

**Script** generated by TTT

Title: Meixner: test2 (14.11.2012)

Date: Wed Nov 14 17:41:44 CET 2012

Duration: 86:21 min

Pages: 41

WS 2012/13

## Zentralübung zur Vorlesung Diskrete Strukturen (Prof. Mayr)

Dr. Werner Meixner

Fakultät für Informatik  
TU München

<http://www14.in.tum.de/lehre/2012WS/ds/uebung/>

14. November 2012

## ZÜ IV

### Übersicht:

1. **Übungsbetrieb:** Fragen, Probleme?
2. **Thema:** Zirkuläre Operationen
3. **Vorbereitung** auf TA Blatt 5:
  - Rechnen modulo  $m$  (VA 1)
  - Darstellung zirkulärer Operationen (VA 2)
  - Beispiel einer Gruppenalgebra (VA 3)
  - Gruppen und Untergruppen (VA 4)

## 1. Übungsbetrieb

### 1.1 Fragen, Probleme?

?

## 2. Thema

### 2.1 Zirkuläre Operationen

Beispiel:

Operation (+1) auf  $\{0, 1, 2, 3\}$ :

0,  
0 + 1 = 1,  
1 + 1 = 2,  
2 + 1 = 3,  
3 + 1 = 0,  
0 + 1 = 1,  
1 + 1 = 2,  
2 + 1 = 3,  
3 + 1 = 0,  
... usw.

Bemerkung:

Wesentliche Teile der Algebra werden von zirkulären Operationen beherrscht, beispielsweise in Form der Potenzierung  $a^m$ , falls  $a^m = 1$  gilt.

$$1, a, a^2, a^3, a^4, \dots, a^{m-1}, a^m = 1, a, a^2, \dots$$

Zirkuläres Rechnen ist eine Rechnungsart, die über die Schulmathematik hinausgeht.

### Rechnen modulo $m$

Ganze Zahlen  $a, b \in \mathbb{Z}$  nennt man

kongruent modulo  $m$ , mit  $m \in \mathbb{N}$ , i.  $\mathbb{Z}$ .

$$a \equiv b \pmod{m},$$

falls sich  $a$  und  $b$  um ein ganzzahliges Vielfaches von  $m$  unterscheiden, d. h.,

falls es ein  $k \in \mathbb{Z}$  gibt, so dass gilt

$$a = b + k \cdot m.$$

Man schreibt auch  $a \equiv_m b$  für  $a \equiv b \pmod{m}$ .

$\equiv_m$  ist eine Äquivalenzrelation über  $\mathbb{Z}$ ,

ja sogar eine „Kongruenzrelation“.

Davon abgeleitet ist die Definition der Operation  $\text{mod} : \mathbb{Z} \times \mathbb{N} \rightarrow \mathbb{Z}$ :

$$b = a \text{ mod } m \iff a \equiv b \pmod{m} \text{ und } 0 \leq b < m.$$

Für jedes  $m$  ist  $\text{mod } m$  eine unäre Operation über  $\mathbb{Z}$ .

$a \text{ mod } m$  heißt Rest der natürlichen Division von  $a$  durch  $m$ .

**Achtung:** Wir werden in der nächsten Zentralübung ein Quiz für zirkuläres Rechnen veranstalten. Lernen Sie also die folgende VA 1.

### 3. Vorbereitung auf TA Blatt 5

#### 3.1 VA 1, Rechnen modulo $m$

Teil 1:

Zeigen Sie für alle  $a, b \in \mathbb{Z}$  und  $m \in \mathbb{N}$ :

$$a \equiv a \pmod{m} \pmod{m}, \quad (1)$$

$$(a + b) \pmod{m} = [(a \pmod{m}) + (b \pmod{m})] \pmod{m}, \quad (2)$$

$$(a \cdot b) \pmod{m} = [(a \pmod{m}) \cdot (b \pmod{m})] \pmod{m}. \quad (3)$$

### 3. Vorbereitung auf TA Blatt 5

#### 3.1 VA 1, Rechnen modulo $m$

Teil 1:

Zeigen Sie für alle  $a, b \in \mathbb{Z}$  und  $m \in \mathbb{N}$ :

$$a \equiv a \pmod{m} \pmod{m}, \quad (1)$$

$$(a + b) \pmod{m} = [(a \pmod{m}) + (b \pmod{m})] \pmod{m}, \quad (2)$$

$$(a \cdot b) \pmod{m} = [(a \pmod{m}) \cdot (b \pmod{m})] \pmod{m}. \quad (3)$$

1 Zu beweisen ist:  $a \equiv a \pmod{m} \pmod{m}$

Lösung:

