Beispiel 40

Behauptung: $n! \in O(n^n)$

Beweis:

$$(\forall n \in \mathbb{N})\big[n! = n(n-1)\cdots 2 \cdot 1 \leq 1 \cdot n^n\ \big]$$

□

Beispiel 41

Behauptung: $\log n! \in O(n \log n)$

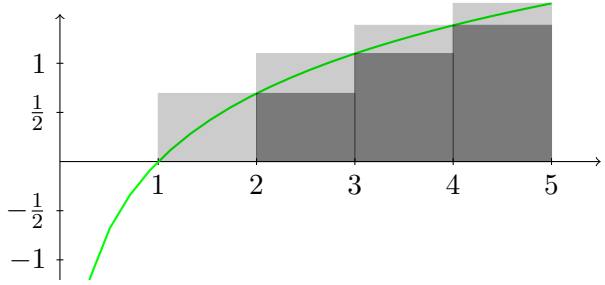
Beweis:
$(\forall n \in \mathbb{N})\big[\log n! = \log n + \log(n-1) + \ldots + \log 1 < 1 \cdot n \cdot \log n\big]$ □

Beispiel 42

Behauptung: $n! = O\left((n+1) \cdot e \cdot \left(\frac{n}{e}\right)^n\right)$

Beweis:

$$(\forall n > 0)\left[\sum_{k=1}^{n-1} \ln k < \int_1^n \ln x \; dx < \sum_{k=2}^{n} \ln k < \int_1^{n+1} \ln x \; dx\right]$$



□

Es ist

$$\int_1^n \ln x \; dx = \big(x \cdot \ln x - x\big)\Big|_1^n = n \cdot \ln n - n + 1$$

und

$$\int_1^{n+1} \ln x \; dx = (n+1) \cdot \ln(n+1) - n$$

Also:

$$\big(\forall n \in \mathbb{N}\big)\left[n \cdot \ln n - n + 1 < \ln n! < (n+1) \cdot \ln(n+1) - n\right]$$

und damit

$$\frac{n^n}{e^{n-1}} \leq n! \leq \frac{(n+1)^{n+1}}{e^n}$$

oder:

$$e \cdot \left(\frac{n}{e}\right)^n \leq n! \leq (n+1) \cdot \left(\frac{n}{e}\right)^n \cdot \left(1 + \frac{1}{n}\right)^n \leq (n+1) \cdot e \cdot \left(\frac{n}{e}\right)^n$$

□

Die Stirling'sche Formel

$$\lim_{n\to\infty}\left(n!\Big/\left(\sqrt{n}\cdot\left(\frac{n}{e}\right)^n\right)\right)=\sqrt{2\pi}$$

oder mit anderen Worten:

$$n!=\sqrt{2\pi n}\cdot\left(\frac{n}{e}\right)^n\cdot(1+o(1))$$

Kapitel II Algebraische Grundlagen

1. Algebren

1.1 Grundbegriffe

Definition 43
Eine Algebra besteht aus einer Trägermenge S und einer Menge Φ von Operationen auf S (der Operatorenmenge). Dabei gilt: Jeder Operator ist eine (totale) Abbildung

$$S^m \to S$$

der Stelligkeit (Arität, arity) $m \in \mathbb{N}_0$.

- Nullstellige Operatoren sind Konstanten, z. B. 0, 47, $\bot$.
- Einstellige Operatoren sind unäre Operatoren, z. B. $x \mapsto 2^x$, $x \mapsto \neg x$, $A \mapsto 2^A$.
- Zweistellige Operatoren sind binäre Operatoren, z. B. $(x, y) \mapsto \max\{x, y\}$, $(x, y) \mapsto \mathrm{ggT}(x, y)$, $(x, y) \mapsto x + y$.
- Dreistellige Operatoren sind ternäre Operatoren, z. B. $(x, y, z) \mapsto$ **if** x **then** y **else** z **fi**

Beispiel 44

Sei U eine Menge, F die Menge der Funktionen von $U \to U$. $(F, \circ)$ ist eine Algebra mit $\circ$ als Komposition von Funktionen.

Beispiel 45

Boolesche Algebra:
$\langle \{t, f\}, \{t, f, \neg, \wedge, \vee\} \rangle$ ist eine (endliche) Algebra.

