

WS 2010/11

Zentralübung zur Vorlesung Diskrete Strukturen

Dr. Werner Meixner

Fakultät für Informatik
TU München

<http://www14.in.tum.de/lehre/2010WS/ds/uebung/>

24. November 2010

ZÜ V

Übersicht:

1. **Übungsbetrieb:** Fragen, Probleme?
„Das Versteh' ich nicht!“
2. **Thema:** Konzepte der Abstraktion:
Morphismen und Algebren.
3. **Vorbereitung** auf TA's Blatt 6:
Rechnung modulo m (VA 3)
Permutationen und Zyklen (VA 2)
Gruppen und Untergruppen (VA 1)

1. Übungsbetrieb

1.1 Fragen, Probleme?

?

1.2 „Das Versteh' ich nicht!“

Falsche Lesetechnik? Lesen und hören Sie strukturiert!

Eine Definition wird zunächst syntaktisch funktional analysiert.

Ein inhaltliches Verständnis entsteht in nachfolgenden Schritten.

2. Thema

2.1 Isomorphismus

Ein **Isomorphismus** vergleicht Bereiche, die bis auf **Bezeichnungsänderung** identisch sind.

Ein Isomorphismus etabliert dadurch einen **abstrakten Standpunkt**, von dem aus Dinge als im Wesentlichen gleich erscheinen, d.h. eine **gleiche Gestalt** haben, insbesondere **unabhängig** von den Bezeichnungen.

Berühmte Beispiele: Die Kardinalzahlen des Zählens (nach Cantor).

2.2 Homomorphismus

Mit einem Homomorphismus betrachtet man eine **Struktur** unter einem gewissen **abstrakten** Aspekt.

Die **Vertauschbarkeit** wird benutzt um komplexe Operationen durch einfachere Operationen zu ersetzen.

Beispiel 1: Wenn man die ganzen Zahlen unter dem Aspekt „gerade Zahl“ bzw. „ungerade Zahl“ betrachtet, dann wird diese Betrachtung durch den folgenden **Homomorphismus** etabliert.

$$f : \mathbb{Z} \ni x \mapsto (x \bmod 2) \in \mathbb{Z}_2 .$$

Beispiel 2: Wenn man die Zeit in Tagen mit je 24 Stunden zählt, dann wird das modelliert durch den Homomorphismus

$$f : \mathbb{Z} \ni x \mapsto (x \bmod 24) \in \mathbb{Z}_{24} .$$

Bemerkung:

Man beachte die Darstellung der ganzen Zahlen durch die Komponenten **Fortschritt** (Tage) und **Wiederholung** (24 Stunden).

Die Tage mit festgehaltener Uhrzeit durchschreiten eine **Restklasse** zur Untergruppe der durch 24 teilbaren Stundenzahlen.

Die Uhrzeit durchläuft **zyklisch wiederholt** die 24 Stunden.

2.3 Abstraktion durch Algebren

Unterschiedliche Rechenstrukturen werden durch Algebren auf einen

gemeinsamen Nenner

gebracht und sind dann in gewisser Weise gleich.

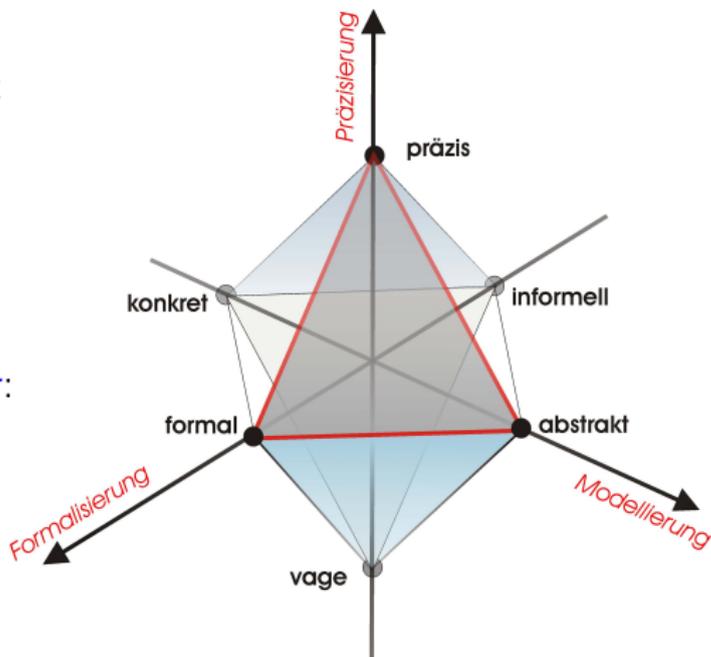
Auch dadurch wird eine **Abstraktion** geleistet.

