq 0$.

Diese Darstellung heißt g-adische Darstellung von n, die a_i heißen Ziffern der Darstellung, $1+k = 1 + \left\lfloor \frac{\log n}{\log g} \right\rfloor = 1 + \lfloor \log_g n \rfloor$ Stellenzahl und g Basis.

Beweis: **Existenz:** Sei $r_0 := n$ und seien $r_0, \dots, r_j, a_0, \dots, a_{j-1}$, so dass gilt:

(*) $r_i = r_{i+1} g + a_i$ und $0 \leq a_i < g \leq r_i$ für $0 \leq i \leq j-1$.

Dann ist $\frac{r_i}{g} \geqslant r_{i+1} > 0$ für $0 \leq i \leq j-1$, also

$$\frac{r_0}{g^j} \geqslant \frac{r_1}{g^{j-1}} \geqslant \dots \geqslant r_j > 0.$$

Wir konstruieren (r_{j+1}, a_j) wie folgt:

(i) Ist $r_j \geq g$, so sei $r_j = r_{j+1} g + a_j$ mit $0 \leq a_j < g$ (Div. mit Rest).

(ii) Ist $r_j < g$, so sei $a_j = r_j$ und wir hören auf.

Wegen $\frac{r_0}{g^j} \geq r_j$ und $r_j \in \mathbb{N}_0$ folgt $r_j = 0$, spätestens wenn

$$\frac{r_0}{g^j} < 1 \iff r_0 = n < g^j \iff \frac{\log n}{\log g} < j \quad \text{gilt.}$$

Sei $k \geq 0$ minimal mit $r_k < 0$. Dann gilt (*) für $j \in \{0, \dots, k-1\}$ und $0 \leq a_k < g$. Es folgt (induktiv) für $j \in \{0, \dots, k\}$:

$$r_0 = r_j g^j + \sum_{i=0}^{j-1} a_i g^i,$$

insb. $$r_0 = \sum_{i=0}^{k} a_i g^i \qquad (r_k = a_k).$$

Eindeutigkeit: $$n = \sum_{i=0}^{k} a_i g^i \geq a_k g^k \geq g^k \quad \text{und}$$

$$n \leq \sum_{i=0}^{k} (g-1) g^i = (g-1) \sum_{i=0}^{k} g^i = (g-1) \frac{g^{k+1} - 1}{g-1}$$

$$\Rightarrow \quad g^k \leq n < g^{k+1}$$

Also ist $k = \left\lfloor \frac{\log n}{\log g} \right\rfloor$ durch n eindeutig bestimmt.

Sei weiters $n = \sum_{i=0}^{k} a_i' g^i$, $a_i' \in S_g$, $a_k' \neq 0$.

$$\Rightarrow \sum_{i=0}^{k} (a_i - a_i') g^i = 0 \Rightarrow g \mid a_0 - a_0' \overset{|a_0 - a_0'| < g}{\Longrightarrow} a_0 = a_0'$$

$$\Rightarrow \sum_{i=0}^{k-1} (a_{i+1} - a_{i+1}') g^i = 0 \overset{\text{Induktion nach } k}{\Longrightarrow} a_i = a_i' \text{ für } i \in \{1, \dots, k\}.$$

□

Bem: $g=10$: Dezimaldarstellung
$g=2$: Binärdarstellung
$g=16$: Hexadezimaldarstellung (Ziffern: 0...9 A...F)

2.2 Entwicklung reeller Zahlen

Bsp: $\frac{1}{5} = 0{,}2 = 2 \cdot 10^{-1}$

$\frac{1}{8} = 0{,}125 = 1 \cdot 10^{-1} + 2 \cdot 10^{-2} + 5 \cdot 10^{-3}$

$\frac{1}{3} = 0{,}\dot{3} = \sum_{i=1}^{\infty} 3 \cdot 10^{-i}$.

Wir möchten zur Darstellung von $x \in [0,1)$ Reihen der Form $\sum_{i=1}^{\infty} a_i g^{-i}$ mit $a_i \in S_g$ verwenden.

Vorbemerkungen:

(1) $0 \leq \sum_{i=1}^{\infty} a_i g^{-i} \leq \sum_{i=1}^{\infty} (g-1) g^{-i} = (g-1) \sum_{i=1}^{\infty} g^{-i} = (g-1) \frac{1}{(g^{-1})^{-1} - 1} = 1$,

also sind diese Reihen nach dem Majorantenkriterium absolut konvergent.

(2) $\sum_{i=1}^{\infty} (g-1) g^{-i} = \cancel{(g-1)} \frac{1}{\cancel{g-1}} = 1$, d.h. $1 = 0{,}\dot{g}$!

Wir müssen derartige Fälle ausschließen um eine eindeutige Darstellung zu erhalten.

(3) Für $\alpha \in \mathbb{R}$ sei $\lfloor \alpha \rfloor = \min \{ k \in \mathbb{Z} : k \leq \alpha \}$ und $\{\alpha\} := \alpha - \lfloor \alpha \rfloor \in [0,1)$ der gebrochene Teil
(nicht mit einelementiger Menge verwechseln!)

Satz 2.2 Jedes $\alpha \in [0,1)$ hat genau eine Entwicklung der Form

$$\alpha = \sum_{i=1}^{\infty} c_i g^{-i}$$

mit $c_1, c_2, \ldots \in S_g$, von denen unendlich viele ungleich $g-1$ sind. Die Koeffizienten c_i ergeben sich rekursiv aus

$$\alpha_1 := \alpha, \quad c_i := \lfloor \alpha_i g \rfloor, \quad \alpha_{i+1} := \{\alpha_i g\} \quad \text{für } i \geq 1.$$

Beweis: Existenz:

Beh: $\forall j \geq 1 \; \forall k \geq 0: \quad \alpha_j = \sum_{i=j}^{j+k-1} c_i g^{j-1-i} + \alpha_{j+k} g^{-k} \quad (1)$

[Induktion nach k: $k=0$: $\alpha_j = \alpha_j g^{-0}$ ✓

$k \geq 1$, $k-1 \to k$

$$\alpha_j \overset{IV}{=} \sum_{i=j}^{j+k-2} c_i g^{j-1-i} + \underbrace{\alpha_{j+(k-1)} g^{-k+1}}_{= (\alpha_{j+(k-1)} g) g^{-k}} = \sum_{i=j}^{j+k-2} c_i g^{j-1-i} + (c_{j+(k-1)} + \alpha_{j+k}) g^{-k}$$

$$= \sum_{i=j}^{j+k-1} c_i g^{j-1-i} + \alpha_{j+k} g^{-k} \qquad \square \;]$$

Wegen $0 \leq \alpha_i < 1$ ist $0 \leq \alpha_i g < g \Rightarrow c_i = \lfloor \alpha_i g \rfloor \in S_g$.

Angenommen alle bis auf endlich viele c_i sind gleich $g-1 \Rightarrow \exists j \geq 1: \forall i \geq j: c_i = g-1$.

Dann ist für $k \geq 0$

$$\alpha_j \overset{(1)}{=} \sum_{i=j}^{j+k-1} (g-1) g^{j-1-i} + \underbrace{\alpha_{j+k} g^{-k}}_{\to 0} \longrightarrow (g-1) \sum_{e \geq 1} g^{-e} = 1. \quad \text{für } k \to \infty$$

↯ zu $\alpha_j < 1$. Also: $c_j \neq g-1$ für unendlich viele j.

Nun gilt für $k \geq 0$

$$\alpha = \alpha_1 \overset{(1)}{=} \sum_{i=1}^{k} c_i g^{-i} + \alpha_{k+1} g^{-k} \longrightarrow \sum_{i=1}^{\infty} c_i g^{-i} \quad \text{für } k \to \infty,$$

Eindeutigkeit: Sei weiters $\alpha = \sum_{i=1}^{\infty} c_i' g^{-i}$ mit $c_i' \in S_g$, aber unendlich oft $c_i' \neq g-1$.

Zz: $\forall i \geq 1: c_i = c_i'$.

Durch Widerspruch. Sei $j \geq 1$ minimal mit $c_j \neq c_j'$.

$$\Rightarrow c_j g^{-j} + \sum_{i>j} c_i g^{-i} = c_j' g^{-j} + \sum_{i>j} c_i' g^{-i}$$

$$\Rightarrow 1 \leq |c_j - c_j'| = \left| \sum_{i>j} (c_i' - c_i) g^{j-i} \right| \leq \sum_{i>j} |c_i' - c_i| g^{j-i}$$

$$\leq \sum_{i>j} (g-1) g^{j-i} = (g-1) \sum_{e \geq 1} g^{-e} = 1.$$

$\Rightarrow \forall i>j: |c_i' - c_i| = g-1$ und entweder

$\forall i>j: c_i' - c_i = g-1$ oder $\forall i>j: c_i - c_i'$

Also: $\forall i>j: c_i' = g-1, c_i = 0$ oder $\forall i>j: c_i' = 0, c_i = g-1$. ↯. □

Korollar 2.3 (1) Jedes $\alpha \in \mathbb{R}$ besitzt genau eine Darstellung der Form $\alpha = \lfloor \alpha \rfloor + \sum_{i=1}^{\infty} c_i g^{-i}$ mit $c_1, c_2, \ldots \in S_g$ von denen unendlich viele $\neq g-1$ sind. Die c_i ergeben sich aus

$$\alpha_1 := \{\alpha\}, \quad c_i = \lfloor \alpha_i g \rfloor, \quad \alpha_{i+1} = \{\alpha_i g\} \text{ für } i \geq 1.$$

(2) Ist $\alpha \in \mathbb{R}_{>0}$, so besitzt α eine eindeutige Darstellung

$$\alpha = \sum_{i=-k}^{\infty} c_i g^{-i} \quad \text{mit } k \in \mathbb{N}_0, \ c_{-k}, c_{-k+1}, \ldots, c_0, c_1, \ldots \in S_g$$

und unendlich vielen c_i ungleich $g-1$.

Beweis: (1) mit Satz 2.2; für (2) wendet man zusätzlich Satz 2.1 auf $[a]$ an. □

Die Darstellung in 2.3(2) heißt g-adische Ziffernentwicklung oder Ziffernentwicklung von x zur Basis g; die Koeffizienten c_i heißen Ziffern von x. Die Folge $(c_i)_{i\geq 1}$ heißt g-adische Nachkommafolge. Die Entwicklung heißt abbrechend wenn nur endlich viele $c_i \neq 0$ sind.

