A - 8 Verbandstruktur und größter gemeinsamer Teiler

Definition A.79 (Verbandstruktur)

Eine partiell geordnete Menge $\mathcal{M}$ heisst **Verband**, wenn es zu jedem Paar $a, b \in \mathcal{M}$ eine **größte untere Schranke** $c = \inf(a, b)$ und **kleinste obere Schranke** $d = \sup(a, b)$ gibt, so daß für alle $c', d' \in \mathcal{M}$ gilt

$$(c \prec a \ \wedge \ c \prec b) \ \wedge \ (c' \prec a \ \wedge \ c' \prec b \Longrightarrow c' \prec c)$$

und

$$(d \succ a \ \wedge \ d \succ b) \ \wedge \ (d' \succ a \ \wedge \ d' \succ b \Longrightarrow d' \succ d)$$

In der Literatur wird oft abgekürzt:

$$a \wedge b = \inf(a, b) \quad \text{und} \quad a \vee b = \sup(a, b)$$

Wir werden wegen der Gefahr der Verwechslung mit logischen Operationen diese Schreibweise vermeiden.

Lemma A.80 (Rechenregeln in Verbänden)

(i) $\inf(a, a) = a \quad \wedge \quad \sup(a, a) = a$ **Idempotenz**

(ii) $\inf(b, a) = \inf(a, b) \quad \wedge \quad \sup(b, a) = \sup(a, b)$ **Kommutativität**

(iii) $\inf(a, \inf(b, c)) = \inf(\inf(a, b), c)$ **Assoziativität**
$\sup(a, \sup(b, c)) = \sup(\sup(a, b), c)$

(iv) $\inf(a, \sup(a, b)) = a \quad \wedge \quad \sup(a, \inf(a, b)) = a$ **Absorption**

(v) $a \preceq b \iff \inf(a, b) = a \iff \sup(a, b) = b$ **Konsistenz**

Beispiel A.81

$\mathcal{M} = \mathcal{P}(A) = \{B : B \subset A\}, \ |\mathcal{M}| = 2^A$ **Potenzmenge von A**

Für $B, C \in \mathcal{P}(A)$ gilt:

- $B \prec C \iff B \subset C$ **Inklusion**
- $\inf(B, C) = B \cap C$ **Schnittmenge**
- $\sup(B, C) = B \cup C$ **Vereinigung**

Beispiel A.82

$\mathcal{M} = \{0, 1\}$ mit Boolschen Verknüpfung $\begin{cases} \inf & = & \textit{Konjunktion} & \wedge \\ \sup & = & \textit{Disjunktion} & \vee \end{cases}$

inf	0	1
0	0	0
1	0	1

sup	0	1
0	0	1
1	1	1

Beispiel A.83
$\mathcal{M} = \mathbb{N}_+ = \mathbb{N} \setminus \{0\}$:

$$a \prec b \iff a|b$$

$$\begin{aligned} \inf(a,b) &= GGT(a,b) &&= \max\{c \in \mathbb{N} : c|a \wedge c|b\} \\ \sup(a,b) &= KGV(a,b) &&= \min\{c \in \mathbb{N} : a|c \wedge b|c\} \end{aligned}$$

Hierbei kann Maximieren bzw. Minimieren bezüglich der üblichen Größenordnung in $\mathbb{N}$ oder der Teilbarkeitsordnung vorgenommen werden.

Beobachtung:
Falls ein größter gemeinsame Teiler **GGT**$(\mathbf{a},\mathbf{b})$ zweier Zahlen $a, b \in \mathbb{N}_+$ tatsächlich existiert, erfüllt $c = GGT(a,b)$ für alle $c' \in \mathbb{Z}$

$$(c|a \wedge c|b) \quad \wedge \quad (c'|a \wedge c'|b \Longrightarrow c'|c)$$

und ist dann wegen der Antisymmetrie der Teilbarkeitsrelation eindeutig.

A - 9 Euklidescher Algorithmus und Anwendungen

Lemma A.85
(i) $0 < a \implies GGT(0,a) = a$
(ii) $0 < a < b \implies GGT(a,b) = GGT(b \bmod a, a)$

Euklidischer Algorithmus:
Input: $a, b \in \mathbb{N}_+$ mit $0 < a < b$
$r := b \bmod a$
`WHILE` $(0 \neq r)$
$b := a$
$a := r$
$r := b \bmod a$
Output: a

Lemma A.86 (Endlicher Abbruch)
Für alle Eingaben $a, b \in \mathbb{N}_+$ mit $a \leq b$ ergibt der Algorithmus nach endlichen vielen Durchläufen der `WHILE`-Schleife den $GGT(a,b)$ als Ergebnis.

Satz A.84 (Existenz des GGT)
Für $a, b \in \mathbb{N}_+$ gibt es $s, t \in \mathbb{Z}$, so daß

$$GGT(a,b) = s * a + t * b$$

Bemerkung:
Der obige Existenzsatz ist nicht konstruktiv, da er kein Verfahren angibt, das den GGT berechnet.
Dazu benutzt man **Euklid's Algorithmus**, welcher rekursiv das vorgegebene Berechnungsproblem auf ein "kleineres" Problem reduziert.

Frage:
Läßt sich die Zahl der Schritte a priori, d.h. durch die Größe von a und b, beschränken?

Lemma A.87
Die maximale Schrittzahl k erfüllt die Bedingung

$$(3/2)^k \leq a + b \qquad \textit{(initial)}$$

was äquivalent ist zu

$$k \leq \frac{1}{\lg_2(3/2)} \lg_2(a+b)$$

wobei $\frac{1}{\lg_2(3/2)} \approx 1.71$

Beispiel A.88
Für Beispiel $GGT(228,612) = 12$ gilt: $3 \leq k_{max} \leq 16.6$, was zeigt, dass die Schranke nicht sehr scharf (d.h. nicht sehr gut) ist.