Die Kongruenz modulo  $m$  ist definiert durch

$$x \equiv y \pmod{m} \iff (\exists k \in \mathbb{Z}) [x = y + k \cdot m].$$

Nach Definition von  $(a \pmod{b})$  gilt für ein bestimmtes  $k \in \mathbb{Z}$

$$a \pmod{b} = a + k \cdot b, \quad \text{d. h.} \quad a = a \pmod{b} + k' \cdot b,$$

mithin

$$a \equiv a \pmod{b} \pmod{b}.$$

1 Zu beweisen ist:  $a \equiv a \pmod{m} \pmod{m}$

Lösung:

Die Kongruenz modulo  $m$  ist definiert durch

$$x \equiv y \pmod{m} \iff (\exists k \in \mathbb{Z}) [x = y + k \cdot m].$$

Nach Definition von  $(a \pmod{b})$  gilt für ein bestimmtes  $k \in \mathbb{Z}$

$$a \pmod{b} = a + k \cdot b, \quad \text{d. h.} \quad a = a \pmod{b} + k' \cdot b,$$

mithin

$$a \equiv a \pmod{b} \pmod{b}.$$

Davon abgeleitet ist die Definition der Operation  $\text{mod} : \mathbb{Z} \times \mathbb{N} \rightarrow \mathbb{Z}$ :

$$b = a \text{ mod } m \iff a \equiv b \pmod{m} \text{ und } 0 \leq b < m.$$

Für jedes  $m$  ist  $\text{mod } m$  eine unäre Operation über  $\mathbb{Z}$ .

$a \text{ mod } m$  heißt Rest der natürlichen Division von  $a$  durch  $m$ .

**Achtung:** Wir werden in der nächsten Zentralübung ein Quiz für zirkuläres Rechnen veranstalten. Lernen Sie also die folgende VA 1.

## Rechnen modulo $m$

Ganze Zahlen  $a, b \in \mathbb{Z}$  nennt man

kongruent modulo  $m$ , mit  $m \in \mathbb{N}$ , i. Z.

$$a \equiv b \pmod{m},$$

falls sich  $a$  und  $b$  um ein ganzzahliges Vielfaches von  $m$  unterscheiden, d. h.,

falls es ein  $k \in \mathbb{Z}$  gibt, so dass gilt

$$a = b + k \cdot m.$$

Man schreibt auch  $a \equiv_m b$  für  $a \equiv b \pmod{m}$ .

$\equiv_m$  ist eine Äquivalenzrelation über  $\mathbb{Z}$ ,

ja sogar eine „Kongruenzrelation“.

Davon abgeleitet ist die Definition der Operation  $\text{mod} : \mathbb{Z} \times \mathbb{N} \rightarrow \mathbb{Z}$ :

$$b = a \text{ mod } m \iff a \equiv b \pmod{m} \text{ und } 0 \leq b < m.$$

Für jedes  $m$  ist  $\text{mod } m$  eine unäre Operation über  $\mathbb{Z}$ .

$a \text{ mod } m$  heißt Rest der natürlichen Division von  $a$  durch  $m$ .

**Achtung:** Wir werden in der nächsten Zentralübung ein Quiz für zirkuläres Rechnen veranstalten. Lernen Sie also die folgende VA 1.

1 Zu beweisen ist:  $a \equiv a \text{ mod } m \pmod{m}$

**Lösung:**

Die Kongruenz modulo  $m$  ist definiert durch

$$x \equiv y \pmod{m} \iff (\exists k \in \mathbb{Z}) \{x = y + k \cdot m\}.$$

Nach Definition von  $(a \text{ mod } b)$  gilt für ein bestimmtes  $k \in \mathbb{Z}$

$$a \text{ mod } b = a + k \cdot b, \quad \text{d. h.} \quad a = a \text{ mod } b + k' \cdot b,$$

mithin

$$a \equiv a \text{ mod } b \pmod{b}.$$

- 2 Zu beweisen ist:  
 $(a + b) \bmod m = [(a \bmod m) + (b \bmod m)] \bmod m.$

Lösung:

Wir setzen linke Seite bzw. rechte Seite der Gleichung

$$\begin{aligned} x^{\text{Ⓢ}} &:= (a + b) \bmod m, \\ y &:= [(a \bmod m) + (b \bmod m)] \bmod m. \end{aligned}$$

und zeigen  $x = y$ .