Schreibweise: $c_{-k} c_{-k+1} \dots c_0, c_1 c_2 \dots$

bzw. $(c_{-k} c_{-k+1} \dots c_0, c_1 c_2 \dots)_g$

2.3 Entwicklung rationaler Zahlen

Def. Sei $(c_i)_{i\geq 1}$ eine Folge in $S_g = \{0, \dots, g-1\}$.
Die Folge $(c_i)_{i\geq 1}$ heißt periodisch (oder schließlich periodisch) wenn es $k, \ell \in \mathbb{N}$ gibt mit $c_{i+\ell} = c_i$ für alle $i \geq k$.
Sei $(c_i)_{i\geq 1}$ eine periodische Folge.

(1) $k_0 := \min\{k \in \mathbb{N}_0 : \exists \ell \in \mathbb{N}\ \forall i > k : c_{i+\ell} = c_i\}$
heißt Vorperiodenlänge. Ist $k_0 \geq 1$, so heißt $(c_1, \dots, c_{k_0})$ Vorperiode. Ist $k_0 = 0$, so heißt $(c_i)_{i\geq 1}$ rein periodisch

(2) Ist $k_0 \in \mathbb{N}_0$ die Vorperiodenlänge, so heißt
$\ell_0 := \min\{\ell \in \mathbb{N} : c_{i+\ell} = c_i$ für $i > k_0\}$
die Periodenlänge und $(c_{k_0+1}, \dots, c_{k_0+\ell_0})$ die primitive Periode von $(c_i)_{i\geq 1}$

Satz 2.4 Eine reelle Zahl ist genau dann rational, wenn ihre g-adische Ziffernfolge periodisch ist.

Beweis „$\Rightarrow$" Sei $\alpha = \frac{a}{b}$ mit $a \in \mathbb{Z}$, $b \in \mathbb{N}$. Die g-adische Nachkommafolge ergibt sich nach Korollar 2.3(1) rekursiv durch

$$\alpha_1 = \{\tfrac{a}{b}\}, \quad c_i = \lfloor \alpha_i g \rfloor, \quad \alpha_{i+1} = \{\alpha_i g\} \text{ für } i \geq 1.$$

$b_i := \alpha_i b$

Es ist $b_1 = \alpha_1 b \in \mathbb{N}_0$ und (induktiv) für alle $i \geq 1$ auch

$$\underbrace{\alpha_{i+1} b}_{b_{i+1}} = \underbrace{(\alpha_i g b)}_{\in \mathbb{N}_0} - \underbrace{\lfloor \alpha_i g \rfloor b}_{\in \mathbb{N}_0} \in \mathbb{N}_0.$$

$0 \leq \alpha_i < 1 \Rightarrow \alpha_i b \in S_b$ für alle $i \geq 1$.

S_b ist endlich, also gibt es $1 \leq k < \ell$ mit $\alpha_k b = \alpha_\ell b$

$\Rightarrow \alpha_k = \alpha_\ell \Rightarrow \forall i \geq k: \alpha_i = \alpha_{i+\ell} \Rightarrow \forall i \geq k: c_i = c_{i+\ell}$.

„$\Leftarrow$" Sei $\alpha \in \mathbb{R}$ mit g-adischer Nachkommafolge $(c_i)_{i \geq 1}$ und seien $k \in \mathbb{N}_0$, $\ell \in \mathbb{N}$: $\forall i > k: c_i = c_{i+\ell}$.

$$\Rightarrow \{\alpha\} = \sum_{i=1}^{\infty} c_i g^{-i} = \sum_{i=1}^{k} c_i g^{-i} + \sum_{i=k+1}^{\infty} c_i g^{-i} = \sum_{i=1}^{k} c_i g^{-i} + \sum_{i=0}^{\infty} \sum_{j=1}^{\ell} c_{k+i\ell+j} g^{-(k+i\ell+j)}$$

$$= \sum_{i=1}^{k} c_i g^{-i} + \sum_{i=0}^{\infty} \sum_{j=1}^{\ell} c_{k+j} g^{-(k+i\ell+j)}$$

$$= \sum_{i=1}^{k} c_i g^{-i} + \sum_{j=1}^{\ell} c_{k+j} g^{-k-j} \underbrace{\sum_{i=0}^{\infty} \left(g^{-\ell}\right)^i}_{= \frac{g^\ell}{g^\ell - 1}}$$

$$= \frac{1}{g^k (g^\ell - 1)} \Bigg(\underbrace{\sum_{i=1}^{k} c_i g^{k-i} (g^\ell - 1) + \sum_{j=1}^{\ell} c_{k+j} g^{\ell - j}}_{\in \mathbb{N}_0} \Bigg) \in \mathbb{Q} \qquad (*)$$

$\Rightarrow \alpha = \lfloor \alpha \rfloor + \{\alpha\} \in \mathbb{Q}$.

□

Bem: (1) Sei $\alpha \in \mathbb{Q}$ und seien a_i, c_i, b_i wie im Beweis von Satz 2.4. Dann ist

$$b_1 = \left\{\frac{a}{b}\right\} b, \qquad b_i g = c_i b + \underbrace{b_{i+1}}_{\in \{0,\dots,b-1\}}.$$

D.h. für $i \geq 1$ erhält man (c_i, b_{i+1}) indem man $b_i g$ mit Rest durch b dividiert.

(2) Ist die Ziffernfolge von $\frac{a}{b}$ periodisch mit Vorperiode $(c_1, \dots, c_k)$ und primitiver Periode $(c_{k+1}, \dots, c_{k+\ell})$, so schreibt man

$$\frac{a}{b} = (c_1 \dots c_k \overline{c_{k+1} \dots c_{k+\ell}})_g$$

Periodizitätseigenschaften

Erinnerung: Sei $m \in \mathbb{N}$ mit $ggT(m,g) = 1$. Dann gibt es $x \in \mathbb{Z}$ mit $gx \equiv 1 \bmod m$ (euklidischer Algorithmus).

Anders ausgedrückt: Die Restklasse $[g] = [g]_m \in \mathbb{Z}/m\mathbb{Z}$ ist invertierbar. ($[g][x] = [1]$).

Es gibt dann ein $k \in \mathbb{N}$ mit $g^k \equiv 1 \bmod m$

(Denn: $\{1, g, g^2, \dots\}$ ist unendlich, also gibt es $i < j$ mit $g^i \equiv g^j \bmod m \overset{\cdot x^i}{\Rightarrow} g^{j-i} \equiv 1 \bmod m$)

Das kleinste $k \in \mathbb{N}$ mit $g^k \equiv 1 \bmod m$ heißt multiplikative Ordnung von g modulo m, $\operatorname{ord}_m(g)$.

z.B.: $g = 3$, $m = 10$: $3^2 \equiv 9 \equiv -1 \bmod 10$, $3^3 \equiv -3 \bmod 10$

$3^4 \equiv -9 \equiv 1 \bmod 10$

$\Rightarrow \operatorname{ord}_{10}(3) = 4$.

Es gilt $\operatorname{ord}_m(g) \mid \varphi(m)$ (Satz von Euler). Ist $\operatorname{ord}_m(g) = \varphi(m)$, so heißt g Primitivwurzel modulo m.

Ist $g^k \equiv 1 \bmod m$ für ein $k \in \mathbb{N}_0$, so folgt $\operatorname{ord}_m(g) \mid k$.

Primitivwurzeln existieren $\Leftrightarrow m \in \{2, 4, p^k, 2p^k : p \in \mathbb{P} \setminus \{2\}, k \geq 1\}$.

Jedes $b \in \mathbb{N}$ lässt sich in eindeutiger Weise schreiben als $b = b^* b^{**}$, so dass gilt $ggT(b^*, g) = 1$ und $b^{**} \mid g^k$ für ein $k \in \mathbb{N}$.

[Wähle $b^* = \max\{d \in \mathbb{N} : d \mid b \text{ und } ggT(d, b) = 1\}$ und $b^{**} = \frac{b}{b^*}$.]

In der Primfaktorenzerlegung: b^* besteht aus jenen Primfaktoren von b, die g nicht teilen

b^{**} — " — die g teilen.

Bsp: $b = 12 = 3 \cdot 2^2$, $g = 10 \Rightarrow b^* = 3$, $b^{**} = 4$.

Satz 2.5 Sei $\alpha = \frac{a}{b}$ mit $a \in \mathbb{Z}$, $b \in \mathbb{N}$, $ggT(a,b) = 1$ und $b = b^* b^{**}$ wie soeben. Sei $(c_i)_{i \geq 1}$ die g-adische Nachkommafolge von α. Dann ist $ord_{b^*}(g)$ die Periodenlänge und $\min\{k \in \mathbb{N}_0 : b^{**} \mid g^k\}$ die Vorperiodenlänge von $(c_i)_{i \geq 1}$.

Beweis: Nach Satz 2.4 ist $(c_i)_{i \geq 1}$ periodisch; seien k bzw. $\ell \geq 1$ die Vorperioden- bzw. Periodenlänge von $(c_i)_{i \geq 1}$.

Sei $m := \min\{t \in \mathbb{N}_0 : b^{**} \mid g^t\}$ und $n = ord_{b^*}(g)$.

Zeigen zuerst: $m \leq k$ und $n \leq \ell$.

Nach (*) aus dem Beweis von Satz 2.4 gilt

$$\frac{a}{b} = \frac{A}{g^k(g^\ell - 1)} \quad \text{für ein } A \in \mathbb{Z}.$$

$\overset{ggT(a,b)=1}{\Longrightarrow} b \mid g^k(g^\ell - 1) \Rightarrow b^* \mid g^\ell - 1$ und $b^{**} \mid g^k$

$\Rightarrow g^\ell \equiv 1 \bmod b^*$, also $n \leq \ell$ und $m \leq k$.

Wegen $b^{**} \mid g^m$, $b^* \mid g^n - 1$ folgt $b = b^* b^{**} \mid g^m (g^n - 1)$

$\Rightarrow \left\{\frac{a}{b}\right\} g^m (g^n - 1) \in \mathbb{N}_0$

Also gibt es $u, v \in \mathbb{N}_0$ mit

$$\left\{\frac{a}{b}\right\} g^m (g^n - 1) = u (g^n - 1) + v \quad \text{und} \quad 0 \leq v < g^n - 1 \qquad (*)$$

(Division mit Rest). Dann ist $0 \leq u < g^m$.