1.2 Eigenschaften

Signatur einer Algebra

Definition 46

Die Signatur einer Algebra besteht aus der Liste der Stelligkeiten der Operatoren.

Beispiel 47

$\langle \mathbb{B}, \{t, f, \neg, \wedge, \vee\} \rangle$ (Boolesche Algebra, $\mathbb{B} = \{t, f\}$): 0, 0, 1, 2, 2

$$\begin{array}{lcrcl} \neg & : & \mathbb{B} & \to & \mathbb{B} \\ \wedge & : & \mathbb{B} \times \mathbb{B} & \to & \mathbb{B} \\ \vee & : & \mathbb{B} \times \mathbb{B} & \to & \mathbb{B} \end{array}$$

Beispiel 48

$\langle 2^U, \{U, \emptyset, \bar{}, \cap, \cup\} \rangle$: 0, 0, 1, 2, 2

$$\begin{array}{lcrcl} \bar{} & : & 2^U & \to & 2^U \\ \cap & : & 2^U \times 2^U & \to & 2^U \\ \cup & : & 2^U \times 2^U & \to & 2^U \end{array}$$

Diese beiden Algebren haben dieselbe Signatur; die Trägermenge ist unwesentlich, es kommt nur auf die Reihenfolge der Stelligkeiten an.

Einselement, Nullelement, Inverses

Sei $\langle S, \circ \rangle$ eine Algebra, $\circ$ beliebiger zweistelliger Operator.

Definition 49

- Ein Element $1 \in S$ heißt linkes (bzw. rechtes) Einselement für den Operator $\circ$, falls

$$(\forall a \in S) \quad 1 \circ a = a \text{ (bzw. } a \circ 1 = a)$$

  1 heißt Einselement, falls es linkes und rechtes Einselement ist.
- Ein Element $0 \in S$ heißt linkes (bzw. rechtes) Nullelement für den Operator $\circ$, falls

$$(\forall a \in S) \quad 0 \circ a = 0 \text{ (bzw. } a \circ 0 = 0)$$

  0 heißt Nullelement, falls es linkes und rechtes Nullelement ist.
- Sei 1 Einselement. Für $a \in S$ heißt $a^{-1} \in S$ Rechtsinverses von a, falls

$$a \circ a^{-1} = 1$$

  Analog: Linksinverses

Beispiel 50

Betrachte $F(U)$, d. h. die Menge aller Abbildungen $U \to U$. Dann gilt (mit der Komposition als Operator):

- $f \in F(U)$ hat genau dann ein Rechtsinverses, wenn f surjektiv ist.

  $$f \circ f^{-1} = id$$

  (Wähle für f^{-1} irgendeine Funktion g, so dass gilt: $g(x)$ wird von f auf x abgebildet.)
- $f \in F(U)$ hat genau dann ein Linksinverses, wenn f injektiv ist.

  $$f^{-1} \circ f = id$$

  (Wähle für f^{-1} irgendeine Funktion g, so dass gilt: $f(x)$ wird von g auf x abgebildet.)

Ist f bijektiv, dann stimmen die beiden f^{-1} aus (1) und (2) überein.

Satz 51

Falls c linkes Einselement ist und d rechtes Einselement (bezüglich des binären Operators $\circ$), dann ist

$$c = d\,.$$

Beweis:

$$d = c \circ d = c\,.$$

□

Satz 52

Falls c linkes Nullelement und d rechtes Nullelement (bezüglich $\circ$) ist, dann ist

$$c = d\,.$$

Beweis:

$$c = c \circ d = d\,.$$

□

Beispiel 53

Betrachte $\langle \{b, c\}, \{\bullet\} \rangle$ mit

$\bullet$	b	c
b	b	b
c	c	c

Es gilt: b und c sind linke Nullelemente, und b und c sind rechte Einselemente.

Abgeschlossenheit

Definition 54

Sei $\langle S, \Phi \rangle$ eine Algebra, T eine Teilmenge von S.

- T ist unter den Operatoren in Φ abgeschlossen (stabil), falls ihre Anwendung auf Elemente aus T wieder Elemente aus T ergibt.
- $\langle T, \Phi \rangle$ heißt Unteralgebra von $\langle S, \Phi \rangle$, falls $T \neq \emptyset$ und T unter den Operatoren $\in \Phi$ abgeschlossen ist.