Es gilt  $0 \leq x, y < m$  und

$$\begin{aligned} x &= a + b + k_x \cdot m, \\ y &= (a \bmod m) + (b \bmod m) + k_y \cdot m, \\ (a \bmod m) &= a + k_a \cdot m, \\ (b \bmod m) &= b + k_b \cdot m \end{aligned}$$

für gewisse  $k_a, k_b, k_x, k_y \in \mathbb{Z}$  und es folgt

$$\begin{aligned} y^{\text{Ⓢ}} &= a + k_a \cdot m + b + k_b \cdot m + k_y \cdot m \\ &= x - k_x \cdot m + k_a \cdot m + k_b \cdot m + k_y \cdot m \\ &= x + (k_a + k_b + k_y - k_x) \cdot m \\ &= x + k \cdot m. \end{aligned}$$

Wegen  $0 \leq x, y < m$  folgt  $x = y$ .

- 2 Zu beweisen ist:  
 $(a + b) \bmod m = [(a \bmod m) + (b \bmod m)] \bmod m.$

Lösung:

Wir setzen linke Seite bzw. rechte Seite der Gleichung

$$\begin{aligned} x^{\text{Ⓢ}} &:= (a + b) \bmod m, \\ y &:= [(a \bmod m) + (b \bmod m)] \bmod m. \end{aligned}$$

und zeigen  $x = y$ .

Es gilt  $0 \leq x, y < m$  und

$$\begin{aligned} x &= a + b + k_x \cdot m, \\ y &= (a \bmod m) + (b \bmod m) + k_y \cdot m, \\ (a \bmod m) &= a + k_a \cdot m, \\ (b \bmod m) &= b + k_b \cdot m \end{aligned}$$

für gewisse  $k_a, k_b, k_x, k_y \in \mathbb{Z}$  und es folgt

$$\begin{aligned} y^{\text{Ⓢ}} &= a + k_a \cdot m + b + k_b \cdot m + k_y \cdot m \\ &= x - k_x \cdot m + k_a \cdot m + k_b \cdot m + k_y \cdot m \\ &= x + (k_a + k_b + k_y - k_x) \cdot m \\ &= x + k \cdot m. \end{aligned}$$

Wegen  $0 \leq x, y < m$  folgt  $x = y$ .

Es gilt  $0 \leq x, y < m$  und

$$\begin{aligned}x &= a + b + k_x \cdot m, \\y &= (a \bmod m) + (b \bmod m) + k_y \cdot m, \\(a \bmod m) &= a + k_a \cdot m, \\(b \bmod m) &= b + k_b \cdot m\end{aligned}$$

für gewisse  $k_a, k_b, k_x, k_y \in \mathbb{Z}$  und es folgt

$$\begin{aligned}y &= a + k_a \cdot m + b + k_b \cdot m + k_y \cdot m \\&= x - k_x \cdot m + k_a \cdot m + k_b \cdot m + k_y \cdot m \\&= x + (k_a + k_b + k_y - k_x) \cdot m \\&= x + k \cdot m.\end{aligned}$$

Wegen  $0 \leq x, y < m$  folgt  $x = y$ .

Analog verläuft der Beweis der Gleichung 3:

$$(a \cdot b) \bmod m = [(a \bmod m) \cdot (b \bmod m)] \bmod m.$$

Teil 2:

In enger Beziehung zur mod-Operation steht die **ganzzahlige Division**  $a \operatorname{div} m$  zweier Zahlen  $a \in \mathbb{Z}, m \in \mathbb{N}$ .

Es gilt

$$a = (a \operatorname{div} m) \cdot m + (a \bmod m).$$

Berechnen Sie:  $\heartsuit$

- (i)  $5 \operatorname{div} 4$ ,    (ii)  $(-5) \operatorname{div} 4$ ,    (iii)  $(-x) \operatorname{div} 1$ .

Teil 2:

In enger Beziehung zur mod-Operation steht die **ganzzahlige Division**  $a \operatorname{div} m$  zweier Zahlen  $a \in \mathbb{Z}, m \in \mathbb{N}$ .

Es gilt

$$a = (a \operatorname{div} m) \cdot m + (a \bmod m).$$

Berechnen Sie:  $\heartsuit$

- (i)  $5 \operatorname{div} 4$ ,    (ii)  $(-5) \operatorname{div} 4$ ,    (iii)  $(-x) \operatorname{div} 1$ .

(i)  $5 \operatorname{div} 4$ :

Seien  $a = 5$  und  $m = 4$ .

