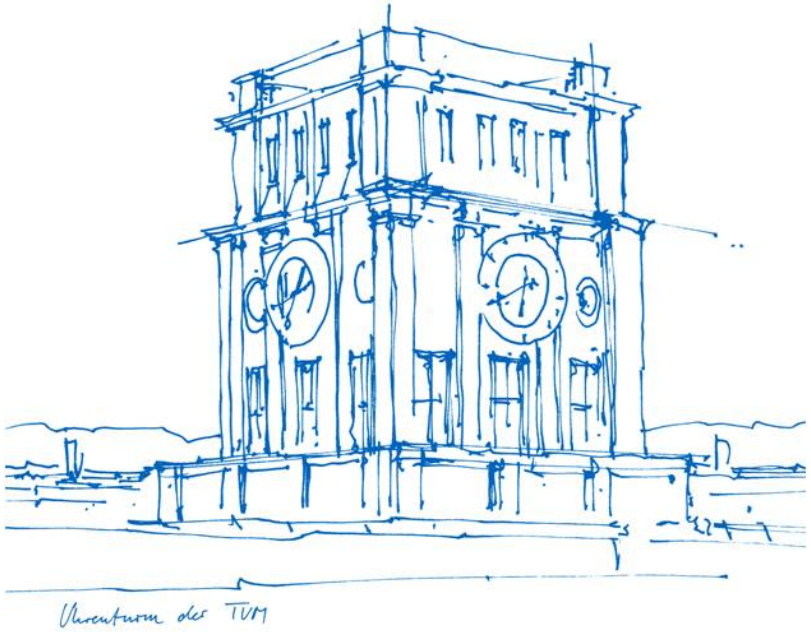
# Diskrete Strukturen – Tutorium KW 05

Jeremias Bohn

Technische Universität München

Fakultät für Informatik

Garching, 28. Januar 2019



# Hausaufgabenbesprechung

- 11.1b) und c)
  - Was ist hier der Unterschied?
- 11.1e)
  - Vorsicht, keine binomische Formel!
  - Vorfaktoren müssen auch beachtet werden!
- 11.2d) und e)
  - Hat keiner wirklich versucht…
  - Bitte für die Klausur Induktion üben!

# Algebraische Strukturen - Notation

- Eine algebraische Struktur $S$ ist ein Tupel bestehend aus Träger (Grundmenge) $U_S$ und Operatoren $I_S$, die ein Funktionssymbol $f$ mit Arität $ar(f)$ (Parameterzahl) interpretieren. Es gilt dann $I_S(f) \coloneqq U_S^{ar(f)} \to U_S$
- Wir schreiben dieses Tupel als $\left\langle U_S, {f_1}^{ar(f_1)}, \dots, {f_n}^{ar(f_n)} \right\rangle$

# Halbgruppe

$\langle A, \cdot^2 \rangle$ heißt Halbgruppe, wenn

- Assoziativität gilt

$\langle A, \cdot^2 \rangle$ heißt kommutative Halbgruppe, wenn

- zusätzlich Kommutativität gilt

$\langle A, \cdot^2, 1^0 \rangle$ heißt (kommutatives) Monoid, wenn

- $\langle A, \cdot^2 \rangle$ (kommutative) Halbgruppe ist
- 1 das neutrale Element zu $\cdot$ ist

$\langle A, \sqcap^2, \sqcup^2 \rangle$ heißt Verband, wenn

- $\langle A, \sqcap^2 \rangle$ und $\langle A, \sqcup^2 \rangle$ kommutative Habgruppen sind
- Absorption gilt (für alle $a, b \in A$: $a \sqcap (a \sqcup b) = a = a \sqcup (a \sqcap b)$)

# Gruppe

$\langle A, \cdot^2, 1^0 \rangle$ heißt (kommutative/abelsche) Gruppe, wenn

- $\langle A, \cdot^2, 1^0 \rangle$ (kommutatives) Monoid ist
- es zu jedem Element aus ein Inverses gibt (d.h. zu jedem $a \in A$ existiert ein $b \in A$: $a \cdot b = 1$

# Ring und Körper

$\langle A, +^2, \cdot^2, 0^0 \rangle$ oder $\langle A, +^2, \cdot^2, 0^0, 1^0 \rangle$ heißt (unitärer) Ring, wenn

- $\langle A, \cdot^2, 1^0 \rangle$ Monoid bzw. $\langle A, \cdot^2 \rangle$ Halbgruppe ist
- $\langle A, +^2, 0^0 \rangle$ kommutative Gruppe ist
- $\cdot$ distributiert $+$ über beide Seiten (Distributivgesetz)

$\langle A, +^2, \cdot^2, 0^0, 1^0 \rangle$ heißt Körper, wenn

- $\langle A, +^2, \cdot^2, 0^0, 1^0 \rangle$ unitärer Ring
- $\langle A \backslash \{0\}, \cdot^2, 1^0 \rangle$ kommutative Gruppe ist

# Erweiterter Euklidscher Algorithmus (EEA)

Berechnet zwei Zahlen $\alpha, \beta$, sodass $ggT(a,b) = \alpha \cdot a + \beta \cdot b$ gilt:

```
# Ass: 0 ≤ a ≤ b
def eea(a, b):
  if a == 0:
    # ggT(a,b) = ggT(0,b) = b = 0 • a + 1 • b
    return (0,1)

  # k = ⌊b/a⌋, r = b mod a = b − k • a
  k, r = divmod(b, a)

  # Test auf r = 0 prinzipiell unnoetig
  if r == 0:
    # ggT(a,b) = ggT(a, k • b) = a = 1 • a + 0 • b.
    return (1,0)

  # ggT(a,b) = ggT(b − k • a, a) = α' • (b − k • a) + β' • a
  α', β' = eea(r, a)

  # ggT(a,b) = (β' − k • α') • a + α' • b
  return (β' − k * α', α')
```