Erinnerung an ZÜ 1:

Wissenschaftliche Schulung und Entwicklung vollzieht sich im Spannungsfeld folgender Begriffspaare:

- vage — präzise
- konkret — abstrakt
- informell — formal

Darstellung im Oktaeder:



3. Vorbereitung auf TA's Blatt 6

3.1 VA 3, 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

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

Diesen Zusammenhang kann man der Definition der Operation $\text{mod} : \mathbb{Z} \times \mathbb{N} \rightarrow \mathbb{Z}$ zugrunde legen:

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

Teil 1:

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

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

$$(a + b) \bmod m = [(a \bmod m) + (b \bmod m)] \bmod m, \quad (2)$$

$$(a \cdot b) \bmod m = [(a \bmod m) \cdot (b \bmod m)] \bmod m. \quad (3)$$

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

Lösung:

Die Kongruenz modulo m ist definiert durch

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

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

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

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

$$x := (a + b) \bmod m ,$$

$$y := [(a \bmod m) + (b \bmod m)] \bmod m .$$

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

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

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

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

Berechnen Sie:

- (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

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

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, Permutationen und Zyklen

Sei M eine endliche Menge und $z = (a_0, a_1, \dots, a_{|M|-1})$ ein $|M|$ -Tupel mit paarweise verschiedenen $a_i \in M$.

Dann ist die Abbildung

$$\pi_z : M \rightarrow M \text{ mit } \pi_z(a_i) = a_{(i+1) \bmod |M|}$$

ein *Zyklus* der Länge $|M|$ mit *Basis* M und *Darstellung* z .

Für jeden Zyklus π bezeichne $M(\pi)$ die Basis von π .

Man kann π_z als zyklische Nachfolgebildung in M auffassen.

- ① Wie viele Darstellungen besitzt ein Zyklus der Länge 3?

Welchen Zyklus

stellt $z = (4, 1, 3, 2)$ dar und welche Basis hat der Zyklus?

Welche verschiedenen Darstellungen

hat π_z^3 ?

Ist π_z^4 ein Zyklus?

Lösung:

Bemerkung:

Für Operationen f über einer Menge M , d.h. $f : M \rightarrow M$, gibt es die **mehrfache Hintereinanderausführung** der Operation f mit entsprechenden Schreibweisen. Es gilt

$$f^2 = f \circ f, \quad \text{und allgemein} \quad f^{n+1} = f \circ f^n \quad \forall n \in \mathbb{N},$$

d. h. für alle $n \in \mathbb{N}$ und $x \in M$

$$f^{n+1}(x) = f(f^n(x)), \quad \text{insbesondere} \quad f^2(x) = f(f(x)).$$

Wie viele Darstellungen besitzt ein Zyklus der Länge 3?

Antwort: 3.

Begründung:

Sei π ein Zyklus der Länge 3 mit Basis $M(\pi) = \{a, b, c\}$. Für jede Darstellung $z = (a_1, a_2, a_3)$ von π gilt

$$a_1 \in M, \quad a_2 = \pi(a_1), \quad a_3 = \pi^2(a_1) = \pi(a_2).$$

Damit gibt es genau die folgenden drei Darstellungen

$$z_1 = (a, \pi(a), \pi^2(a)), \quad z_2 = (b, \pi(b), \pi^2(b)), \quad z_3 = (c, \pi(c), \pi^2(c)).$$

Welchen Zyklus stellt $z = (4, 1, 3, 2)$ dar und welche Basis hat der Zyklus?

