Mathematik I

Vorlesungsskript

Falk Jonatan Strube

Vorlesung von Herrn Meinhold

9. November 2015

Inhaltsverzeichnis

I. Elementare Grundlagen **1**

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

2. Mengen **1**

3. Zahlen **1**

3.1. Gruppen, Ringe, Körper 1

3.2. Zahlentheorie 2

3.3. Reelle Zahlen 5

3.3.1. Algebraische Struktur 5

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* 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. $\mathbb{Z}_7 = \{0, 1, ..., 6\}$, $5 \oplus 4 = 2$, da $5 + 4 \equiv 9 \equiv 2(mod\ 7)$ $5 \odot 6 = 2$, 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.

Def. 5:
Wenn es zu $c \in \mathbb{Z}_m$ eine Zahl $d \in \mathbb{Z}_m$ gibt, mit $c \cdot d \equiv 1(mod\ m)$ (bzw. $c \odot d \equiv 1$), so heißt d die *(multiplikative) modulare Inverse* zu c in $\mathbb{Z}_m$.
Bezeichnung: $d = c^{-1}$

Bsp. 2:
$c = 3 \in \mathbb{Z}_7$, wegen $3 \cdot 5 \equiv 1(mod\ 7)$ ist (in $\mathbb{Z}_7$) $3^{-1} = 5$.

Satz 2: Zu $a \in \mathbb{Z}_m, a \neq 0$, gibt es genau dann eine modulare Inverse in $\mathbb{Z}_m$, wenn a und m teilerfremd sind ($ggT(a, m) = 1$).

Satz 3: Es sei p eine Primzahl. Dann ist $(\mathbb{Z}_m, \oplus, \odot)$ ein Körper.
Bemerkung: Falls m keine Primzahl ist, so ist $(\mathbb{Z}_m, \oplus, \odot)$ ein kommutativer Ring.

EUKLIDischer Algorithmus

- Verfahren zur Ermittlung des größten gemeinsamen Teilers t zweier positiver natürlicher Zahlen, $t = ggT(a, b)$.
- In erweiterter Form bietet der Algorithmus eine Möglichkeit zur Bestimmung der modularen Inversen von a zum Modul m (mit $a < m$ und a, m teilerfremd).

Satz 4: (EUKLIDischer Algorithmus)
Es seien $a, b \in \mathbb{N}^*, a > b$. Man bildet die endliche Folge
$r_0 := b,\ r_1 = mod\ (a, b),\ r_2 = mod\ (r_0, r_1), ...,\ r_n = mod\ (r_{n-2}, r_{n-1})$, Abbruch falls $r_n = 0$.
In diesem Fall gist $\boxed{ggT(a, b) = r_{n-1}}$ (letzter nicht verschwindender Rest).
Bezeichnung: j-te Division ... $\boxed{r_{j-2} : r_{j-1} = q_j \text{ Rest } r_j}$ $(j = 1, ..., n)$ (dabei $r_1 := a$).

Satz 5: (erweiterter EUKLIDischer Algorithmus)
Zusätzlich zur Folge (r_n) aus Satz 4 bilde man die Folgen
$x_0 = 0,\ x_1 = 1,\ x_2 = x_0 - q_2 x_1, ...,\ x_j = x_{j-2} - q_j x_{j-1} \quad (j \le n-1)$ und
$y_0 = 1,\ y_1 = -q_1,\ y_2 = y_0 - q_2 y_1, ...,\ y_j = y_{j-2} - q_j y_{j-1} \quad (j \le n-1)$
Dann gilt für alle $j = 0, ...,\ n-1$: $\boxed{r_j = x_j \cdot a + y_j \cdot b}$
Insbesondere gilt $\boxed{ggT(a, b) = x_{n-1} \cdot a + y_{n-1} \cdot b}$

Diskussion:

1.) Der Sinn der erweiterten EUKLIDischen Algorithmus besteht darin, in jedem Schrit den *Divisionsrest* r *als linearkombination von* a *und* b *mit ganzzahligen Koeffizienten* x *und* y darzustellen: $r = x \cdot a + y \cdot b$
Der Mechanismus wird am besten im Rechenschema des nachfolgenden Bsp. 4 deutlich.

