

WS 2011/12

Zentralübung zur Vorlesung Diskrete Strukturen (Prof. Mayr)

Dr. Werner Meixner

Fakultät für Informatik
TU München

<http://www14.in.tum.de/lehre/2011WS/ds/uebung/>

23. November 2011

ZÜ VI

Übersicht:

1. Übungsbetrieb

2. Tipps: **Neu:** Hin.Ti's für HA

3. Zusatzaufgabe: für Interessierte

4. Vorbereitung: auf TA's Blatt 6:
Abstrakte Ringe (VA1 + VA2)
Euklidischer Algorithmus (VA3)

1. Übungsbetrieb

Fragen?

2. Tipps

Neu: Zu jedem Übungsblatt wird es in Zukunft ein

Informationsblatt mit **Hin.Ti's**

geben, d. h. Hinweise und Tipps für eine erfolgreiche Lösung der Hausaufgaben.

Empfehlung:

- Versuchen Sie zunächst einige Minuten lang, ohne Hilfestellung auszukommen, und verwenden Sie die Tipps erst dann, wenn Sie nicht weiter kommen.
- Prüfen Sie abschließend, ob die Hinweise zu Ihrer Lösung passen.

Beispiel HA 1, Blatt 6:

Wahr oder falsch? Begründen Sie Ihre Antwort!

- 1 Falls F und $\neg F$ erfüllbare aussagenlogische Formeln sind, dann ist $F \wedge \neg F$ erfüllbar.
- 2 $(-13) \bmod 7 = 8$.
- 3 Es gibt eine Funktion $f(n)$ mit $n \in o(f(n))$ und $f(n) \in o(n^2)$.
- 4 Die Mathematiker Leonhard Euler und Pierre de Fermat sind sich in Paris begegnet.

Hin.Ti's ad HA 1:

- 2 Zu beachten ist der Unterschied zwischen der Operation $x \bmod 7$ und der Kongruenzrelation $x \equiv y \pmod{7}$.
- 3 Man verwende das Kriterium für $g \in o(h)$ aus TA 2.2 von Blatt 4.

3. Zusatzaufgabe für Interessierte

Wir betrachten Algebren $A = \langle S, \circ, e \rangle$ mit Einselement e , die die beidseitigen Kürzungsregeln („Sudoku-Regeln“) erfüllen, d. h., dass für alle $x, y, z \in S$ die folgenden Implikationen gelten:

$$x \circ z = y \circ z \implies x = y, \quad (1)$$

$$z \circ x = z \circ y \implies x = y. \quad (2)$$

- 1 Zeigen Sie: Falls $|S| \leq 4$ gilt, dann ist A eine Gruppe.
- 2 Sei $|S| = 5$. Geben Sie bis auf Isomorphie alle nicht assoziativen Verknüpfungen \circ mit obigen Eigenschaften an. Die entsprechenden Algebren sind dann also keine Gruppen.

Hinweis: Wählen Sie $S = \{e, a, b, c, d\}$, und betrachten Sie isomorphe Algebren als gleich.

Die besten Lösungsdarstellungen werden prämiert!!

4. Vorbereitung auf TA's Blatt 6

4.1 VA 1, Abstrakte Ringe, elementare Eigenschaften

① Man zeige:

In einem beliebigen Ring $\langle R, \oplus, \odot, 0, 1 \rangle$ gelten die folgenden Gleichungen.

$$a \odot 0 = 0 \odot a = 0, \quad a \odot b = (-a) \odot (-b).$$

Bemerkung 1: Das Inverse eines Elements x bezüglich der Operation \oplus wird mit $-x$ bezeichnet.

Bemerkung 2: Da a und b beliebige Elemente aus R sind, schreiben wir die Gleichungen ohne Allquantoren. Natürlich darf man auch $\forall a, b$ ergänzen.

Beweis:

1. Gleichung(en): $a \odot 0 = 0 \odot a = 0$.

- Es gilt

$$a \odot 0 = a \odot (0 \oplus 0) = (a \odot 0) \oplus (a \odot 0).$$

Daraus folgt mit additiver Kürzungsregel $a \odot 0 = 0$.

Da die Kommutativität der Multiplikation nicht vorausgesetzt wurde, müssen wir $0 \odot a = 0$ gesondert beweisen.

Dies folgert man aber [analog](#) wie vorhin.

2. Gleichung: $a \odot b = (-a) \odot (-b)$.

- Es gilt

$$0 = a \odot 0 = a \odot (b \oplus (-b)) = a \odot b \oplus a \odot (-b).$$

Daraus folgt $-(a \odot b) = a \odot (-b)$.