Sei $u = u_m + u_{m-1} g + \dots + u_1 g^{m-1}$ und $v = v_n + v_{n-1} g + \dots + v_1 g^{n-1}$.

Wegen $v < g^n - 1$ gibt es ein $0 \leq i_0 \leq n-1$ mit $v_{i_0} \neq g-1$.

Einsetzen in $(*)$:

$$\left\{\frac{a}{b}\right\} = u g^{-m} + v \underbrace{(g^n - 1)^{-1}}_{= g^{-n} \sum_{k=0}^{\infty} g^{-nk}} g^{-m} = \sum_{i=1}^{m} u_i g^{-i} + g^{-m} \left(\sum_{j=1}^{n} v_j g^{-j}\right)\left(\sum_{k=0}^{\infty} g^{-nk}\right) =$$

$$= \sum_{i=1}^{m} u_i g^{-i} + \sum_{k=0}^{\infty} \sum_{j=1}^{n} v_j g^{-nk-m-j} = \sum_{i=1}^{\infty} d_i g^{-i}$$

mit $\begin{cases} d_i = u_i & \text{für } 1 \leq i \leq m \\ d_{m+nk+j} = v_j & \text{für } k \geq 0,\ 1 \leq j \leq n. \end{cases}$

$d_i \in S_g$ und wegen $v_{i_0} \neq g-1$, sind unendlich viele $d_i \neq g-1$, d.h. hierbei handelt es sich um die g-adische Ziffernentwicklung von $\left\{\frac{a}{b}\right\}$, und diese hat Vorperiodenlänge $\leq m$ und Periodenlänge $\leq n$, also folgt: $m = k$ und $n = l$.

□

(*) (Bsp) von S. 43 $(0,123455789101111\dots)$

Korollar 2.6 Die g-adische Entwicklung von $\frac{a}{b}$ mit $a \in \mathbb{Z}$, $b \in \mathbb{N}$ und $ggT(a,b)=1$, ist genau dann abbrechend, wenn es ein $k \in \mathbb{N}_0$ gibt mit $b \mid g^k$ ($\Leftrightarrow b^* = 1$ $\Leftrightarrow$ alle Primfaktoren von b teilen g)

Beweis Die g-adische Entwicklung von $\frac{a}{b}$ ist abbrechend

$$\Leftrightarrow \left\{\frac{a}{b}\right\} = \sum_{i=1}^{e} c_i g^{-i} \text{ für geeignete } c_i \in S_g$$

$$\Leftrightarrow \exists A \in \mathbb{Z}: \frac{a}{b} = \frac{A}{g^e} \overset{ggT(a,b)=1}{\Leftrightarrow} b \mid g^e \qquad \square$$

Bemerkungen

(1) Die Ziffernfolge ist reinperiodisch $\Leftrightarrow b^* = 1 \Leftrightarrow ggT(b,g)=1$.

(2) Die Periodenlänge ist $1 \Leftrightarrow g \equiv 1 \bmod b^*$. (z.B. $g=10$, $b=3$)

(3) Perioden- und Vorperiodenlänge hängen nur vom reduzierten Nenner, nicht aber vom Zähler, ab!

(4) Ist g eine Primitivwurzel modulo b^*, so ist $ord_{b^*}(g) = \varphi(b^*)$.
(z.B. $g=10$ ist Primitivwurzel modulo $b=b^*=7$, weswegen $\frac{1}{7}$ Periodenlänge $\varphi(7)=6$ hat)

Bsp: $\frac{1}{7} = 0,\overline{142857}$, $\frac{2}{7} = 0,\overline{285714}$, $\frac{3}{4} = 0,\overline{428571}$, $\frac{4}{7} = 0,\overline{571428}$,
$\frac{5}{7} = 0,\overline{714285}$, $\frac{6}{7} = 0,\overline{857142}$

Satz 2.7 Sei $p \in \mathbb{P}$ mit $p \nmid g$, so dass $\mathrm{ord}_p(g) = \varphi(p) = p-1$. Dann haben die Zahlen $\frac{a}{p}$, $1 \le a \le p-1$ reinperiodische g-adische Entwicklungen der P.L. $p-1$ und ihre Perioden gehen auseinander durch zyklische Vertauschung hervor.

Beweis: Nach Satz 2.5 ist die Darstellung reinperiodisch mit PL $\mathrm{ord}_p(g) = p-1$. Betrachten zuerst $\alpha = \frac{1}{p}$.

Sei $b_1 = \{\frac{1}{p}\}p = 1$, $b_i g = c_i p + b_{i+1}$ mit $c_i \in \mathbb{N}_0$, $0 \le b_{i+1} < p$ (*) für $i \ge 1$. Dann ist $(c_i)_{i \ge 1}$ die g-adische Nachkommafolge von $\frac{1}{p}$ (Bem nach Satz 2.4).

Es gilt:

- $b_i \neq 0$ für alle $i \ge 1$ (sonst wäre die Entwicklung abbrechend)
- $b_1, \dots, b_{p-1}$ sind paarweise verschieden (sonst wäre die PL $< p$)

Also ist $\{b_1, \dots, b_{p-1}\} = \{1, \dots, p-1\}$, d.h. $\exists i: 1 \le i \le p-1 \wedge b_p = b_i$.
Da die PL $p-1$ ist, muss aber $i = 1$, also $b_p = b_1$ gelten.

Sei nun $1 \le a \le p-1$ und seien

$$b_1' := \{\tfrac{a}{p}\}p = a, \quad b_i' g = c_i' p + b_{i+1}' \text{ mit } c_i' \in \mathbb{N}_0,\ 0 \le b_{i+1}' < p,$$

Dann gibt es ein $1 \le i \le p-1$ mit $b_1' = b_i$. Entsprechend ist $b_j' = b_{i+(j-1)}$ für alle $j \ge 1$, und deshalb $c_j' = c_{i+(j-1)}$, d.h.

$$\frac{a}{p} = 0, \overline{c_i c_{i+1} \dots c_{p-1} c_1 \dots c_{i-1}}$$

□

Bsp: Sei $\alpha = 0,1234567891011121314\ldots$

Dann ist α irrational, denn die Ziffernfolge enthält beliebig lange Folgen von 0'en (von 10^k), aber bricht nicht ab. (α ist sogar transzendent)

2.4 Cantorsche Entwicklung

Sei $(q_i)_{i\geq 1}$ eine Folge in $\mathbb{N}_{\geq 2}$ und $P_i := q_1 \cdots q_i$ für $i \geq 0$.

Satz 2.8 (Cantorsche Entwicklung)

Jedes $\alpha \in \mathbb{R}$ besitzt eine eindeutige Darstellung

$$\alpha = \lfloor \alpha \rfloor + \sum_{i=1}^{\infty} c_i P_i^{-1}$$

mit $c_i \in S_{q_i}$ $(i \geq 1)$ und $c_i \neq q_i - 1$ unendlich oft.

Die Folge $(c_i)_{i\geq 1}$ ergibt sich rekursiv durch

$$\alpha_1 := \{\alpha\}, \qquad \alpha_{i+1} := \{\alpha_i q_i\}, \quad c_i := \lfloor \alpha_i q_i \rfloor \text{ für } i \geq 1.$$

Beweis: Existenz: Induktiv folgt: $\forall n \geq 0$:

$$\alpha = \lfloor \alpha \rfloor + \sum_{i=1}^{n} c_i P_i^{-1} + \alpha_{n+1} P_n^{-1}. \qquad (*)$$

$$0 \leq \alpha_{n+1} < 1 \;\wedge\; P_n^{-1} < \frac{1}{2^n} \Rightarrow \lim_{n\to\infty} \alpha_{n+1} P_n^{-1} = 0$$

$$\Rightarrow \alpha = \lfloor \alpha \rfloor + \sum_{i=1}^{\infty} c_i P_i^{-1}.$$

Angenommen $\exists n \geq 0\ \forall i \geq n \quad c_i = q_i - 1$

$$\rightarrow \sum_{i=n+1}^{\infty} c_i P_i^{-1} = \sum_{i=n+1}^{\infty} P_{i-1}^{-1} - \sum_{i=n+1}^{\infty} P_i^{-1} = P_n^{-1}$$

$$(*) \Rightarrow P_n^{-1} = \alpha_{n+1} P_n^{-1} \Rightarrow \alpha_{n+1} = 1 \quad \lightning$$

Eindeutigkeit Angenommen $\alpha = \lfloor\alpha\rfloor + \sum_{i=1}^{\infty} c_i P_i^{-1} = c' + \sum_{i=1}^{\infty} c_i' P_i^{-1}$ sind zwei verschiedene Cantorsche Darstellungen. Dann ist $c' = \lfloor\alpha\rfloor$ mega $\sum_{i=1}^{\infty} c_i' P_i^{-1} < 1$.

Sei $n \geq 1$ minimal mit $c_n' \neq c_n$.

$$\Rightarrow |c_n' - c_n| = \left| P_n \sum_{i=n+1}^{\infty} (c_i - c_i') P_i^{-1} \right| < P_n \underbrace{\sum_{i=n+1}^{\infty} (g_i - 1) P_i^{-1}}_{= P_n^{-1}}$$

(Es gilt die strikte Ungleichung, weil sonst $c_i - c_i' = g_i - 1$ oder $c_i' - c_i = g_i - 1$ für alle $i > n$)

$\Rightarrow c_n' - c_n$ ↯.

□

Korollar 2.9 Sei $(g_i)_{i \geq 1}$ zusätzlich derart, dass jedes $p \in \mathbb{P}$ endlich viele der g_i teilt. ~~Ist $\alpha \in \mathbb{R}$ und $(c_i)_{i \geq 1}$ die „Cantorsche Nachkommafolge" wie in Satz 2.8, so folgt:~~ Dann gilt

$\alpha \in \mathbb{Q} \Leftrightarrow$ nur endlich viele c_i sind $\neq 0$.

Beweis: „$\Leftarrow$": Klar

„$\Rightarrow$" Sei $\alpha = \frac{a}{b}$. Es gibt ein $n \geq 0$ mit $b \mid P_n$.

$$\Rightarrow \underbrace{\left\{\frac{a}{b}\right\}}_{\in \mathbb{Z}} P_n = \underbrace{\sum_{i=1}^{n} c_i P_n P_i^{-1}}_{\in \mathbb{Z}} + \underbrace{P_n \sum_{i=n+1}^{\infty} c_i P_i^{-1}}_{\in [0,1)}$$

$$\Rightarrow \left\{\frac{a}{b}\right\} P_n = \sum_{i=1}^{n} c_i P_n P_i^{-1}.$$

□

Bsp: $e = 1 + \sum_{n=1}^{\infty} \frac{1}{n!}$ ist irrational.