2.) Sind c und m teilerfremd, $1 \le c < m$, d.h. $ggT(m, c) = 1$, so erhält man mit dem erweiterten EUKLIDischen Algorithmus ($a = m, b = c$) eine Darstellung in der Form $\boxed{1 = x \cdot m + y \cdot c}$.
$\curvearrowright y \cdot c \equiv 1 (mod\ m)$ und damit $c^{-1} \equiv y (mod\ m)$ (für die modulare Inverse muss eventuell noch der in $\mathbb{Z}_m$ liegende, zu y kongruente, Wert gebildet werden!).

Bsp. 3:
Man ermittle den größten gemeinsamen Teiler t sowie das kleinste gemeinsame Vielfache v der Zahlen 132 und 84.

- Es genügt der „einfache“ Algorithmus:

$$\begin{aligned} 132 : 84 &= 1 \text{ Rest } 48 \\ 84 : 48 &= 1 \text{ Rest } 36 \\ 48 : 36 &= 1 \text{ Rest } 12 \quad \curvearrowright t = ggT(132, 84) = \underline{\underline{12}} \\ 36 : 12 &= 3 \text{ Rest } \boxed{0} \curvearrowright \text{ Ende.} \end{aligned}$$

- $v = \dfrac{a \cdot b}{t} = \dfrac{132 \cdot 84}{12} = \underline{\underline{924}} = kgV(132, 84)$

Bsp. 4:

Man ermittle die modulare Inverse von $\overbrace{11}^{b}$ zum Modul $\overbrace{25}^{a}$.

		$11 = 0 \cdot 25 + 1 \cdot 11$ (1)
$25 : 11 = 2$ Rest 3	$3 = 25 - 2 \cdot 11$	$3 = 1 \cdot 25 - 2 \cdot 11$ (2)
$11 : 3 = 3$ Rest 2	$2 = 11 - 3 \cdot 3$	$2 = -3 \cdot 25 + 7 \cdot 11$ (3)
$3 : 2 = 1$ Rest 1	$1 = 3 - 2$	$\boxed{1} = 4 \cdot 25 - 9 \cdot 11$
$2 : 1 = 2$ Rest 0		

$\curvearrowright (-9) \cdot 11 \equiv 1 (mod\ 25)$
$\curvearrowright 11^{-1} \equiv -9 \equiv 16 (mod\ 25)$, die Inverse von 11 in $\mathbb{Z}_{25}$ ist 16.
Zu den Schritten:

(1) $b = 0 \cdot a + 1 \cdot b$

(2) mittleres Feld als Linearkombination

(3) ab hier Rechnung links spaltenweise durchführen, dabei Faktoren a und b beibehalten.

EULERsche φ-Funktion, Satz von EULER

Def. 6:
Es sei $n \in \mathbb{N}^*$. Dann *EULERsche φ-Funktion*:
$\varphi(n) :=$ Anzahl der zu n teilerfremden Elemente aus $\{1, 2, ..., n\}$. Eigenschaften der φ-Funktion:

- Es sei p eine Primzahl, dann ist $\boxed{\varphi(p) = p - 1}$, $\boxed{\varphi(p^k) = p^{k-1}(p-1)}$ $(k \in \mathbb{N}^*$
- Falls $ggT(m, n) = 1$, so gilt $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$.
- Speziell: $n = p \cdot q$ (p, q Primzahlen), dann $\boxed{\varphi(n) = (p-1) \cdot (q-1)}$ (1).

Satz 6: (Satz von EULER)
Es sei $ggT(a, n) = 1$, dann gilt:
$\boxed{a^{\varphi(n)} \equiv 1 (mod\ n)}$ (2).

RSA-Verschlüsselung

- Die Formeln (1) und (2) [siehe oberhalb] bilden die Grundlage für die sogenannte RSA-Verschlüsselung (RIVES, SHAMIR, ADLEMAN - 1978)
- Schlüsselerzeugung:
  1.) Man wählt (in der Praxis sehr große) Primzahlen d und q.
  2.) $n := p \cdot q$, $m := \varphi(n) \overset{(1)}{=} (p-1)(q-1)$
  3.) e wird so gewählt, dass $ggT(e, m) = 1$
  4.) $d := e^{-1} (mod\ m)$ (modulare Inverse)
  5.) (n, e) ... öffentlicher Schlüssel
  (n, d) ... geheimer Schlüssel (geheim ist nur d)
  p, q und m werden nicht mehr benötigt, bleiben aber geheim!

