

---

# Diskrete Mathematik 2

FS 2013

# Contents

<b>1</b>	<b>1. Woche</b>	<b>1</b>
1.1	Semesterablauf(?) . . . . .	1
1.2	Quantifizierung . . . . .	1
1.3	Semantik . . . . .	3
<b>2</b>	<b>2. Woche</b>	<b>4</b>

# 1 1. Woche

## 1.1 Semesterablauf(?)

- Arithmetik in  $\mathbb{Z}$
- Modulares Rechnen
- Gruppen
- RSA
- Quantifizierung
- Induktion
  - Rekursion
  - Invarianten

- 
- Kein Laptop
  - Zwischenprüfung: 30.04.2013 (1 Stunde)
  - 5. März 2013 Unterricht nur bis 18:20

- 
- Bücher:
    - Gries/Schneider  
A logical approach to Discrete Math  
Springer, 1993
    - Jean Gallier  
Discrete Math  
Springer, 2010
    - Struckermann/Waetiger  
Mathematik fuer Informatiker  
Spektrum, 2007
- 

## 1.2 Quantifizierung

$$\mathbb{N} = \begin{cases} \{0, 1, 2, \dots\} (?) \\ \{1, 2, \dots\} (?) \end{cases}$$

$$\sum_{i=1}^n i^2 = 1^2 + 2^2 + \dots + n^2$$

$$\sum_{i=1}^{-1} i^2 = \begin{cases} \text{ungueltig (?) } \\ 1^2 \text{ (?) } \\ 1^2 + 0^2 + (-1)^2 \text{ (?) } \\ 0 \text{ (} \rightarrow ja, \text{ Neutrales Element) } \end{cases}$$

$$\sum_{i=1}^n i^2 + 1 = 1^2 + 2^2 + \dots + n^2 + 1 \text{ (?)}$$

$$\sum_{i=1}^n (i^2 + 1) = (1^2 + 1) + (2^2 + 1) + \dots + (n^2 + 1) \text{ (?)}$$

$$\sum_{\substack{i=1 \\ \text{odd}(i)}}^n i^2 = 1^2 + 3^2 + \dots + n^2 \text{ , falls odd}(n), \text{ sonst } (n-1)^2$$

$$\prod_{i=1}^n i^2 = 1^2 * 2^2 * \dots * n^2$$

$$\prod_{i=1}^{-1} i^2 = 1 \text{ (neutrales Element)}$$

(Java ==)

$$\forall_{i=0}^{n-1} (b[i] == 0) = (b[0] == 0) \wedge (b[1] == 0) \wedge \dots \wedge (b[n-1] == 0)$$

$$\exists_{i=0}^{n-1} (b[i] == 0) = (b[0] == 0) \vee (b[1] == 0) \vee \dots \vee (b[n-1] == 0)$$

$$\sum_{i=1}^n i^2 = (\sum i : \mathbb{N} \mid 1 \leq i \leq n : i^2)$$

$$(\sum i : \mathbb{N}, j : \mathbb{N} \mid 1 \leq i \leq 2 \wedge 1 \leq j \leq 3 : i^j)$$

$$(\circ v_1 : T_1, \dots, v_n : T_n \mid R : P)$$

$$- \circ : T \times T \rightarrow T \text{ (wobei T ein Typ ist)}$$

$$\text{Bsp: } + : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$$

$$+(3, 4) = 7$$

$a \circ b = b \circ a$  fuer alle  $a, b : T$  (Symmetrie)(Kommutativitaet) — ABELSCHES MONOID

$(a \circ b) \circ c = a \circ (b \circ c)$  fuer alle  $a, b, c : T$  (Assoziativitaet)

$$u \circ a = a = a \circ u$$

es gibt ein  $u : T$ , so dass fuer alle  $a : T$  (neutrales Element) — MONOID

$\circ$	$T$	$u$
$+$	$\sum$	$\mathbb{Z}$
$*$	$\prod$	$\mathbb{Z}$
$\forall$	$\mathbb{B}$	$true$
$\exists$	$\mathbb{B}$	$false$

---

String mit Konkatination nicht-abelsches Monoid

$(\text{"a"} + \text{"b"}) + \text{"c"} \text{ equals } \text{"a"} + (\text{"b"} + \text{"c"})$

$\text{"a"} + \text{""} \text{ equals } \text{"a"}$

$\text{"a"} + \text{"b"} \text{ !equals } \text{"b"} + \text{"a"} \text{ (nicht equals)}$

-  $T_1, \dots, T_n$  Datentypen

-  $V_1, \dots, V_n$  Variablen

alle paarweise verschieden

$V_i$  vom Typ:  $T_i$

-  $R$  : boolescher Ausdruck, kann  $V_1 \dots V_n$  enthalten, Bereich (Range)

-  $P$  : beliebiger Ausdruck vom Typ  $T$ , kann  $V_1 \dots V_n$  enthalten, Koerper (Body)

Typ der Quantifizierung :  $T$

---

$(\forall i : \mathbb{N} \mid 0 \leq i \leq n : b[i] = 0)$  und das Ganze ist :  $\mathbb{B}$

$(\circ V_1 : T_1 \mid R : P)$  wobei  $T_1 : \mathbb{N}, P : \mathbb{B}$

$\wedge : \mathbb{B} \times \mathbb{B} \rightarrow \mathbb{B}$

$P : T_1 \times T_2 \times \dots \times T_n \rightarrow T$

---

### 1.3 Semantik

Bsp:  $(+i : \mathbb{Z} \mid -1 \leq i \leq 2 : i^2)$

1. Fall (Topf  $\neq \emptyset$ )

Von  $\mathbb{Z}$  alle Zahlen ausfiltern  $(-1, 0, 1, 2)$  (Menge)