(Tatsächlich sogar transzendent)

3. Kettenbrüche

Bsp: $\frac{19}{7} = 2 + \frac{5}{7} = 2 + \frac{1}{\frac{7}{5}} = 2 + \frac{1}{1+\frac{2}{5}} = 2 + \frac{1}{1+\frac{1}{\frac{5}{2}}} =$

$$= 2 + \frac{1}{1+\frac{1}{2+\frac{1}{2}}} = 2 + \frac{1}{1+\frac{1}{2+\frac{1}{1+1}}}$$

Schreibweise: $\frac{19}{7} = [2; 1, 2, 2] = [2; 1, 2, 1, 1]$

Def 3.1 Sei $(a_i)_{i\geq 0} = (a_0, \dots, a_n (, \dots))$ eine (endliche oder unendliche) Folge in $\mathbb{R}$, mit $a_i > 0$ für $i \geq 1$. Für $n \geq 0$ sei der Kettenbruch $[a_0; a_1, \dots, a_n] \in \mathbb{R}$ rekursiv definiert durch

$$[a_0] := a_0, \quad [a_0; a_1, \dots, a_{n-1}, a_n] := [a_0; a_1, \dots, a_{n-2}, a_{n-1} + \frac{1}{a_n}]$$

(insb. $[a_0; a_1] = a_0 + \frac{1}{a_1}$)

Weiters seien Folgen $(p_i)_{i\geq -2}$, $(q_i)_{i\geq -2}$ rekursiv definiert durch

$$p_{-2} = 0, \ p_{-1} = 1, \quad p_i := a_i p_{i-1} + p_{i-2},$$

$$q_{-2} = 1, \ q_{-1} = 0, \quad q_i := a_i q_{i-1} + q_{i-2}.$$

(sogl. ish)

Für $i \geq 0$ heißen p_i bzw. q_i i-ter Näherungszähler bzw. i-ter Näherungsnenner, und $\frac{p_i}{q_i}$ i-ter Näherungsbruch dieses Kettenbruchs.

Bem: $q_0 = 1$ und $q_i > 0$ für alle $i \geq 1$

Ist $a_i \in \mathbb{Z}$ für alle $i \geq 0$, so gilt: $p_i \in \mathbb{Z}$, ,

$q_0 = 1$, $q_i \geq q_{i-1} + q_{i-2} \Rightarrow q_i \geq i$ für $i \geq 1$, also $q_i \in \mathbb{N}$.

Ist $(a_i)_{i\geq 0}$ endlich, so ist $(q_i)_{i\geq 0}$ unbeschränkt

Wir behalten im Folgenden die Notation aus Def. 3.1.

Lemma 3.2

(1) $\forall 0 \leq i \,[\leq k]$: $[a_0, a_1, \ldots, a_{i-1}, X] = \dfrac{p_{i-1}X + p_{i-2}}{q_{i-1}X + q_{i-2}}$ (X Unbestimmte bzw. $X \in \mathbb{R}_{>0}$)

Insb. $[a_0, a_1, \ldots, a_i] = \dfrac{p_i}{q_i}$

(2) $\forall 0 \leq m < n$: $[a_0, a_1, \ldots, a_n] = [a_0, a_1, \ldots, a_m, [a_{m+1}, \ldots, a_n]]$

Beweis: (1) Induktion nach i. $i=0$ ✓

$i \geq 0$, $i \to i+1$:

$$[a_0, a_1, \ldots, a_i, X] = \left[a_0, a_1, \ldots, a_i + \frac{1}{X}\right] = \frac{p_{i-1}\left(a_i + \frac{1}{X}\right) + p_{i-2}}{q_{i-1}\left(a_i + \frac{1}{X}\right) + q_{i-2}}$$

$$= \frac{p_i + p_{i-1}\frac{1}{X}}{q_i + q_{i-1}\frac{1}{X}} = \frac{p_i X + p_{i-1}}{q_i X + q_{i-1}}.$$

(2) Induktion nach n bei festem $m \geq 0$.

$n = m+1$ ✓

$n > m+1$, $n-1 \to n$:

$$[a_0, a_1, \ldots, a_m, [a_{m+1}, \ldots, a_{n-1}, a_n]] = \left[a_0, a_1, \ldots, a_m, \left[a_{m+1}, \ldots, a_{n-1} + \frac{1}{a_n}\right]\right]$$

$$\overset{IV}{=} \left[a_0, a_1, \ldots, a_m, a_{m+1}, \ldots, a_{n-1} + \frac{1}{a_n}\right] = [a_0, a_1, \ldots, a_n]$$

□

Lemma 3.3

(1) $\forall -1 \leq i \,[\leq k]$: $p_{i-1}q_i - p_i q_{i-1} = (-1)^i$

Insbesondere: $\forall i \geq -2$: $ggT(p_i, q_i) = 1$, $ggT(q_i, q_{i+1}) = 1$, $ggT(p_i, p_{i+1}) = 1$

und $\forall i \geq 1$: $\dfrac{p_{i-1}}{q_{i-1}} - \dfrac{p_i}{q_i} = \dfrac{(-1)^i}{q_{i-1}q_i}$

(2) $\forall 0 \leq i \,[\leq k]$: $p_{i-2}q_i - p_i q_{i-2} = (-1)^{i-1}a_i$

und $\forall i \geq 2$: $\dfrac{p_{i-2}}{q_{i-2}} - \dfrac{p_i}{q_i} = \dfrac{(-1)^{i-1}a_i}{q_{i-2}q_i}$

Beweis: (1) Induktion nach i. $i=-1$ ✓

$i \geq -1$, $i \to i+1$:

$$p_i q_{i+1} - p_{i+1} q_i = p_i \left(a_{i+1} q_i + q_{i-1}\right) - \left(a_{i+1} p_i + p_{i-1}\right) q_i$$

$$= -\left(p_{i-1} q_i - p_i q_{i-1}\right) \overset{IV}{=} -(-1)^i.$$

(2) analog □

Proposition 3.4: (1) $\frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \dots$

(2) $\frac{p_1}{q_1} > \frac{p_3}{q_3} > \frac{p_5}{q_5} > \dots$

(3) Ist n gerade und m ungerade, so gilt

$$\frac{p_n}{q_n} < \frac{p_m}{q_m}.$$

Beweis: (1) & (2) Folgen aus Lemma 3.3 (2).

(3) Fall 1: $n < m$:

$$\frac{p_n}{q_n} \overset{(1)}{<} \frac{p_{m-1}}{q_{m-1}} < \frac{p_m}{q_m}$$

↑ Lemma 3.3 (1)

Fall 2: $m < n$:

$$\frac{p_m}{q_m} \overset{(1)}{>} \frac{p_{n-1}}{p_{n-1}} > \frac{p_n}{q_n}$$

↑ Lemma 3.3 (1)

□

Def. 3.5 Seien $a_0 \in \mathbb{Z}$, $a_1, \dots, a_n \in \mathbb{N}$ und $z \in \mathbb{Q}$.
Ist $z = [a_0; a_1, \dots, a_n]$, so nennt man diese Gleichung eine (endliche) Kettenbruchentwicklung von z.

Satz 3.6 Jedes $z \in \mathbb{Q}$ besitzt genau zwei (endliche) Kettenbruchentwicklungen:

$z = [a_0; a_1, \dots, a_n] = [a_0; a_1, \dots, a_k - 1, 1]$ mit $a_0 \in \mathbb{Z}, a_1, \dots, a_n \in \mathbb{N}$

entweder $k = 0$ oder $k \geq 1$ und $a_k \geq 2$.

Beweis: Existenz einer Darstellung:

Sei $z = \frac{a}{b}$ mit $a \in \mathbb{Z}$, $b \in \mathbb{N}$, $ggT(a,b) = 1$

Fall 1: $z = a \in \mathbb{Z}$: $z = [a] = [a-1; 1]$.

Fall 2: $z \in \mathbb{Q} \setminus \mathbb{Z}$. $(b \nmid a)$

Euklidischer Algorithmus liefert, mit $r_{-1} := a$, $r_0 := b$,

$$\overset{a}{r_{-1}} = \overset{b}{r_0}\, a_0 + r_1 \quad \text{mit } a_0 \in \mathbb{Z},\ 1 \le r_1 \le r_0 - 1$$

$$r_0 = r_1 a_1 + r_2 \quad \text{mit } a_1 \in \mathbb{N},\ 1 \le r_2 \le r_1 - 1$$

$$r_1 = r_2 a_2 + r_3 \quad \text{mit } a_2 \in \mathbb{N},\ 1 \le r_3 \le r_2 - 1$$

$$\vdots$$

$$r_{k-2} = r_{k-1} a_{k-1} + r_k \quad \text{mit } a_{k-1} \in \mathbb{N},\ 1 \le r_k \le r_{k-1} - 1$$

$$r_{k-1} = r_k a_k \quad \text{mit } a_k \in \mathbb{N},\ \boxed{a_k \ge 2.}$$

und $k \ge 1$.

Beh. A: $\forall -1 \le i \le k-1$: $\frac{a}{b} = [a_0; \dots, a_i, \frac{r_i}{r_{i+1}}]$

$i = -1$: ✓, $i \ge 0$, $i-1 \to i$

$$\frac{a}{b} \overset{IV}{=} [a_0; \dots a_{i-1}, \frac{r_{i-1}}{r_i}] = [a_0; \dots, a_{i-1}, \frac{r_i a_i + r_{i+1}}{r_i}]$$

$$= [a_0; \dots, a_{i-1}, a_i + \frac{r_{i+1}}{r_i}] = [a_0; \dots a_{i-1}, a_i, \frac{r_i}{r_{i+1}}] \qquad \square \text{(Beh.)}$$

Also: $\frac{a}{b} = [a_0; \dots, a_{k-1}, \frac{r_{k-1}}{r_k}] = [a_0; \dots, a_{k-1}, a_k] = [a_0; a_1, \dots, a_{k-1}, a_k - 1, 1]$.

Eindeutigkeit: Sei $z = [a_0; a_1, \dots, a_k]$ mit $k \ge 0$, $a_0 \in \mathbb{Z}$, $a_1, \dots, a_k \in \mathbb{N}$

Fall 1: $z \in \mathbb{Z}$ Ist $k = 0$, so ist $a = [a_0] = [a]$.