- Verschlüsselung:
  Klartext a teilerfremd zu n verschlüsseln mit e, d.h. $b :\equiv a^e (mod\ n)$ bilden (b ... Geheimtext)
- Entschlüsselung:
  Der Empfänger und Besitzer des geheimen Schlüssels bildet $b^d (mod\ \ m)$ und erhält $b^d \equiv a(mod\ n)$ denn $b^d \equiv (a^e)^d \equiv a^{ed} \equiv a^{1+k\cdot m} \equiv a \cdot \underbrace{\left(a^{\varphi(n)}\right)}_{\equiv 1 \text{ wegen Satz 5}}{}^{k} \equiv a(mod\ n)$.
- Praktische Durchführung vgl Übungsaufgabe 2.4

3.3. Reelle Zahlen

$\mathbb{R}$ ... Menge der reellen Zahlen.
Auf $\mathbb{R}$ existiert eine algebraische Struktur und eine Ordnungsstruktur.

3.3.1. Algebraische Struktur

$(\mathbb{R}, +, \cdot)$ mit den arithmetischen Operationen $+$ (Addition) und $\cdot$ (Multiplikation) ist ein Körper.

Def. 7:

a.) $\boxed{0! := 1,\ n! = n \cdot (n-1)!}$ mit $n \in \mathbb{N}^*$ *Fakultät* (rekursive Funktion)

b.) Sei $\alpha \in \mathbb{R}, k \in \mathbb{N}^*$, dann sei $\boxed{\binom{\alpha}{0} := 1, \binom{\alpha}{k} := \frac{\alpha}{k}\binom{\alpha-1}{k-1}}$ Binominalkoeffizient α über k.

d.h. $\boxed{\binom{\alpha}{k} = \frac{\alpha(\alpha-1)(\alpha-2)...(\alpha-k-1)}{k!}}$

Diskussion:

1.) Für $k, n \in \mathbb{N},\ 0 \leq k \leq n$ gilt $\boxed{\binom{n}{k} = \binom{n}{n-k} = \frac{n!}{k!(n-k)!}}$

2.) Für $k \in \mathbb{N}, \alpha \in \mathbb{R}$ gilt $\boxed{\binom{\alpha}{k} + \binom{\alpha}{k+1} = \binom{\alpha+1}{k+1}}$

3.) *Binomischer Lehrsatz*: $(a+b)^k = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} \cdot b^k = a^n + n \cdot a^{n-1} \cdot b + \binom{n}{2} a^{n-2} \cdot b^2 + ... + b^n$

Pascalsches Dreieck: (Spalte $\hat{=} k$ in $\binom{n}{k}$)

					1							$n=0$
				1		1						1
			1		2		1					2
		1		3		3		1				3
	1		4		6		4		1			4
1		5		10		10		5		1		5

Stellenwertsysteme:

- Es sei $k > 1$ eine natürliche Zahl (die sogenannte Basis)
- $x = (\underbrace{x_p x_{p-1} ... x_1 x_0}_{\text{Vorkomma}}, \underbrace{x_{-1} x_{-2} ... x_{-q}}_{\text{Nachkomma}})_b$
  $:= \underbrace{x_p \cdot b^p + x_{p-1} \cdot b^{p-1} + ... + x_1 \cdot b^1 + x_0 \cdot b^0}_{\text{Vorkomma}} + \underbrace{x_{-1} \cdot b^{-1} + x_{-2} \cdot b^{-2} + ... + x_{-q} \cdot b^{-q}}_{\text{Nachkomma}}$
  heißt Darstellung zur Basis b (*).