Dann gilt

$$(5 \operatorname{div} 4) \cdot 4 = 5 - (5 \bmod 4) = 5 - 1 = 4.$$

Es folgt  $5 \operatorname{div} 4 = 1$ .

(ii)  $(-5) \operatorname{div} 4$ :

Seien  $a = -5$  und  $m = 4$ .

Dann gilt

$$\begin{aligned} ((-5) \operatorname{div} 4) \cdot 4 &= -5 - ((-5) \bmod 4) \\ &= -5 - ((-5 + 8) \bmod 4) \\ &= -5 - 3 = -8. \end{aligned}$$

Es folgt  $(-5) \operatorname{div} 4 = -2$ .

(iii)  $(-x) \operatorname{div} 1$ :

Seien  $a = -x$  und  $m = 1$ .

Dann gilt

$$((-x) \operatorname{div} 1) \cdot 1 = -x - ((-x) \bmod 1) = -x - 0 = -x.$$

Es folgt  $(-x) \operatorname{div} 1 = -x$ .

### 3.2 VA 2, 3-D Darstellung der mod-Operation

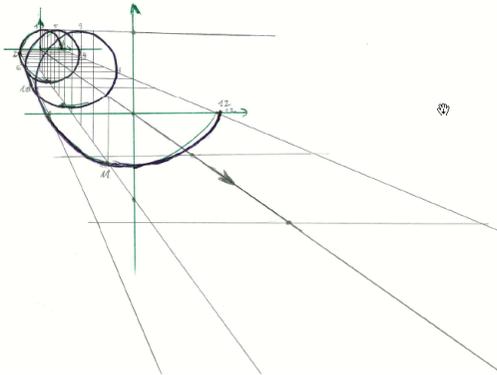
Die Operation  $g \bmod m$  mit  $m \in \mathbb{N}$  über den ganzen Zahlen  $g \in \mathbb{Z}$  eröffnet den Zugang zu zirkulären Operationen.

Für  $m = 4$  betrachten wir die folgende Abbildung  $f_4 : \mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{C}$  für alle  $g \in \mathbb{Z}$ :

$$f_4(g) = (g, i^{(g \bmod 4)}).$$

Entwickeln Sie für den Bereich  $g \in [-1, 6]$  mit Hilfe der Gauß'schen Ebene der komplexen Zahlen eine 3-dimensionale graphische Darstellung von  $f_4$ .

Darstellung:



### 3.3 VA 3, Beispiel einer Gruppenalgebra

Seien  $S = \mathbb{R} \setminus \{-1\}$  und für alle  $x, y \in S$

$$x \circ y = x + \frac{xy}{1+y} + xy.$$

Zeigen Sie, dass die Algebra  $A = \langle S, \circ \rangle$  bezüglich des binären Operators  $\circ$  eine Gruppe bildet.

Lösung:

- Zunächst ist zu prüfen, ob durch die Gleichung  $x \circ y = x + y + \frac{xy}{1+y} + xy$  tatsächlich eine Abbildung von  $S \times S$  in  $S$  definiert ist.

Seien  $x, y \in \mathbb{R} \setminus \{-1\}$ . Es gilt offenbar  $x \circ y \in \mathbb{R}$ .

Wir zeigen, dass  $-1 = x + y + \frac{xy}{1+y} + xy$  einen Widerspruch ergibt und deswegen  $x, y \in \mathbb{R} \setminus \{-1\}$  gelten muss.

$$\begin{aligned} -1 = x + y + \frac{xy}{1+y} + xy &\Rightarrow -1 - y = x(1+y) \\ &\Rightarrow x = \frac{-1-y}{1+y} \\ &\Rightarrow x = -1. \end{aligned}$$

### 3.3 VA 3, Beispiel einer Gruppenalgebra

Seien  $S = \mathbb{R} \setminus \{-1\}$  und für alle  $x, y \in S$

$$x \circ y = x + y + xy.$$

Zeigen Sie, dass die Algebra  $A = \langle S, \circ \rangle$  bezüglich des binären Operators  $\circ$  eine Gruppe bildet.

Lösung:

- 1 Zunächst ist zu prüfen, ob durch die Gleichung  $x \circ y = x + y + x \cdot y$  tatsächlich eine Abbildung von  $S \times S$  in  $S$  definiert ist.

Seien  $x, y \in \mathbb{R} \setminus \{-1\}$ . Es gilt offenbar  $x \circ y \in \mathbb{R}$ .