Ist $k \ge 1$, so ist $z = a_0 + \frac{1}{[a_1; a_2, \dots, a_k]}$ und $[a_1; a_2, \dots, a_k] \ge 1$.

Wegen $z - a_0 \in \mathbb{Z}$ folgt $[a_1; a_2, \dots, a_k] = 1 \overset{a_k \ge 1}{\Longrightarrow} k = 1,\ a_1 = 1$

$\Rightarrow [a_0; a_1, \dots, a_k] = [a-1; 1]$.

Fall 2: $z = \frac{a}{b} \in \mathbb{Q}$

Induktion nach b. $b=1$ ✓ (Fall 1)

Sei $b>1 \Rightarrow a_0 \leq z \leq a_0 + \frac{1}{a_1} \leq 1$

Wegen $z \notin \mathbb{Z}$ gilt $a_0 < z < a_0+1$, also ist $a_0 = \lfloor z \rfloor$ eindeutig bestimmt.

Sei $z = a_0 + \frac{a'}{b}$ mit $1 \leq a' < b$. und $\alpha_1 := \frac{b}{a'} > 1$

$\overset{IV}{\Rightarrow}$ α_1 besitzt genau zwei Kettenbruchdarstellungen

$\alpha_1 = [a_1, \dots, a_k]$ und $\alpha_1 = [a_1, \dots, a_{k-1}, 1]$.

$\Rightarrow [a_0; a_1, \dots, a_k]$ und $[a_0; a_1, \dots, a_{k-1}, 1]$ sind die einzigen Darstellungen von z. □

Proposition 3.7 (Konvergenzsatz) Sei $a_0 \in \mathbb{Z}$, $a_1, a_2, \dots \in \mathbb{N}$. Dann existiert $\lim_{n\to\infty} \frac{p_n}{q_n}$ und ist irrational. ~~Ist umgekehrt $\alpha \in \mathbb{R}\setminus\mathbb{Q}$, dann gibt es eindeutig bestimmte $a_0 \in \mathbb{Z}$, $a_1, a_2, \dots \in \mathbb{N}$ so dass $\alpha = \lim_{n\to\infty} \frac{p_n}{q_n}$.~~

Beweis: $\left(\frac{p_{2n}}{q_{2n}}\right)_{n\geq 0}$ ist monoton wachsend und beschränkt,

$\left(\frac{p_{2n+1}}{q_{2n+1}}\right)_{n\geq 0}$ ist monoton fallend und beschränkt.

$\Rightarrow$ $\alpha' := \lim_{n\to\infty} \frac{p_{2n}}{q_{2n}}$ und $\alpha'' := \lim_{n\to\infty} \frac{p_{2n+1}}{q_{2n+1}}$ existieren.

Wegen $\frac{p_{n-1}}{q_{n-1}} - \frac{p_n}{q_n} = \frac{(-1)^n}{q_n q_{n-1}}$ und $q_n \geq n$ folgt

$$0 \leq \alpha'' - \alpha' \leq \frac{p_{2n-1}}{q_{2n-1}} - \frac{p_{2n}}{q_{2n}} = \frac{1}{q_{2n} q_{2n-1}} \leq \frac{1}{(2n)(2n-1)} \to 0 \text{ für } n\to\infty \quad (n\geq 1)$$

$\Rightarrow$ $\alpha = \alpha'' = \lim_{n\to\infty} \frac{p_n}{q_n}$

Angenommen $\alpha = \frac{a}{b} \in \mathbb{Q} \Rightarrow \alpha \neq \frac{p_i}{q_i}$ für alle $i \geq 0$

$$\Rightarrow \quad \frac{1}{b q_i} \leq \left|\alpha - \frac{p_i}{q_i}\right| < \left|\frac{p_{i+1}}{q_{i+1}} - \frac{p_i}{q_i}\right| = \frac{1}{q_i q_{i+1}}$$

$\Rightarrow$ $q_{i+1} < b$ für $i \geq 0$ $\lightning$ $(q_i)_{i\geq 0}$ unbeschränkt.

□

Def 3.8 Seien $a_0 \in \mathbb{Z}$, $a_1, a_2, \ldots \in \mathbb{N}$.

Ist $\alpha = \lim\limits_{n\to\infty} \frac{p_n}{q_n} = \lim\limits_{n\to\infty} [a_0; a_1, \ldots a_n]$ so schreibt man $\alpha = [a_0; a_1, a_2, \ldots]$ und nennt diese Gleichung eine (unendliche) Kettenbruchentwicklung von α.

Satz 3.9 Jedes $\alpha \in \mathbb{R}\setminus\mathbb{Q}$ besitzt genau eine (unendliche) Kettenbruchentwicklung.

Beweis: ~~Existenz~~ Wir definieren rekursiv

$\alpha_0 := \alpha$, $a_0 := \lfloor \alpha \rfloor \in \mathbb{Z}$ und für $i \geq 1$ a_i, α_i durch $\alpha_{i-1} = a_{i-1} + \frac{1}{\alpha_i}$, $a_i := \lfloor \alpha_i \rfloor$

$\Rightarrow a_0 \in \mathbb{Z}$, $\alpha_0, \alpha_1, \ldots \in \mathbb{R}\setminus\mathbb{Q}$, $a_1, a_2, \ldots \in \mathbb{N}$, $\alpha_1, \alpha_2, \ldots > 1$

Beh: $\alpha = [a_0; a_1, a_2, \ldots]$

Für $n \geq 0$ gilt $\alpha = [a_0; a_1, a_2, \ldots, a_n, \alpha_{n+1}]$ (Induktion nach n)

$\Rightarrow \alpha = \frac{p_n \alpha_{n+1} + p_{n-1}}{q_n \alpha_{n+1} + q_{n-1}}$ ... (Lemma 3.2)

$\Rightarrow \alpha - \frac{p_n}{q_n} = \frac{q_n(p_n\alpha_{n+1} + p_{n-1}) - p_n(q_n\alpha_{n+1} + q_{n-1})}{q_n(q_n\alpha_{n+1} + q_{n-1})} = \frac{q_n p_{n-1} - p_n q_{n-1}}{q_n(q_n\alpha_{n+1} + q_{n-1})} = \frac{(-1)^n}{q_n(q_n\alpha_{n+1} + q_{n-1})}$

$\Rightarrow \left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2} \to 0$ für $n \to \infty$ $\Rightarrow \alpha = \lim\limits_{n\to\infty} \frac{p_n}{q_n} = [a_0; a_1, a_2, \ldots]$

Eindeutigkeit: $\alpha = [a_0; a_1, a_2, \ldots] = a_0 + \frac{1}{[a_1, a_2, \ldots]}$

$\Rightarrow 0 \leq \alpha - a_0 < 1 \Rightarrow a_0 = \lfloor \alpha \rfloor$ ist eindeutig

$\Rightarrow \alpha_1 = [a_1, a_2, \ldots]$ ist eindeutig $\Rightarrow a_1 = \lfloor \alpha_1 \rfloor$ ist eindeutig usw. usf. □

Bem: $\alpha \in \mathbb{Q} \Leftrightarrow \alpha$ besitzt eine endliche Kettenbruchentwicklung.
In diesem Fall ist jede Kettenbruchentwicklung von α endlich

Bsp: (1) $(\sqrt{2}-1)(\sqrt{2}+1)=1 \Rightarrow \sqrt{2}-1=\frac{1}{1+\sqrt{2}}$

$\Rightarrow \sqrt{2}=1+\frac{1}{1+\sqrt{2}} = 1+\frac{1}{1+(1+\frac{1}{1+\sqrt{2}})} = 1+\frac{1}{2+\frac{1}{1+\sqrt{2}}}$

$\Rightarrow \sqrt{2}=[1;2,1+\sqrt{2}] \overset{\text{Induktion}}{=} [1;2,2,2,\dots]$

(2) Sei $\alpha=[1;1,1,\dots]$

$\Rightarrow \alpha=[1;[1;1,1,\dots]] = 1+\frac{1}{[1;1,1,\dots]} = 1+\frac{1}{\alpha}$

$\Rightarrow \alpha^2-\alpha-1=0$

$\Rightarrow \alpha=\frac{1+\sqrt{5}}{2}$ (wegen $\alpha \geq 1$)

Näherungszähler/-nenner: $p_n=p_{n-1}+p_{n-2}$, $p_0=1$, $p_1=2$

$q_n=q_{n-1}+q_{n-2}$, $q_0=1$, $q_1=1$

$\Rightarrow q_n=F_{n+1}$, $p_n=F_{n+2}$ mit $(F_n)_{n\geq 0}$ der Fibonaccifolge.

3.1 Periodische Kettenbrüche

Def: 3.10 Ein unendlicher Kettenbruch $[a_0;a_1,a_2,\dots]$ heißt periodisch, wenn die Folge $(a_i)_{i\geq 0}$ periodisch ist.
Ist $(a_i)_{i\geq 0}$ periodisch mit VPL $k\geq 0$ und PL $m\geq 1$, so schreibt man $[a_0;a_1,\dots,a_{k-1},\overline{a_k,\dots,a_{k+m-1}}]$

Bsp: (1) Sei $\beta=[2;3,2,3,\dots]=\overline{[2,3]}$

$\Rightarrow \beta=[2;3,\beta]=2+\frac{1}{3+\frac{1}{\beta}}$

ausrechnen $\Rightarrow 3\beta^2-6\beta-2=0 \overset{\beta>0}{\Longrightarrow} \beta=\frac{3+\sqrt{15}}{3}$

(2) Sei $\alpha=[4;1,\overline{2,3}] \Rightarrow \alpha=4+\frac{1}{1+\frac{1}{\beta}}=4+\frac{\beta}{\beta+1}=\frac{29+\sqrt{15}}{7}$.

Def 3.11 Eine Zahl $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ heißt (reell)-quadratische Irrationalzahl, wenn es ein quadratisches Polynom $f \in \mathbb{Q}[X]$ gibt mit $f(\alpha) = 0$.
($\Leftrightarrow$ α ist algebraisch vom Grad 2)

Satz 3.12 (Euler „$\Rightarrow$" 1737; Lagrange „$\Leftarrow$" 1770)
Die Kettenbruchentwicklung von $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ ist genau dann periodisch, wenn α eine quadratische Irrationalzahl ist.