Beispiel 55

- $\langle \mathbb{N}_0, + \rangle$ ist Unteralgebra von $\langle \mathbb{Z}, + \rangle$
- $\langle \{0, 1\}, \cdot \rangle$ ist Unteralgebra von $\langle \mathbb{N}_0, \cdot \rangle$
- $\langle \{0, 1\}, + \rangle$ ist keine Unteralgebra von $\langle \mathbb{Z}, + \rangle$, da sie nicht abgeschlossen ist $(1 + 1 = 2)$.

2. Morphismen

Seien $A = \langle S, \Phi \rangle$ und $\tilde{A} = \langle \tilde{S}, \tilde{\Phi} \rangle$ zwei Algebren mit derselben Signatur.

2.1 Isomorphismus

Definition 56
Eine Abbildung

$$h : S \to \tilde{S}$$

heißt ein Isomorphismus von A nach $\tilde{A}$, falls

- h bijektiv ist und
- h mit den in Φ und $\tilde{\Phi}$ einander entsprechenden Operatoren vertauschbar ist (kommutatives Diagramm):

$$\begin{array}{ccc} S^m & \xrightarrow{\circ} & S \\ {\scriptstyle (h,\ldots,h)}\downarrow & & \downarrow{\scriptstyle h} \\ \tilde{S}^m & \xrightarrow{\tilde{\circ}} & \tilde{S} \end{array}$$

h ist also ein Isomorphismus gdw

- $h(c) = \tilde{c}$ für alle nullstelligen Operatoren (Konstanten) c
- $h\big(u(x)\big) = \tilde{u}\big(h(x)\big)$ für alle unären Operatoren $u \in \Phi$, $\forall x \in S$
- $h\big(b(x,y)\big) = \tilde{b}\big(h(x), h(y)\big)$ für alle binären Operatoren $b \in \Phi$, $\forall x, y \in S$

Notation: $A \cong \tilde{A}$: „A isomorph zu $\tilde{A}$“, d. h. es existiert ein Isomorphismus von A nach $\tilde{A}$ (und von $\tilde{A}$ nach A).

Ein Isomorphismus von A nach A heißt Automorphismus.

Zur Vereinfachung der Notation schreiben wir statt $\langle S, \{o_1, \ldots, o_k\}\rangle$ auch

$$\langle S, o_1, \ldots, o_k\rangle \ ,$$

solange keine Verwechslung zu befürchten ist.

Beispiel 57

$\langle \mathbb{N}_0, + \rangle$ und $\langle 2 \cdot \mathbb{N}_0, + \rangle$ ($2 \cdot \mathbb{N}_0$: gerade Zahlen) mit

$$h : \mathbb{N}_0 \ni n \mapsto 2 \cdot n \in 2\mathbb{N}_0$$

ist ein Isomorphismus zwischen den beiden Algebren.

Beispiel 58

$\langle \mathbb{R}^+, \cdot \rangle$ und $\langle \mathbb{R}, + \rangle$ $\left(\mathbb{R}^+ = \{x \in \mathbb{R}; x > 0\}\right)$

$$h : \mathbb{R}^+ \ni x \mapsto \log x \in \mathbb{R}$$

ist ein Isomorphismus (der sog. Rechenschieberisomorphismus)

Satz 59

Ein Algebra-Isomorphismus bildet Einselemente auf Einselemente, Nullelemente auf Nullelemente und Inverse auf Inverse ab.

Beweis:

Sei die Abbildung $h : S \to \tilde{S}$ ein Isomorphismus von $A = \langle S, \Phi \rangle$ nach $\tilde{A} = \langle \tilde{S}, \tilde{\Phi} \rangle$.
Sei 1 ein rechtes Einselement für den Operator $\circ \in \Phi$ in A. Dann gilt für alle $\tilde{b} \in \tilde{S}$:

$$\tilde{b} \tilde{\circ} h(1) = h(b) \tilde{\circ} h(1) = h(b \circ 1) = h(b) = \tilde{b}$$

Also ist $h(1)$ ein rechtes Einselement in $\tilde{A}$. Die Argumentation für linke Einselemente, Nullelemente und Inverse ist analog. □

2.2 Homomorphismus

Definition 60
Eine Abbildung

$$h\colon S \to \tilde{S}$$

heißt ein Homomorphismus von A nach $\tilde{A}$, falls h mit den in Φ und $\tilde{\Phi}$ einander entsprechenden Operatoren vertauschbar ist.