$\rightarrow^{1^2} ((-1)^2, 1^2, 0^2, 2^2)(1, 1, 0, 4)$  (Multimenge)

$\rightarrow 2^2 + 1^2 + (-1)^2 + 0^2$

2. Fall (Topf = 0)

$\rightarrow$  Topf leer  $\rightarrow$  Resultat: Neutrales Element (von  $+$ )  $\rightarrow 0$

---

Beispiele:

$$1) (+ i : \mathbb{N} \mid 0 \leq i \leq 4 : i * 8) = (0 * 8) + (1 * 8) + \dots$$

$$2) (* i : \mathbb{N} \mid 0 \leq i \leq 3 : i + 1) = (0 + 1) * (1 + 1) * \dots$$

$$3) (\wedge i : \mathbb{N} \mid 0 \leq i \leq 2 : i * d \neq 6) = (0 * d) \neq 6 \wedge (1 * d) \neq 6 \wedge \dots$$

$$4) (\vee i : \mathbb{N} \mid 0 \leq i \leq 21 : b[i] = 0) = b[0] = 0 \vee b[1] = 0 \vee \dots$$

$$5) (\sum k : \mathbb{N} \mid k^2 = 4 : k^2) = 2$$

$$6) (\sum k : \mathbb{Z} \mid k^2 = 4 : k^2) = 2 + (-2) = 0$$

---

## 2 2. Woche

$$(\circ v_1 : T_1, \dots, v_n : T_n \mid R : P)$$

$$\text{E1: } \sum i : \mathbb{Z} \mid 0 \leq i < n : i^2)$$

- Wert haengt von  $n$  ab, nicht von  $i$

$$n = 3 : \quad 0 \quad 1 \quad 2$$

$$0^2 + 1^2 + 2^2 = 5$$

$$n = 0 : \text{kein } i$$

$$0 \text{ (neutral +)}$$

---

$$\text{E2: } (\sum j : \mathbb{Z} \mid 0 \leq j < n : j^2)$$

$$n = 3 \rightarrow 5$$

$$n = 0 \rightarrow 0$$

$$\text{E1: } (\sum i : \mathbb{Z} \mid 0 \leq i < n : i^2)$$

$$\text{E3: } (\sum i \textcircled{1} : \mathbb{Z} \mid 0 \leq i \textcircled{2} < n : i^2 \textcircled{3}) + 1 \textcircled{4}$$

$(\leftarrow \rightarrow)$  : Gueltigkeitsbereich von  $i$  (scope)

$i$  tritt hier 4 mal auf (occurs)

Auftreten (occurrences) ①, ②, ③ gebunden

Auftreten ④ frei

② und ③ gebunden an ①

② und ③ angewandte Auftreten (applied)

① bindende, deklarierende Auftreten (binding)

Eine Variable heisst frei in einem Ausdruck  $E$  (expresion), falls sie in  $E$  frei vorkommt.

$FV(E)$  = Menge der freie Variablen von  $E$

$FV(E_3) = \{ 'n', 'i' \}$  (Die Variablennamen und nicht die Werte der Variablen)

$x, y : \mathbb{Z}$

$x = 3, y = 5$

$\{x, y\} = \{3, 5\}$

$x = y = 3$

$\{x, y\} = \{3\}$

$x + y * 2$

$y, 2 : *$  Operator

dann das Resultat mit  $x$  und  $+$  Operator

E4:  $(\sum i : \mathbb{Z} \mid 0 \leq i < n : i^2) * (\sum i : \mathbb{Z} \mid 0 \leq i < n : i^3)$

$FV(E_4) = \{ 'n' \}$

E5:  $(\prod n \mid k \leq n \leq l : (\sum i : \mathbb{Z} \mid 0 \leq i < n : i^2) * (\sum i : \mathbb{Z} \mid 0 \leq i < n : i^3))$

$FV(E_5) = \{ 'k', 'l' \}$

E6:  $(\sum i : \mathbb{Z} \mid 0 \leq i \leq (\sum i : \mathbb{Z} \mid 2 \leq i < 3 : i^2) : i^2)$

$FV(E_6) = \emptyset$

Ein Ausdruck  $E$  ohne freie Variablen ( $FV(E_6) = \emptyset$  oder  $\{ \}$ ) heisst geschlossen

$(\sum i : \mathbb{Z} \mid 1 \leq i < 2 : (\sum j : \mathbb{Z} \mid 1 \leq j < 3 : i + j))$

$i$  zuerst:

$i :$   $\begin{matrix} 1 & & 2 \\ (\sum j : \mathbb{Z} \mid 1 \leq j < 3 : 1 + j) + (\sum j : \mathbb{Z} \mid 1 \leq j < 3 : 2 + j) \end{matrix}$

$j :$   $\begin{matrix} 1 & 2 & 3 & 1 & 2 & 3 \\ ((1 + 1) + (1 + 2) + (1 + 3)) + ((2 + 1) + (2 + 2) + (2 + 3)) \end{matrix}$

$j$  zuerst:

$$j : \quad (\sum i : \mathbb{Z} \mid 1 \leq i < 2 : ((i+1) + (i+2) + (i+3)))$$

$$i : \quad ((1+1) + (1+2) + (1+3)) + ((2+1) + (2+2) + (2+3))$$