Beweis: „$\Rightarrow$" Sei $\alpha = [b_0; b_1, \dots, b_{k-1}, \overline{a_0, a_1, \dots, a_{m-1}}]$ und $\beta = \overline{[a_0, \dots, a_{m-1}]}$.

$\Rightarrow \beta = [a_0, \dots, a_{m-1}, \beta] \overset{L3.2(1)}{=} \frac{p_{m-1}\beta + p_{m-2}}{q_{m-1}\beta + q_{m-2}}$, wobei $(p_i)_{i \geq -2}$, $(q_i)_{i \geq -2}$ die Folge der Näherungszähler/-nenner von β ist.

$\Rightarrow \beta(q_{m-1}\beta + q_{m-2}) - p_{m-1}\beta - p_{m-2} = 0$

$\Rightarrow \underbrace{q_{m-1}}_{\neq 0}\beta^2 + (q_{m-2} - p_{m-1})\beta - p_{m-2} = 0$

Wegen $\beta \notin \mathbb{Q}$ ist β quadratische Irrationalzahl;

$\alpha = \frac{\beta p + p'}{\beta q + q'}$ wobei $\frac{p'}{q'}, \frac{p}{q}$ die letzten beiden Näherungsbrüche von $[b_0; b_1, \dots, b_{k-1}]$ sind

Da β die Form $\frac{a \pm \sqrt{b}}{c}$ mit $a, b, c \in \mathbb{Z}$, $c \neq 0$ hat, gilt das auch für α.
Wegen $\alpha \notin \mathbb{Q}$ ist α eine quadratische Irrationalzahl.

„⇐" Sei $\alpha = \frac{a+\sqrt{b}}{c}$ mit $a,b,c \in \mathbb{Z}$, $b>0$, $c \neq 0$ und b ist kein Quadratzahl (in $\mathbb{Z}$).

$\xRightarrow{\cdot|c|/|c|}$ $\alpha = \frac{ac+\sqrt{bc^2}}{c^2}$ oder $\alpha = \frac{-ac+\sqrt{bc^2}}{-c^2}$ (je nach Vz. von c)

D.h. $\alpha = \frac{s_0+\sqrt{d}}{t_0}$ mit $d, s_0, t_0 \in \mathbb{Z}$, $t_0 \neq 0$, d ist kein Quadrat, und $t_0 \mid d - s_0^2$.

(Algorithmus) Definiere rekursiv

$\forall i \geq 0$: $a_i := \lfloor \alpha_i \rfloor$, $\alpha_i := \frac{s_i+\sqrt{d}}{t_i}$, $s_{i+1} := a_i t_i - s_i$, $t_{i+1} := \frac{d-s_{i+1}^2}{t_i}$

Dann gilt:

$$\alpha_i - a_i = \frac{s_i+\sqrt{d}-a_i t_i}{t_i} = \frac{\sqrt{d}-s_{i+1}}{t_i} = \frac{d^2-s_{i+1}}{t_i(\sqrt{d}+s_{i+1})} = \frac{t_{i+1}}{\sqrt{d}+s_{i+1}} = \frac{1}{\alpha_{i+1}}$$

Also: $\alpha_i = [a_i; \alpha_{i+1}]$

Induktiv $\Longrightarrow$ $\alpha_0 = \alpha = [a_0; a_1, a_2, \dots, a_{n-1}, \alpha_n] = [a_0; a_1, a_2, \dots]$

Wegen $0 < \alpha_i - a_i = \frac{1}{\alpha_{i+1}} < 1$ folgt $\alpha_{i+1} > 1$, also $a_{i+1} \geq 1$ für $i \geq 0$.

Also ist dies die Kettenbruchentwicklung von α.

Beh A: $\forall i \geq 0$: $s_i, t_i \in \mathbb{Z}$, $t_i \neq 0$, $t_i \mid d - s_i^2$.

Bew A: Induktion nach i. $i=0$ ✓

$i \geq 0$, $i \to i+1$: $s_{i+1} = a_i t_i - s_i \Rightarrow s_{i+1} \in \mathbb{Z}$

$$t_{i+1} = \frac{d-s_{i+1}^2}{t_i} = \frac{d - a_i^2 t_i^2 + 2a_i t_i s_i - s_i^2}{t_i} = \underbrace{\frac{d-s_i^2}{t_i}}_{\in \mathbb{Z} \text{ (IV)}} + \underbrace{a_i^2 t_i + 2a_i s_i}_{\in \mathbb{Z}}$$

$\Rightarrow t_{i+1} \in \mathbb{Z}$.

Wäre $t_{i+1} = 0 \Rightarrow d = s_{i+1}^2 \Rightarrow d$ ist ein Quadrat ↯

$t_i = \frac{d-s_{i+1}^2}{t_{i+1}} \Rightarrow t_{i+1} \mid d - s_{i+1}^2$.

$\square$ (Beh A)

Sei α_i' die zu α_i konjugierte Zahl, d.h. $\alpha_i' = \frac{S_i - \sqrt{d}}{t_i}$.

Aus $\alpha_0 = \frac{\alpha_n p_{n-1} + p_{n-2}}{\alpha_n q_{n-1} + p_{n-2}}$ (Lemma 3.2) folgt $\alpha_0' = \frac{\alpha_n' p_{n-1} + p_{n-2}}{\alpha_n' q_{n-1} + q_{n-2}}$

$\Rightarrow$ (N.R) $\alpha_n' = -\frac{q_{n-2}}{q_{n-1}} \left(\frac{\alpha_0' - \frac{p_{n-2}}{q_{n-2}}}{\alpha_0' - \frac{p_{n-1}}{q_{n-1}}} \right)$ $\to \alpha_0$ für $n \to \infty$

$\to \alpha_0$

Wegen $\sqrt{d} \neq 0$ ist $\alpha_0' \neq \alpha_0$, also $\lim_{n\to\infty} \frac{\alpha_0' - \frac{p_{n-2}}{q_{n-2}}}{\alpha_0' - \frac{p_{n-1}}{q_{n-1}}} = 1$

$\Rightarrow \exists N \geq 0 \; \forall n \geq N: \; \frac{\alpha_0' - \frac{p_{n-2}}{q_{n-2}}}{\alpha_0' - \frac{p_{n-1}}{q_{n-1}}} > 0$

$\Rightarrow \forall n \geq N: \; \alpha_n' < 0$.

Wegen $\alpha_n > 0$ folgt $\alpha_n - \alpha_n' = \frac{2\sqrt{d}}{t_n} > 0 \Rightarrow t_n > 0$ für $n > N$.

Weiters:

$$0 > \underbrace{\alpha_n}_{>0} \underbrace{\alpha_n'}_{<0} = \frac{S_n^2 - d}{t_n} \Rightarrow \boxed{|S_n| < \sqrt{d}} \quad (n > N)$$

Wegen $\alpha_n > 1$:

$$\underline{0 < t_n} < S_n + \sqrt{d} < \underline{2\sqrt{d}}$$

$\Rightarrow \{ (S_n, t_n) : n > N \}$ ist endlich.

$\Rightarrow \exists j, k \in \mathbb{N}: \; j < k: \quad S_j = S_k, \; t_j = t_k$

$\Rightarrow \alpha_j = \alpha_k$, also

$$\alpha = [a_0, \dots, a_{j-1}, \overline{a_j, a_{j+1}, \dots, a_{k-1}}].$$

□

Bem: Ist $t_i > 0$, so gilt $a_i = \left\lfloor \frac{S_i + \sqrt{d}}{t_i} \right\rfloor = \left\lfloor \frac{S_i + \lfloor \sqrt{d} \rfloor}{t_i} \right\rfloor$

(Sei $u = \left\lfloor \frac{S_i + \sqrt{d}}{t_i} \right\rfloor \Rightarrow S_i + \sqrt{d} = t_i u + v$ mit $0 \leq v \leq t_i - 1$

$\Rightarrow u \leq \frac{S_i + \sqrt{d}}{t_i} < \frac{S_i + \sqrt{d} + 1}{t_i} \leq u + 1$, also $u = \left\lfloor \frac{S_i + \lfloor \sqrt{d} \rfloor}{t_i} \right\rfloor$)

D.h. man braucht nur $\lfloor \sqrt{d} \rfloor$ an der Stelle $\sqrt{d}$ auszurechnen.

3.3 Approximation reeller Zahlen durch rationale

Konvention Sei $\alpha = [a_0; a_1, \dots, a_k, \dots]$. Ist $\alpha \in \mathbb{Q}$, so sei a_k das letzte von 0 verschiedene Element der Darstellung. Ist dabei $k \geq 1$, so setzen wir weiter $a_k \neq 1$ voraus (damit besitzt jedes $\alpha \in \mathbb{R}$ eine eindeutige Darstellung solcher Form).

Es gilt $\left|\alpha - \frac{p_i}{q_i}\right| \leq \frac{1}{q_i q_{i+1}}$ (Bem. v. Satz 3.6) (falls $i \leq k-1$).

Wir betrachten nun Näherungen reeller Zahlen durch rationale; dabei messen wir die Annäherung von α durch $\frac{a}{b}$ nicht durch $\left|\alpha - \frac{a}{b}\right|$ sondern durch $|b\alpha - a|$ (das ergibt später glattere Resultate)

Lemma 3.13

(i) Ist $\alpha \in \mathbb{Q}$, so gilt für alle $c \in \mathbb{Z}$, $d \in \mathbb{N}$ $|q_k \alpha - p_k| \leq |d\alpha - c|$ mit „$=$" $\Leftrightarrow \frac{c}{d} = \frac{p_k}{q_k}$ $(= \alpha)$

(ii) Sei $\alpha \in \mathbb{Q}$ und $q_k > 1$. Dann gilt für alle $c \in \mathbb{Z}$, $d \in \mathbb{N}$ mit $d < q_k$:

$$|q_{k-1}\alpha - p_{k-1}| \leq |d\alpha - c|$$

mit Gleichheit genau dann, wenn $(c,d) = (p_{k-1}, q_{k-1})$ oder $(c,d) = (p_k - p_{k-1}, q_k - q_{k-1})$

(iii) Ist ($\alpha \in \mathbb{Q}$, $0 \leq i \leq k-2$, oder $\alpha \in \mathbb{R}\setminus\mathbb{Q}$, $i \geq 0$), aber nicht gleichzeitig $i=0$ und $a_1 = 1$, so gilt für alle $c \in \mathbb{Z}$, $d \in \mathbb{N}$ mit $d < q_{i+1}$:

$$|q_i \alpha - p_i| \leq |d\alpha - c|$$

mit Gleichheit genau für $(c,d) = (p_i, q_i)$.