Analog folgt $-(a \odot b) = (-a) \odot b$.

Damit erhalten wir

$$(-a) \odot (-b) = -(a \odot (-b)) = -(- (a \odot b)) = a \odot b.$$

- 2 Geben Sie zwei nichtkommutative Ringe an.

Lösung:

Man nehme die Ringe der $n \times n$ -Matrizen für verschiedene $n \geq 2$.

Für die Matrixmultiplikation mit $n = 2$ gilt beispielsweise

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Was erhält man bei Rechnung modulo 2?

4.2 VA 2, Abstrakte Ringe, weitere Eigenschaften

Beweisen Sie:

- 1 Es gibt bis auf Isomorphie genau einen Ring $R = \langle S, \oplus, \odot, 0, 1 \rangle$ mit drei Elementen, d. h. $S = \{0, 1, a\}$.

Insbesondere also muss R isomorph sein zum Ring $\langle \mathbb{Z}_3, +_3, \cdot_3, 0, 1 \rangle$.

Erinnerung: Sei $R = \langle S, \oplus, \odot, 0, 1 \rangle$ ein Ring. Nach Vorlesung ist $\langle S, \oplus, 0 \rangle$ eine abelsche Gruppe mit neutralem Element 0 und $\langle S, \odot, 1 \rangle$ ist ein Monoid mit neutralem Element 1. Außerdem gelten die beidseitigen Distributivgesetze. Für Ringe mit mehr als einem Element gilt stets $1 \neq 0$. Der Ring ist kommutativ, falls die Multiplikation kommutativ ist.

Beweis:

Eine Gruppe mit 3 Elementen ist notwendigerweise zyklisch, denn die Ordnung eines Elements ungleich dem Neutralen kann, nach dem [Satz von Lagrange](#), nicht 2 sein, weil dann 2 Teiler der Gruppenordnung 3 sein müsste.

Jedes Element ungleich dem neutralen Element erzeugt die Gruppe. Die [Verknüpfungstafel für \$\oplus\$](#) lautet deshalb wie folgt.

\oplus		0	1	a
0		0	1	a
1		1	a	0
a		a	0	1

Dass diese Verknüpfungstafel eine [Gruppe](#) definiert, ergibt sich aus der [Isomorphie](#) zu $\langle \mathbb{Z}_3, +_3 \rangle$.

Auch die **Verknüpfungstafel** für die Multiplikation ergibt sich zwingend wegen

$$a \odot a = (1 \oplus 1) \odot (1 \oplus 1) = 1 \oplus 1 \oplus 1 \oplus 1 = 1$$

wie folgt:

\odot	0	1	a
0	0	0	0
1	0	1	a
a	0	a	1

Dass **alle** Ringaxiome erfüllt sind, zeigt man wiederum mithilfe der **Isomorphie** auf den Ring $\langle \mathbb{Z}_3, +_3, \cdot_3, 0, 1 \rangle$.

Es folgt, dass R ein Ring ist.

Die Eindeutigkeit von R ist eine Konsequenz der Herleitung, denn die Verknüpfungstafeln hatten sich zwingend ergeben.

- 2 Der Ring $R = \langle S, \oplus, \odot, 0, 1 \rangle$ mit drei Elementen ist ein Körper.

Beweis:

R ist genau dann ein Körper, wenn $\langle S \setminus \{0\}, \odot, 1 \rangle$ eine kommutative Gruppe ist.

Zum Beweis genügt der Hinweis auf die Isomorphie mit $\langle \mathbb{Z}_3, +_3, \cdot_3, 0, 1 \rangle$, weil $\langle \mathbb{Z}_n, +_n, \cdot_n, 0, 1 \rangle$ bekanntlich ein Körper ist, wenn n eine Primzahl ist.

Wir geben aber auch einen direkten Beweis an, wie folgt.

Direkter Beweis:

Wir streichen aus der Verknüpfungstafel die Zeile bzw. Spalte der Multiplikation mit 0 und erhalten.

$$\begin{array}{c|cc} \odot & 1 & a \\ \hline 1 & 1 & a \\ a & a & 1 \end{array}$$

Offenbar definiert die Multiplikation eine Gruppe.
Sie ist isomorph zu $\langle \mathbb{Z}_2, +_2 \rangle$.

Definition:

Es heie $y \in S \setminus \{0\}$ **co-Nullteiler** von $x \in S \setminus \{0\}$, falls $x \odot y = 0$.