Beispiel 61

$\langle \mathbb{N}_0, + \rangle$ und $\tilde{A} = \langle \mathbb{Z}_m, +_{(m)} \rangle$ mit $+_{(m)}$ als Addition modulo m.

$$h \colon \mathbb{N}_0 \ni n \mapsto n \bmod m \in \mathbb{Z}_m$$

ist ein (surjektiver) Homomorphismus ($\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$).

Beispiel 62

$\langle \Sigma^*, \circ \rangle$ und $\langle \mathbb{N}_0, + \rangle$ mit Σ^* Menge der endlichen Zeichenreihen über dem Alphabet Σ.

$$h \colon \Sigma^* \ni \sigma \mapsto |\sigma| \in \mathbb{N}_0$$

mit $|\sigma|$ der Länge der Zeichenreihe ist ein Homomorphismus.

Satz 63

Sei h ein Homomorphismus von $A = \langle S, \Phi \rangle$ nach $\tilde{A} = \langle \tilde{S}, \tilde{\Phi} \rangle$. Dann ist $\langle h(S), \tilde{\Phi} \rangle$ eine Unteralgebra von $\tilde{A}$.

Beweis:

Offensichtlich. □

3. Halbgruppen

Definition 64

Eine Halbgruppe ist eine Algebra $\langle S, \circ \rangle$ mit einem assoziativen binären Operator $\circ$, d. h. für alle $a, b, c \in S$ gilt:

$$(a \circ b) \circ c = a \circ (b \circ c)$$

Beispiel 65

$\langle \Sigma^*, \circ \rangle$: Menge der endlichen Zeichenreihen über dem Alphabet Σ, mit Konkatenation als $\circ$.

Beispiel 66

$S \subseteq \mathbb{R}$, $\langle S, \max \rangle$: Da die Maximumbildung assoziativ ist, ist $\langle S, \max \rangle$ eine Halbgruppe.

Beispiel 67

$\langle \{b, c\}, \circ \rangle$ mit

$\circ$	b	c
b	b	b
c	c	c

Auch diese Operation ist assoziativ.

Beweis:

$$
\begin{aligned}
c = c \circ (c \circ c) &= (c \circ c) \circ c = c \\
b = b \circ (c \circ c) &= (b \circ c) \circ c = b \\
c = c \circ (b \circ c) &= (c \circ b) \circ c = c \\
c = c \circ (c \circ b) &= (c \circ c) \circ b = c \\
b = b \circ (b \circ b) &= (b \circ b) \circ b = b \\
c = c \circ (b \circ b) &= (c \circ b) \circ b = c \\
b = b \circ (c \circ b) &= (b \circ c) \circ b = b \\
b = b \circ (b \circ c) &= (b \circ b) \circ c = b
\end{aligned}
$$

□

3.1 Unterhalbgruppen

Definition 68
Sei $\langle S, \circ \rangle$ eine Halbgruppe, $\emptyset \neq T \subseteq S$. $\langle T, \circ \rangle$ heißt Unterhalbgruppe, falls es eine Unteralgebra ist.

3.2 Abelsche Halbgruppen

Definition 69
Eine Halbgruppe $\langle S, \circ \rangle$ heißt abelsch, falls $\circ$ symmetrisch (kommutativ) ist. Also

$$a \circ b = b \circ a \quad \forall a, b \in S\,.$$

Abelsche (Halb-)Gruppen sind nach Nils H. Abel (1802–1829) benannt.

4. Monoide

Definition 70

Ein Monoid $\langle S, \circ, 1\rangle$ ist eine Halbgruppe $\langle S, \circ\rangle$ mit (linkem und rechtem) Einselement 1. Eine Algebra $\langle T, \circ\rangle$, $T \subseteq S$ heißt Untermonoid von $\langle S, \circ, 1\rangle$, wenn $\langle T, \circ\rangle$ eine Halbgruppe mit Einselement ist.

Beispiel 71

$\langle \mathbb{N}_0, \max\rangle$ ist ein Monoid mit 0 als Einselement, ein Untermonoid davon ist $\langle \{0, 1\}, \max\rangle$.

Beispiel 72

$\langle \Sigma^*, \circ\rangle$, mit $\circ$ Konkatenation von Zeichenreihen und der leeren Zeichenreihe ε als Einselement ist ein Monoid.