Bem: •) in (ii) ist $k \geq 1$ und $q_k = a_k q_{k-1} + q_{k-2} \geq 2q_{k-1}$.

Für beide möglichen (c,d) gilt also $0 < d < q_k$.

(Gleichheit wegen $q_k \alpha = p_k$)

•) zu (iii): im ersten Unterfall (i∈ℕ) gilt $k \geq 2$.

Stets: $q_i \leq q_{i+1}$ mit "$=$" $\Leftrightarrow$ $(a_{i+1} - 1) q_i + q_{i-1} = 0$

$\Leftrightarrow$ $i = 0 \wedge a_1 = 1$,

was ausgeschlossen wurde

Also gilt in (iii): $q_i < q_{i+1}$.

Beweis: (i) trivial

(ii)+(iii) Bei (ii) setze $i := k-1$

Betrachte LGS

$$\begin{cases} p_i X + p_{i+1} Y = c \\ q_i X + q_{i+1} Y = d. \end{cases} \qquad (*)$$

Wegen $\det \begin{pmatrix} p_i & p_{i+1} \\ q_i & q_{i+1} \end{pmatrix} = (-1)^{i+1}$ (Lemma 3.3) ist $(*)$ in $\mathbb{Z}$ eindeutig lösbar.

Sei $(x,y) \in \mathbb{Z}^2$ die Lösung von $(*)$. ~~(bei (ii): i=k-1)~~

(ii) Sei $i = k-1$. Wäre $x = 0$, so wäre $q_k \mid d$ ↯ $d < q_k$. Also $x \neq 0$.

$(*) \Rightarrow d\alpha - c = (q_{k-1}\alpha - p_{k-1}) x + \underbrace{(q_k \alpha - p_k)}_{=0} y = (q_{k-1}\alpha - p_{k-1}) x$

Fall $|x| \geq 2$: $|d\alpha - c| > |q_{k-1}\alpha - p_{k-1}|$ ✓

Fall $|x| = 1$: $\Leftrightarrow c q_k - d p_k = \varepsilon$ mit $\varepsilon \in \{\pm 1\}$ (folgt aus $(*)$)

~~Wegen $q_k > 1$ ist $p_k > 0$.~~ Betrachte die lin. diophantische Glg.

$$C q_k - D p_k = \varepsilon \qquad (**)$$

Wegen $q_k > 1$ ist $p_k > 0$. Es gilt $(-1)^k p_{k-1} q_k - (-1)^k q_{k-1} p_k = 1$.

Die Lösungsmenge von $(**)$ ist deshalb

$$\{ (\varepsilon(-1)^k p_{k-1} + t p_k, \; \varepsilon(-1)^k q_{k-1} + t q_k) : t \in \mathbb{Z} \}$$

(vgl. Elementare Zahlentheorie)

Also: $|d\alpha - c| = |q_{k-1}\alpha - p_{k-1}|$

$\Leftrightarrow (c,d) = (\varepsilon' p_{k-1} + t p_k,\ \varepsilon' q_{k-1} + t q_k)$ mit $\varepsilon' \in \{\pm 1\}$, $t \in \mathbb{Z}$, so dass $0 < d < q_k$

$0 < d < q_k \Leftrightarrow (\varepsilon' = 1 \text{ und } t = 0)$ oder $(\varepsilon' = -1 \text{ und } t = 1)$

Also: $(c,d) \in \{(p_{k-1}, q_{k-1}),\ (p_k - p_{k-1},\ q_k - q_{k-1})\}$.

(iii) Ist $y = 0$, ist $\frac{c}{d} = \frac{p_i x}{q_i x} = \frac{p_i}{q_i}$ (wegen $i \geq 1$ oder $a_i \geq 1$)

$x = 0$ ist nicht möglich, da $q_{i+1} \geq q_i > d$, im Widerspruch zu $q_{i+1} \mid d$ steht.

Seien $x, y \neq 0$. Wegen $q_{i+1} > d$ muss $xy < 0$ gelten.

$|\alpha q_i - p_i|$ und $|\alpha q_{i+1} - p_{i+1}|$ haben verschiedene Vorzeichen, denn entweder $\frac{p_i}{q_i} < \alpha < \frac{p_{i+1}}{q_{i+1}}$ oder $\frac{p_{i+1}}{q_{i+1}} < \alpha < \frac{p_i}{q_i}$ (falls $\alpha \in \mathbb{Q}$, gilt die strikte Ugl. wegen $i \leq k-2$).

$\Rightarrow x(q_i\alpha - p_i)$, $y(q_{i+1}\alpha - p_{i+1})$ haben gleiches Vorzeichen

$\Rightarrow |d\alpha - c| \overset{(*)}{=} |q_i x\alpha + q_{i+1} y\alpha - p_i x - p_{i+1} y|$

$= |x(q_i\alpha - p_i) + y(q_{i+1}\alpha - p_{i+1})| \overset{\text{Vorzeichen!}}{=} \underbrace{|x|}_{\geq 1} |q_i\alpha - p_i| + \underbrace{|y|}_{\geq 1} \underbrace{|q_{i+1}\alpha - p_{i+1}|}_{> 0}$

$> |q_i\alpha - p_i|$. □

Def 3.14 $\frac{a}{b}$ mit $a \in \mathbb{Z}$, $b \in \mathbb{N}$ heißt beste Näherung für $\alpha \in \mathbb{R}$, wenn für alle $c \in \mathbb{Z}$, $b \in \mathbb{N}$ mit $\frac{c}{d} \neq \frac{a}{b}$ und $\boxed{d \leq b}$ gilt:

$|d\alpha - c| > |b\alpha - a|$

Satz 3.15 Jede beste Näherung von α ist ein Näherungsbruch von α.

Beweis: Sei $\frac{a}{b} \neq \frac{p_0}{q_0}, \dots, \frac{p_k}{q_k}, \dots$. zz: $\frac{a}{b}$ ist keine beste Näherung für α.

Fall 1: $\alpha \in \mathbb{Q}$, $b \geq q_k$: Wähle $c = p_k$, $d = q_k$ $\rightarrow$ $0 = |q_k\alpha - p_k| = |d\alpha - c| < |b\alpha - a|$

Fall 2: $\alpha \in \mathbb{R}\setminus\mathbb{Q}$ oder $\alpha \in \mathbb{Q}$ und $b < q_k$:

$1 = q_0 \leq q_1 < \dots < q_k < \dots \Rightarrow \exists!\, i$ mit $q_i \leq b < q_{i+1}$. (Falls $a_1 = 1$)

Ist $\alpha \in \mathbb{Q}$, so gilt $i < k$.

$1 < q_{i+1} = a_{i+1}q_i + q_{i-1} \Rightarrow$ entweder $i \geq 1$ oder ($i = 0$ und $a_1 > 1$).

$\overset{\text{Lemma 3.13 (ii)+(iii)}}{\Longrightarrow}$ $|q_i\alpha - p_i| \leq |b\alpha - a|$

Wegen $\frac{a}{b} \neq \frac{p_i}{q_i}$ ist $\frac{a}{b}$ keine beste Näherung. □

Satz 3.16 Jeder Näherungsbruch von $\alpha \in \mathbb{R}$ ist eine beste Näherung für α, außer $\frac{p_0}{q_0}$ für α der Form $[a_0; 2]$, $[a_0; 1, a_1, \dots, a_k]$ $(k \geq 2)$, bzw. $[a_0; 1, a_2 \dots]$.

(In den Ausnahmefällen ist $\frac{p_0}{q_0}$ keine beste Näherung)

Beweis: Sei $\frac{p_i}{q_i}$ ein Näherungsbruch, mit $i \geq 1$ in den Ausnahmefällen.

zz: $\forall c \in \mathbb{Z}, d \in \mathbb{N}$: $\frac{c}{d} \neq \frac{p_i}{q_i}$, $d \leq q_i \Rightarrow |q_i\alpha - p_i| < |d\alpha - c|$

Fall $\alpha \in \mathbb{Q}$: (i) $i = k$ ✓ nach Lemma 3.13(i)

(ii) $i = k-1$: wegen $\alpha \neq [a_0; 2]$ ist $k > 1$ oder $a_k > 2$,

$a_k > 2 \Rightarrow q_k = a_k q_{k-1} + q_{k-2} > 2q_{k-1} \Rightarrow q_k - q_{k-1} > q_{k-1}$

$k > 1 \Rightarrow a_k \geq 2 \Rightarrow q_k \geq 2q_{k-1} \Rightarrow q_k - q_{k-1} \geq q_{k-1}$

D.h. nach Lemma 3.13(ii) ist $|q_i\alpha - p_i| < |d\alpha - c|$

(iii) $0 \leq i \leq k-2$: nach Lemma 3.13(iii)

Fall $\alpha \notin \mathbb{Q}$ nach Lemma 3.13 (iii)

Ausnahmefälle:

- $\alpha = a_0 + \frac{1}{2}$: $(p_0, q_0) = (a_0, 1)$, $(p_1, q_1) = (2a_0+1, 2)$, also $\frac{p_0}{q_0} = a_0$, $\frac{p_1}{q_1} = a_0 + \frac{1}{2}$

  $\Rightarrow |q_0\alpha - p_0| = \frac{1}{2}$ aber auch $|1\cdot\alpha - (a_0+1)| = |-\frac{1}{2}| = \frac{1}{2}$.