Beispiel: In \mathbb{Z}_8 sind $2, 4, 6$ co-Nullteiler von 4 .

- 3 Sei t_x die Anzahl der co-Nullteiler eines Ringelementes $x \in S \setminus \{0\}$ eines endlichen, kommutativen Ringes $\langle S, \oplus, \odot, 0, 1 \rangle$.

Dann ist $t_x + 1$ ein **Teiler** der Anzahl $n = |S|$ aller Ringelemente.

Beweis:

Sei $N_x = \{y \in S \setminus \{0\} ; x \odot y = 0\}$.

Wir zeigen, dass $N_x \cup \{0\}$ eine **additive Untergruppe** von $\langle S, \oplus \rangle$ bildet.

- Es gilt offensichtlich $0 \in N_x \cup \{0\}$.
- Abgeschlossenheit: Seien $y, z \in N_x \cup \{0\}$.
Dann gilt $x \odot (y \oplus z) = x \odot y \oplus x \odot z = 0$, d. h.
 $y \oplus z \in N_x \cup \{0\}$.
- Inverse sind enthalten: Sei $y \in N_x \cup \{0\}$.
Dann gilt $x \odot (-y) = -x \odot y = 0$, d. h. $-y \in N_x \cup \{0\}$.

Da $N_x \cup \{0\}$ eine additive Untergruppe von $\langle S, \oplus \rangle$ ist,
gilt nach dem Satz von Lagrange,
dass $t_x + 1 = |N_x \cup \{0\}|$ ein **Teiler** von $|S|$ ist,
w.z.b.w.

Bemerkung:

Die Konsequenz der Aussage in dieser Teilaufgabe ist, dass
jeder endliche kommutative Ring,
dessen Anzahl von Elementen eine Primzahl ist,
notwendigerweise auch ein **Körper** ist!

4.3 VA 3, Euklidischer Algorithmus

In gewissen kommutativen Ringen $R = \langle S, +, \cdot, 0, 1 \rangle$ stellt sich der erweiterte Euklidische Algorithmus zur Berechnung des größten gemeinsamen Teilers $\text{ggT}(a, b)$ zweier Elemente $a \in S$ und $b \in S$ dar als eine iterierte Transformation (Matrixmultiplikation) Q_i angewandt auf Δ_{i-1} wie folgt mit $r_0 = a$ und $r_1 = b$.

$$\Delta_0 = \begin{pmatrix} a \\ b \end{pmatrix},$$

$$\Delta_i = \begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix} = Q_i \Delta_{i-1} = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \begin{pmatrix} r_{i-1} \\ r_i \end{pmatrix},$$

für alle $i := 1, 2, \dots, n \in \mathbb{N}$.

Dabei werden die Quotienten q_i so gewählt (geschätzt), dass die Δ_i mit wachsendem i in einem gewissen Sinn stets echt kleiner werden.

Eine Berechnung wird beendet, wenn die Folge der Δ_i maximale Länge besitzt, d. h. wenn kein Quotient existiert, der die Bildung eines noch kleineren Restes erlaubt.

Zur Bemessung der Größe von Elementen eines Ringes dient beispielweise im Ring der ganzen Zahlen $\langle \mathbb{Z}, +, \cdot, 0, 1 \rangle$ die Betragsfunktion. In Polynomringen wird der Grad eines Polynoms verwendet.

Wir betrachten im Folgenden den Ring $\langle \mathbb{Z}, +, \cdot, 0, 1 \rangle$ der **ganzen Zahlen**.

- 1 Zeigen Sie für alle entsprechenden i

$$\text{ggT}(a, b) = \text{ggT}(r_i, r_{i+1}).$$

Beweis:

Gemeinsame Teiler zweier Ringelemente r_{i-1}, r_i übertragen sich auf deren Linearkombination $sr_{i-1} + tr_i$ wie folgt:

Falls x Teiler von r_{i-1} und von r_i , i. Z. $x|r_{i-1} \wedge x|r_i$, dann gilt für gewisse Faktoren $h, k \in R$

$$sr_{i-1} + tr_i = sxh + txk = (sh + tk)x,$$

mithin $x|(sr_{i-1} + tr_i)$.

Die Matrixmultiplikation liefert eine Linearkombination wie folgt.

$$\Delta_i = \begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix} = \begin{pmatrix} r_i \\ r_{i-1} - q_i r_i \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \begin{pmatrix} r_{i-1} \\ r_i \end{pmatrix}.$$

Da die Matrix $Q_i = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix}$ invertierbar ist mit

$$Q_i^{-1} = \begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix},$$

haben die Komponentenpaare der Δ_i für alle i die gleichen Teiler.
w.z.b.w.