Wir zeigen, dass  $-1 = x + y + x \cdot y$  einen Widerspruch ergibt und deswegen  $x, y \in \mathbb{R} \setminus \{-1\}$  gelten muss.

$$\begin{aligned} -1 = x + y + x \cdot y &\Rightarrow -1 - y = x(1 + y) \\ &\Rightarrow x = \frac{-1 - y}{1 + y} \\ &\Rightarrow x = -1. \end{aligned}$$

- 2 Wir zeigen die Assoziativität von  $\circ$ .

$$\begin{aligned} x \circ (y \circ z) &= x + (y \circ z) + x \cdot (y \circ z) \\ &= x + (y + z + y \cdot z) + x \cdot (y + z + y \cdot z) \\ &= x + y + z + y \cdot z + x \cdot y + x \cdot z + x \cdot y \cdot z \\ &= (x + y + x \cdot y) + z + (x + y + x \cdot y) \cdot z \\ &= (x \circ y) + z + (x \circ y) \cdot z \\ &= (x \circ y) \circ z. \end{aligned}$$

- 3  $x = 0$  ist das Einselement bezüglich  $(x \circ y)$ .

$$0 \circ y = 0 + y + 0 \cdot y = y.$$

Das linke Einselement ist offensichtlich auch rechtes Einselement, d. h. Einselement.

- 4 Wir zeigen, dass zu einem Element  $x \in S$  das Inverse gegeben ist durch  $x^{-1} = -\frac{x}{1+x}$ .

Es gilt

$$\begin{aligned} x \circ y = 0 &\Leftrightarrow x + y + x \cdot y = 0 \\ &\Leftrightarrow y = -\frac{x}{1+x}. \end{aligned}$$

Die Existenz eines linken Inversen ist damit bewiesen.

- 4 Wir zeigen, dass zu einem Element  $x \in S$  das Inverse gegeben ist durch  $x^{-1} = -\frac{x}{1+x}$ .

Es gilt

$$\begin{aligned} x \circ y = 0 &\Leftrightarrow x + y + x \cdot y = 0 \\ &\Leftrightarrow y = -\frac{x}{1+x}. \end{aligned}$$

Die Existenz eines linken Inversen ist damit bewiesen.

### 3.4 VA 4, Gruppen und Untergruppen

Sei  $S' = (S, \circ)$  eine Halbgruppe.

Dann nennen wir ein Element  $x \in S$  vertauschbar bezüglich  $\circ$ , falls gilt

$$(\forall a \in S) [a \circ x = x \circ a].$$

Es sei  $V(S)$  die Menge aller bezüglich  $\circ$  vertauschbarer Elemente von  $S$ .

- 1 Zeigen Sie die Abgeschlossenheit von  $V(S)$  unter der Verknüpfung  $\circ$ , d. h.:

$$x, y \in V(S) \implies x \circ y \in V(S).$$

Lösung:

Seien  $x, y \in V(S)$ .

Zu zeigen ist

$$(\forall a \in S) [a \circ (x \circ y) = (x \circ y) \circ a].$$

Es gilt

$$\begin{aligned} a \circ (x \circ y) &= (a \circ x) \circ y \\ &= (x \circ a) \circ y \\ &= x \circ (a \circ y) \\ &= x \circ (y \circ a) \\ &= (x \circ y) \circ a. \end{aligned}$$

- 2 Nun nehmen wir an, dass  $S'$  eine Gruppe mit Einselement 1 ist.

Zeigen Sie, dass die Unterhalbgruppe  $(V(S), \circ_{V(S)})$  von  $S'$  dann ebenfalls eine Gruppe ist.

Lösung:

Wir zeigen die restlichen Abgeschlossenheitseigenschaften von  $V(S)$ , d. h., dass gilt

$$1 \in V(S), \text{ und} \\ x \in V(S) \implies x^{-1} \in V(S).$$

$1 \in V(S)$ :

Ein Einselement ist mit allen Elementen vertauschbar, also folgt

$$a \circ 1 = 1 \circ a \quad \text{für alle } a \in S.$$

$x \in V(S) \implies x^{-1} \in V(S)$ :

Aus  $a \circ 1 = 1 \circ a$  folgt (Klammern können weggelassen werden)

$$a \circ x^{-1} \circ x = x^{-1} \circ x \circ a \\ = x^{-1} \circ a \circ x.$$

Durch Multiplikation beider Seiten mit  $x^{-1}$  von rechts folgt die Gleichung

$$a \circ x^{-1} = x^{-1} \circ a.$$