Bsp. 5:

- $b = 2 \ldots$ *Dual- oder Binärsystem* (Ziffern $\{0, 1\}$)
- $b = 3 \ldots$ Trialsystem
- $b = 10 \ldots$ *Dezimalsystem*
- $b = 16 \ldots$ *Hexadezimalsystem* (Ziffern $\{0, 1, 2, ..., 9, \underset{10}{A}, \underset{11}{B}, \underset{12}{C}, \underset{13}{D}, \underset{14}{E}, \underset{15}{F}\}$

z.B. $(47)_{10} = (101111)_2 = (1202)_3 = (57)_8 = (2F)_{16}$

Übergang von einem Ziffernsystem zu einem anderen

z.B. $p = 3,\ q = 2$

$$\begin{aligned} x &= x_3 b^3 + x_2 b^2 + x_1 b^1 + x_0 + x_{-1} b^{-1} + x_{-2} b^{-2} \\ &= (x_3 b^2 + x_2 x^1 + x_1) b + x_0 + (x_{-1} + x_{-2} b^{-1}) b^{-1} \\ &= ((x_3 b^1 + x_2) b + x_1) b + x_0 + (x_{-1} + x_{-2} b^{-1}) b^{-1} \end{aligned}$$

Grundlage: fortgesetztes Klammern:

$$\begin{aligned} x = ((....((x_p b + x_{p-1}) b + x_{p-2}) b + ... + x_2) b + x_1) b + x_0 + \\ ((...(x_{-q} b^{-1} + x_{-(q-1)}) b^{-1} + ... + x_{-2}) b^{-1} + x_{-1}) b^{-1} \end{aligned}$$

(**)

Bsp. 6: Übergang Dezimalsystem $\rightarrow$ anderes System

- ganzer Teil: fortgesetzte Division durch b und Restabspaltung liefert b-Ziffern in der Reihenfolge $x_0, x_1, x_2, ...$
- gebrochener Teil: fortgesetzte Multiplikation mit b und Abspaltung des ganzzahligen Anteils liefert b-Ziffern in der Reihenfolge $x_{-1}, x_{-2}, ...$

z.B. Dezimalsystem $\rightarrow$ Hexadezimalsystem ($b = 16$)
$x = 435, 9$
ganzer Teil:

$435 : 16 =$	27	Rest 3	$\rightarrow x_0$
$27 : 16 =$	1	Rest 11	$\rightarrow x_1$
$1 : 16 =$	$\boxed{0}$	Rest 1	$\rightarrow x_2$

gebrochener Teil:

$0,9 \cdot 16 =$	0.4	$+14$	$\rightarrow x_{-1}$
$0,4 \cdot 16 =$	$\boxed{0.4}$	$+6$	$\rightarrow x_{-2}$ (Periode, da gleicher „Nachkommarest“)

$\curvearrowright x = (1B3, E\overline{6})_{16}$

Bsp. 7: Übergang anderer Systeme $\to$ Dezimalsystem
Entweder direkte Auswertung von (*) (v.a. beim Dualsystem $\to$ Addition von 2er-Potenzen) *oder* Klammern in (**) von innen nach außen berechnen (zweckmäßig HORNER-Schema).

- ganzer Teil: beginnend mit x_p
  ABB1
- gebrochener Teil: beginnend mit x_{-q}
  ABB 2

$x = (1E2, B8)_{16}$
ganzer Teil:

$$\begin{array}{c|ccc} & 1 & 14 & 2 \\ 16 & & 16 & 480 \\ \hline & 1 & 30 & \boxed{482} \end{array}$$

gebrochener Teil:

$$\begin{array}{c|ccc} & 8 & 11 & * \\ \frac{1}{16} = 0,0625 & & 0,5 & \boxed{0,71875} \\ \hline & 8 & 11,5 & \end{array}$$

$\curvearrowright x = \underline{\underline{482,71875}}$

Bsp. 8: Hexadezimalsystem $\leftrightarrow$ Dualsystem
4 Dualziffern entsprechen einer Hexadezimalziffer ($2^4 = 16$) $\curvearrowright$ 4er Gruppen von Dualziffern ab Komma bilden.

a.) $(A8C, B2)_{16} = (1010\ 1000\ 1100,\ 1011\ 1011\ 001(0))_2$

b.) $((0)110\ 1110,\ 101(0))_2 = (6E, A)_{16}$