- 1 Berechnen Sie mit dem Euklidischen Algorithmus den $\text{ggT}(10800, 122)$.

Berechnung:

Wir rechnen im Ring der ganzen Zahlen.

Im Euklidischen Algorithmus für den Ring ganzer Zahlen zur Berechnung des $\text{ggT}(a, b)$ werden die Quotienten q_i durch ganzzahlige Division bestimmt.

$$q_i = r_{i-1} \text{ div } r_i .$$

Abweichend davon könnte man aber auch grob schätzen.

Für die Linearkombination $r_{i+1} = r_{i-1} - q_i r_i$ folgt dann

$$r_{i+1} = r_{i-1} \bmod r_i .$$

Die Berechnung wird beendet, wenn $r_{n+1} = 0$ eintritt für irgendein $n \in \mathbb{N}$.

Berechnung (Fortsetzung):

$$r_0 = 10800,$$

$$r_1 = 122,$$

$$r_2 = 10800 \bmod 122 = 64,$$

$$r_3 = 122 \bmod 64 = 58,$$

$$r_4 = 64 \bmod 58 = 6,$$

$$r_5 = 58 \bmod 6 = 4,$$

$$r_6 = 6 \bmod 4 = 2,$$

$$r_7 = 4 \bmod 2 = 0.$$

Ergebnis: $\text{ggT}(10800, 122) = r_6 = 2.$

Ein äußerst wichtiger nächster Schritt besteht darin, den größten gemeinsamen Teiler r_6 von a und b als Linearkombination von $a = r_0$ und $b = r_1$ zu bestimmen.

Dies geschieht mit dem *erweiterten Euklidischen Algorithmus* wie folgt.

Der erweiterte Euklidische Algorithmus lässt sich als Matrixmultiplikation wie folgt darstellen:

$$\begin{pmatrix} r_n \\ r_{n+1} \end{pmatrix} = Q_n \cdot Q_{n-1} \cdot \dots \cdot Q_2 \cdot Q_1 \cdot \begin{pmatrix} a \\ b \end{pmatrix}.$$

Mit

$$P_0 := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

$$P_k := \prod_{i=1}^k Q_i, \quad k = 1, \dots, n$$

(wir definieren hier $\prod_{i=1}^j Q_i = Q_j \cdot \prod_{i=1}^{j-1} Q_i$)

erhält man r_n, r_{n+1} als Linearkombination von a, b
wie folgt für alle $n \in \mathbb{N}_0$

$$\begin{pmatrix} r_n \\ r_{n+1} \end{pmatrix} = P_n \cdot \begin{pmatrix} a \\ b \end{pmatrix}.$$

Die Matrizen P_k enthalten die Koeffizienten der jeweiligen Linearkombinationen. Man berechnet diese Koeffizienten gleichzeitig mit den r_k durch sukzessive Berechnung von

$$P_k = Q_k \cdot P_{k-1} = \begin{pmatrix} 0 & 1 \\ 1 & -q_k \end{pmatrix} \cdot \begin{pmatrix} m_{k-1} & n_{k-1} \\ m_k & n_k \end{pmatrix}.$$

Es gelten die folgenden Gleichungen.

$$\begin{aligned} q_k &= r_{k-1} \operatorname{div} r_k, \\ r_{k+1} &= r_{k-1} \bmod r_k, \\ m_{k+1} &= m_{k-1} - q_k \cdot m_k, \\ n_{k+1} &= n_{k-1} - q_k \cdot n_k, \\ r_k &= m_k \cdot a + n_k \cdot b. \end{aligned}$$

Wir führen die Auswertung der Formeln von Hand aus mit Buchführung in einer Tabelle.

k	r_{k-1}	r_k	q_k	m_{k-1}	m_k	n_{k-1}	n_k
$k = 1$	10800	122	88	1	0	0	1
$k = 2$	122	64	1		1		-88
$k = 3$	64	58	1		-1		89
$k = 4$	58	6	9		2		-177
$k = 5$	6	4	1		-19		1682
$k = 6$	4	2	2		21		-1859
$k = 7$	2	0			-61		5400

Ergebnis:

$$m_6 \cdot a + n_6 \cdot b = 21 \cdot 10800 + (-1859) \cdot 122 = 2.$$