Antwort:

Die Basis von $z = (4, 1, 3, 2)$ ist $M_z = \{1, 2, 3, 4\}$.

Für den dargestellten Zyklus $\pi_z : M \rightarrow M$ gilt

$$\pi_z(1) = 3, \quad \pi_z(2) = 4, \quad \pi_z(3) = 2, \quad \pi_z(4) = 1.$$

Welche verschiedenen Darstellungen hat π_z^3 ?

Antwort:

Es gilt

$$\begin{aligned}\pi_z^3(1) &= \pi_z^2(\pi_z(1)) = \pi_z^2(3) = \pi_z(\pi_z(3)) = \pi_z(2) = 4, \\ \pi_z^3(2) &= \pi_z^2(\pi_z(2)) = \pi_z^2(4) = \pi_z(\pi_z(4)) = \pi_z(1) = 3, \\ \pi_z^3(3) &= \pi_z^2(\pi_z(3)) = \pi_z^2(2) = \pi_z(\pi_z(2)) = \pi_z(4) = 1, \\ \pi_z^3(4) &= \pi_z^2(\pi_z(4)) = \pi_z^2(1) = \pi_z(\pi_z(1)) = \pi_z(3) = 2.\end{aligned}$$

π_z^3 ist ein Zyklus mit genau den folgenden 4 Darstellungen.

$$z_1=(1, 4, 2, 3), \quad z_2=(2, 3, 1, 4), \quad z_3=(3, 1, 4, 2), \quad z_4=(4, 2, 3, 1).$$

Ist π_z^4 ein Zyklus?

Antwort: Nein!

Begründung:

Es gilt

$$\pi_z^4(1) = \pi_z(\pi_z^3(1)) = 1,$$

$$\pi_z^4(2) = \pi_z(\pi_z^3(2)) = 2,$$

$$\pi_z^4(3) = \pi_z(\pi_z^3(3)) = 3,$$

$$\pi_z^4(4) = \pi_z(\pi_z^3(4)) = 4.$$

π_z^4 ist **kein Zyklus**, weil $|\{(\pi^4)^n(1) \mid n \in \mathbb{N}\}| = 1 \neq 4$.

Tatsächlich ist π_z^4 gleich der Identität *id*.

Zyklen ρ, σ heißen *disjunkt*, falls $M(\rho) \cap M(\sigma) = \emptyset$ gilt, d. h., falls deren Basismengen disjunkt sind.

Eine Menge Z von paarweise disjunkten Zyklen heißt *Zykluspartition*.

Dabei bildet die Menge der Basismengen

$$P_Z = \{M(\pi); \pi \in Z\}$$

eine Mengenpartition der Vereinigung der Basismengen

$$M(Z) = \bigcup_{\pi \in Z} M(\pi).$$

Wir sagen, dass Z eine *Zykluspartition* der Menge $M(Z)$ ist.

- 2 Welche Basis haben die Zyklen zu
 $z_1 = (2, 5)$, $z_2 = (1)$, $z_3 = (5, 4, 3, 2, 1)$?

Geben Sie eine extensionale Darstellung
der Abbildungen π_{z_i} an!

Warum ist $Z = \{\pi_{z_1}, \pi_{z_2}, \pi_{z_3}\}$ keine Zyklenpartition von $[5]$?

Welche Basis haben die Zyklen zu
 $z_1 = (2, 5)$, $z_2 = (1)$, $z_3 = (5, 4, 3, 2, 1)$?

Antwort:

Für die Basismengen $M(\pi_{z_i})$ gelten die Gleichungen

$$M(\pi_{z_1}) = \{2, 5\},$$

$$M(\pi_{z_2}) = \{1\},$$

$$M(\pi_{z_3}) = \{1, 2, 3, 4, 5\}.$$

Geben Sie eine extensionale Darstellung der Abbildungen π_{z_i} an!