- $\alpha = [a_0; 1, a_2, \dots, a_k, \dots]$, $k \geq 2$

  $\alpha - a_0 \geq \frac{p_2}{q_2} - a_0 = \frac{1}{1+\frac{1}{a_2}} \geq \frac{1}{2}$ falls $k \geq 3$ oder $\alpha \notin \mathbb{Q}$

  $\alpha - a_0 = \frac{p_2}{q_2} - a_0 = \frac{1}{1+\frac{1}{a_2}} \geq \frac{2}{3} > \frac{1}{2}$ falls $k = 2$ $(\Rightarrow a_2 \geq 2)$

$\Rightarrow \alpha - a_0 > \frac{1}{2}$

$\Rightarrow \frac{a_0}{1}$ ist keine beste Näherung ($\frac{a_0+1}{1}$ ist besser) $\square$

Bem: (1) Ist $\frac{a}{b}$ beste Näherung von α und $\frac{c}{d}$ mit $1 \leq d < b$,

so ist $|\alpha - \frac{a}{b}| < \frac{d}{b}|\alpha - \frac{c}{d}| < |\alpha - \frac{c}{d}|$

(2) $\frac{a}{b}$ $(b \in \mathbb{N})$ ist eine gute Näherung für α, wenn gilt

$$|\alpha - \frac{a}{b}| = \min\{|\alpha - \frac{c}{d}| : c \in \mathbb{Z}, d \in \mathbb{N}, d \leq b\}$$

Jede gute Näherung ist entweder ein Näherungsbruch von α oder ein Nebennäherungsbruch, d.h. von der Form

$$\frac{p_{i,r}}{q_{i,r}} := \frac{r p_{i+1} + p_i}{r q_{i+1} + q_i}, \quad 1 \leq r < a_{i+2} - 1.$$

(siehe z.B. Dujella, Number Theory, Theorem 8.31)

Aber nicht jeder Nebennäherungsbruch ist eine gute Approximation!

3.4 Kettenbruchentwicklung der eulerschen Zahl

Wir zeigen: $e = [2; 1,2,1, 1,4,1, 1,6,1, 1,8,1, \dots]$

MB: $\frac{2}{1}, \frac{3}{1}, \frac{8}{3}, \frac{11}{4}, \frac{19}{7}, \frac{87}{32}, \dots$

Zuerst:

Lemma 3.17 Für $k \in \mathbb{N}$ ist $\frac{e^{\frac{2}{k}}+1}{e^{\frac{2}{k}}-1} = [k; 3k, 5k, 7k, 9k, \dots]$

(Bundschuh, Einf. id. Z., §3.11)

Beweis: Für $n \in \mathbb{N}_0$ seien

$$\xi_n \overset{(1)}{:=} \frac{1}{n!}\int_0^1 x^n(1-x)^n e^{\frac{2x}{k}}\,dx \quad \text{und} \quad \eta_n \overset{(2)}{:=} \frac{1}{n!}\int_0^1 x^{n+1}(1-x)^n e^{\frac{2x}{k}}\,dx$$

Für $n \geq 1$ gilt:

$$(1) \Rightarrow \xi_n = \frac{1}{n!}\left[e^{\frac{2x}{k}} \cdot \frac{k}{2} \cdot x^n(1-x)^n \Big|_0^1 - \int_0^1 \frac{k}{2} e^{\frac{2x}{k}} \left[n x^{n-1}(1-x)^n - n x^n (1-x)^{n-1} \right] \right]$$

$$= -\frac{k}{2n!}\int_0^1 e^{\frac{2x}{k}} \left[n \underbrace{[(1-x)-x]}_{1-2x} \left(x^{n-1}(1-x)^{n-1} \right) \right]$$

$$= \frac{k}{2(n-1)!}\int_0^1 e^{\frac{2x}{k}} (2x-1)\, x^{n-1}(1-x)^{n-1}$$

$$\Rightarrow \frac{2}{k}\xi_n = 2\eta_{n-1} - \xi_{n-1}$$

$$\Rightarrow \boxed{\frac{2}{k}\xi_n + \xi_{n-1} = 2\eta_{n-1}} \quad (3)$$

$$(2) \Rightarrow \eta_n = \frac{1}{n!}(-1)\int_0^1 \frac{k}{2} e^{\frac{2x}{k}} \left[(n+1) x^n (1-x)^n - n x^{n+1}(1-x)^{n-1} \right] dx$$

$$= \frac{1}{n!}\int_0^1 \frac{k}{2} e^{\frac{2x}{k}} \left[\underbrace{\left(n x - (n+1)(1-x) \right)}_{\substack{\| \\ n(x-1)+n \\ = n - (2n+1)(1-x)}} \left(x^n (1-x)^{n-1} \right) \right] dx$$

$$= \frac{k}{2}\eta_{n-1} - (2n+1)\frac{k}{2}\xi_n$$

$$\Rightarrow \boxed{(2n+1)\xi_n = \eta_{n-1} - \frac{2}{k}\eta_n} \quad (4)$$

(3) in (4) einsetzen um η_n, η_{n-1} zu eliminieren:

$$(2n+1)\xi_n = \frac{\xi_n}{k} + \frac{\xi_{n-1}}{2} - \frac{1}{k}\left(\frac{2}{k}\xi_{n+1} + \xi_n\right)$$

$$\Rightarrow \boxed{(2n+1)k\,\xi_n = \frac{k\xi_{n-1}}{2} - \frac{2}{k}\xi_{n+1}} \qquad (n \geq 1)$$

$$\Leftrightarrow \boxed{\frac{k}{2}\frac{\xi_{n-1}}{\xi_n} = (2n+1)k + \frac{2\xi_{n+1}}{k\xi_n}} \quad (5)$$

und $\xi_0 = \frac{k}{2}\left(e^{\frac{2}{k}} - 1\right)$, $\eta_0 = \frac{k}{2}e^{\frac{2}{k}} - \left(\frac{k}{2}\right)^2\left(e^{\frac{2}{k}} - 1\right)$

$\overset{(3)}{\Longrightarrow}$ $\xi_1 = \left(\frac{k}{2}\right)^2\left(e^{\frac{2}{k}} + 1 - k\left(e^{\frac{2}{k}} - 1\right)\right)$

$$\frac{\xi_1}{\xi_0} = \left(\frac{k}{2}\right)\left(\frac{e^{\frac{2}{k}}+1}{e^{\frac{2}{k}}-1} - k\right) \Rightarrow \frac{e^{\frac{2}{k}}+1}{e^{\frac{2}{k}}-1} = k + \frac{2}{k}\frac{\xi_1}{\xi_0} = \left[k; \frac{k\xi_0}{2\xi_1}\right] =$$

$$\overset{(5),n=1}{\ldots} = \left[k; 3k; \frac{k\xi_n}{2\xi_{n+1}}\right] \overset{(5),\text{Induktion}}{=} [k; 5k, 7k, \ldots] \qquad \square$$

Korollar/Bem $e^{\frac{2}{k}}$ ist für kein $k \in \mathbb{Z}\setminus\{0\}$ algebraisch vom Grad höchstens 2.

($k>0$: $z := e^{\frac{2}{k}}$, $y := \frac{z+1}{z-1} \Rightarrow z = \frac{y+1}{y-1}$ …,

$k<0$: $1 = e^{\frac{2}{k}}e^{-\frac{2}{k}}$)

(Folgen nun Rockett, Szüsz, Continued Fractions, World Scientific Publishing, 1992.)

Insbesondere: $\frac{e+1}{e-1} \overset{k=2}{=} [2; 6; 10; 14; \ldots] = [b_0; b_1, \ldots]$

mit $b_i = 2(2i+1)$

Die Näherungszähler/-nenner $\tilde{p}_n/\tilde{q}_n$ erfüllen: $(n \geq 0)$

$$\tilde{p}_n = 2(2n+1)\tilde{p}_{n-1} + \tilde{p}_{n-2},$$

$$\tilde{q}_n = 2(2n+1)\tilde{q}_{n-1} + \tilde{q}_{n-2}.$$

Satz 3.18: $e = [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, \dots]$

(d.h. $a_0 = 2$, $a_1 = 1$, $a_{3i-1} = 2i$, $a_{3i} = a_{3i+1} = 1$ für $i > 0$)

Beweis: Sei $z = [2; 1, 2, 1, 1, 4, 1, \dots] = [a_0, a_1, \dots]$ zz. $z = e$.

Seien p_i, q_i die Z.Z. / N.N. von z. Für $i \geq 2$:

$$\Rightarrow p_{3i+1} = p_{3i} + p_{3i-1} = (p_{3i-1} + p_{3i-2}) + p_{3i-1} = 2p_{3i-1} + p_{3i-2}$$

$$= 2(2i\, p_{3i-2} + p_{3(i-1)}) + p_{3i-2} = (2(2i)+1)\, p_{3i-2} + 2p_{3i-3}$$

$$= (2(2i)+1)\, p_{3i-2} + \underbrace{p_{3i-3} + (p_{3i-4} + p_{3i-5})}_{= p_{3i-2}}$$

$$= 2(2i)+1)\, p_{3i-2} + p_{3i-5} = 2(2i+1)\, p_{3(i-1)+1} + p_{3(i-2)+1}$$

analog: $q_{3i+1} = 2(2i+1)\, q_{3(i-1)+1} + q_{3(i-2)+1}$ $(i \geq 2)$

D.h. p_{3i+1}, q_{3i+1} erfüllen gleiche Rekursionsvorschrift wie $\tilde{p}_i, \tilde{q}_i$, mit anderen Startwerten. $\frac{2}{1}, \frac{3}{1}, \frac{8}{3}, \frac{11}{4}, \frac{19}{7}, \frac{87}{32}, \dots$

$p_1 = 3$, $q_1 = 1$ $\qquad$ $\tilde{p}_0 = 2$ $\qquad$ $\tilde{q}_0 = 1$

$p_4 = 19$, $q_4 = 7$ $\qquad$ $\tilde{p}_1 = 13$ $\qquad$ $\tilde{q}_1 = 6$

$\Rightarrow$ $p_1 = \tilde{p}_0 + \tilde{q}_0$, $p_4 = \tilde{p}_1 + \tilde{q}_1$ $\overset{\text{Induktion}}{\Longrightarrow}$ $p_{3i+1} = \tilde{p}_i + \tilde{q}_i$ $\quad \forall i \geq 0$

$q_1 = \tilde{p}_0 - \tilde{q}_0$, $q_4 = \tilde{p}_1 - \tilde{q}_1$ $\Rightarrow$ $q_{3i+1} = \tilde{p}_i - \tilde{q}_i$ $\quad \forall i \geq 0$

$$\Rightarrow z = \lim_{i\to\infty} \frac{p_{3i+1}}{q_{3i+1}} = \lim_{i\to\infty} \frac{\tilde{p}_i + \tilde{q}_i}{\tilde{p}_i - \tilde{q}_i} = \lim_{i\to\infty} \frac{\tilde{p}_i/\tilde{q}_i + 1}{\tilde{p}_i/\tilde{q}_i - 1} = \frac{\left(\frac{e+1}{e-1}\right)+1}{\left(\frac{e+1}{e-1}\right)-1}$$

$$= \frac{(e+1)+(e-1)}{(e+1)-(e-1)} = \frac{2e}{2} = e.$$

□