Mathematik I

Vorlesungsskript

Falk Jonatan Strube

Vorlesung von Herrn Meinhold

2. November 2015

Inhaltsverzeichnis

I. Elementare Grundlagen **1**

1. Aussagen und Grundzüge der Logik **1**

2. Mengen **1**
- 2.1. Begriffe . . . 1
- 2.2. Mengenverknüpfungen . . . 2
- 2.3. Relationen . . . 3
  - 2.3.1. Grundbegriffe . . . 3
  - 2.3.2. Operationen auf Relationen . . . 6
  - 2.3.3. Äquivalenzrelationen . . . 9
  - 2.3.4. Ordnungsrelationen . . . 10
  - 2.3.5. Funktionen . . . 12
- 2.4. Gleichmächtigkeit, Kardinalzahlen . . . 15
- 2.5. Prinzip der vollständigen Induktion . . . 17

3. Zahlen **18**
- 3.1. Gruppen, Ringe, Körper . . . 18
- 3.2. Zahlentheorie . . . 19

Teil I. Elementare Grundlagen

1. Aussagen und Grundzüge der Logik

2. Mengen

3. Zahlen

3.1. Gruppen, Ringe, Körper

- Gegeben sei eine Menge M und eine zweistellige Operation $\circ$ (d.h. Abb. von $M \times M$ in M) Bezeichnung: $(M, \circ)$, analog $(M, \circ, *)$
- Die Operation $\circ$ heißt *kommutativ*, wenn $a \circ b = b \circ a$ für alle $a, b \in M$.
- Die Operation $\circ$ heißt *assoziativ*, wenn $(a \circ b) \circ c = a \circ (b \circ c)$ für alle $a, b, c \in M$.

Def. 1:
$(M, \circ)$ heißt *Gruppe*, wenn gilt:

1.) Die Operation $\circ$ ist assoziativ

2.) Es gibt genau ein *neutrales Element* $e \in M$ mit $a \circ e = e \circ a = a$ (für alle $a \in M$)

3.) Es gibt zu jedem $a \in M$ genau ein *inverses Element* a^{-1} mit $a \circ a^{-1} = a^{-1} \circ a = e$

4.) Eine Gruppe heißt *ABELsch*, wenn zusätzlich folgendes gilt:
$\circ$ ist kommutativ

Def. 2:
$(M, \oplus, *)$ heißt *Ring*, wenn gilt:

1.) $(M, \oplus)$ ist eine ABELsche Gruppe.

2.) Die Operation $*$ ist assoziativ.

3.) Es gelten für beliebige $a, b, c \in M$:
$a * (b \oplus c) = (a * b) \oplus (a * c)$
$(a \oplus b) * c = (a * c) \oplus (b * c)$ (Distributivgesetze)

4.) Ein Ring heiß *kommutativer Ring*, wenn gilt:
$*$ ist kommutativ

Def. 3:
$(M, \oplus, *)$ heißt *Körper*, wenn gilt:

1.) $(M, \oplus, *)$ ist ein Ring
(mit dem neutralen Element E_0 für die Operation $\oplus$)

2.) $(M \setminus \{E_0\}, *)$ ist eine ABELsche Gruppe
(mit dem neutralen Element E_1 für die Operation $*$)

3.2. Zahlentheorie

- Eine natürliche Zahl $p > 1$, die nurch durch 1 und sich selbst teilbar ist heißt *Primzahl*.
- Jede natürliche Zahl $n > 1$ ist entweder eine Primzahl, oder sie lässt sich als Produkt von Primzahlen schreiben.
  Diese sogenannte *Primfaktorzerlegung* ist bis auf die Reihenfolge der Faktoren eindeutig.

Def. 4:
Zwei natürliche zahlen aus $\mathbb{N}^*$ heißen *teilerfremd*, wenn sie außer 1 keine gemeinsamen teiler besitzen.

- Es sei $a \in \mathbb{Z}$ und $m \in \mathbb{N}^*$. Dann gibt es eine eindeutige Darstellung der Gestalt $\boxed{a = q \cdot m + r}$ mit $\boxed{0 \leq r < m}$ und $q \in \mathbb{Z}$.
  Bezeichnung: m ... *Modul* $\quad r$ ... (kleinste nichtnegative) *Rest modulo m* ($r \equiv mod(a, m)$)
- Zur Erinnerung: a und b seien ganze Zahlen, $m \in \ltimes^*$, dann $a \equiv b(mod\ \ m)$ [a kongruent $b\ modulo\ m$]
  $\Leftrightarrow a$ und b haben den gleicher Rest $modulo\ m$
  $\Leftrightarrow a - b$ ist durch m teilbar (d.h. $\exists k \in \mathbb{Z} \quad a - b = k \cdot m$)

  Satz 1:
  Es sei $a \equiv b(mod\ m)$, $c \equiv d(mod\ m)$, dann gilt: $a + c \equiv b + d(mod\ m)$ und $a \cdot c \equiv b \cdot d(mod\ m)$ (d.h. in Summen und Produktenn darf jede Zahl durch einen beliebigen Vertreter der gleichen Restklasse ersetzt werden).

  Bsp. 1:
  a) $307 + 598 \equiv 1 + (-2) \equiv -1 \equiv 5(mod\ 6)$
  b) $307 \cdot 598 \equiv 1 \cdot (-2) \equiv -2 \equiv 4(mod\ 6)$
  c) $598^6 \equiv (-2)^6 \equiv 64 \equiv 4(mod\ 6)$

- Man wählt aus jeder Restklasse den kleinsten nichtnegativen Vertreter
  $\curvearrowright$ Menge von Resten $modulo\ m$: $\mathbb{Z}_m := \{0, 1, ..., m-1\}$
  $\curvearrowright$ „modulare Arithmetik“: Operation $\oplus$ und $\odot$ für Zahlen aus $\mathbb{Z}_m$ erklärbar, in dem für das Ergebnis jeweils der kleinste nichtnegative Rest $modulo\ m$ gewählt wird (vgl. Satz 1)
  z.B. $\mathbb{Z}_7 = \{0, 1, ..., 6\}$, $\quad 5 \oplus 4 = 2$, da $5 + 4 \equiv 9 \equiv 2(mod\ 7)$ $\quad 5 \odot 6 = 2$, da $5 \cdot 6 \equiv 30 \equiv 2(mod\ 7)$
  Falls keine Verwechselung zu befürchten ist, wird die übliche Schreibweise $+$ und $\cdot$ anstelle von $\oplus$ und $\odot$ verwendet.