Antwort:

Es gilt mit Auflistung der Funktionswerte

$$\pi_{z_1}(2) = 5, \quad \pi_{z_1}(5) = 2.$$

$$\pi_{z_2}(1) = 1.$$

$$\pi_{z_3}(1) = 5, \quad \pi_{z_3}(2) = 1, \quad \pi_{z_3}(3) = 2, \quad \pi_{z_3}(4) = 3, \quad \pi_{z_3}(5) = 4.$$

Warum ist $Z = \{\pi_{z_1}, \pi_{z_2}, \pi_{z_3}\}$ keine Zyklenspartition von $[5]$?

Antwort:

Offenbar sind die Zyklen nicht paarweise disjunkt.

Für die Basismengen gilt z. B. $M(\pi_{z_1}) \cap M(\pi_{z_3}) \neq \emptyset$.

Sei Z eine Zyklenpartition von $[n]$. Dann ist eine bijektive Abbildung $f_Z : [n] \rightarrow [n]$ gegeben für alle $i \in [n]$ durch

$$f_Z(i) = \pi(i), \quad \text{falls } i \in M(\pi) \text{ und } \pi \in Z.$$

- 3 Zyklenpartitionen werden häufig durch eine Folge $z_1 z_2 \dots z_k$ von Zyklusdarstellungen z_i definiert, wobei die Reihenfolge der z_i in der Folge keine Rolle spielt.

Sei $Z = (4, 5, 1)(3)(2)$ eine Zyklenpartition.

Beschreiben Sie die Abbildung f_Z **extensional!**

Lösung:

Für f_Z gilt mit Auflistung der Funktionswerte

$$f_Z(1) = 4, \quad f_Z(2) = 2, \quad f_Z(3) = 3, \quad f_Z(4) = 5, \quad f_Z(5) = 1.$$

- 4 Eine Funktion f sei gegeben durch die folgende Matrixdarstellung.

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 1 & 6 & 2 & 7 & 9 & 5 & 4 & 3 \end{pmatrix}.$$

Berechnen Sie

$\{f^i(2); i \in \mathbb{N}\}$, $\{f^i(3); i \in \mathbb{N}\}$, $\{f^i(5); i \in \mathbb{N}\}$!

Bestimmen Sie eine *Zyklendarstellung* von f ,

d. h. eine *Zykluspartition* Z von $[9]$,

so dass $f(i) = f_Z(i)$ für alle $i \in [9]$ gilt!

Lösung:

Durch Auswertung von $f_Z^i(x)$ erhält man

$$\{f_Z^i(2); i \in \mathbb{N}\} = \{1, 8, 4, 2\}, \quad (1)$$

$$\{f_Z^i(3); i \in \mathbb{N}\} = \{6, 9, 3\}, \quad (2)$$

$$\{f_Z^i(5); i \in \mathbb{N}\} = \{7, 5\}. \quad (3)$$

Wir bezeichnen die Mengen in den Gleichungen (1), (2) und (3) entsprechend mit M_1 , M_2 bzw. M_3 . Dann definiert f je einen Zyklus f_i auf den Basismengen M_1 , M_2 und M_3 mit den entsprechenden Darstellungen

$$z_1 = (1, 8, 4, 2), \quad z_2 = (6, 9, 3) \quad \text{bzw.} \quad z_3 = (7, 5).$$

Zyklenpartition bzw. Zyklendarstellung von f :

$$Z = (1, 8, 4, 2) (6, 9, 3) (7, 5).$$

3.3 VA 1, Gruppen und Untergruppen

Sei $S' = \langle S, \circ \rangle$ 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 $\langle V(S), \circ_{V(S)} \rangle$ 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

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

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

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

$$\begin{aligned} a \circ x^{-1} \circ x &= x^{-1} \circ x \circ a \\ &= x^{-1} \circ a \circ x. \end{aligned}$$

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

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

- ③ Sei S' wieder eine Gruppe mit Einselement 1.
Ist $V(S)$ ein **Normalteiler** von S' ? Begründung!

Antwort: Ja!

Begründung:

Offensichtlich gilt für alle $a \in S$

$$a \circ V(S) = V(S) \circ a.$$