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/

8. Dezember 2010

ZÜ VII

Übersicht:

1. Übungsbetrieb:	Klausur am 11.12.10 Beginn, Ausweise
2. Thema:	Nachtrag TA 3.3, Blatt 6.
3. Hausaufgaben	Besprechung HA Blatt 8:

1. Übungsbetrieb

1.1 Beginn

Beginn der Prüfung ist 9.00 Uhr.

Bitte 15 Minuten vor Beginn erscheinen und Platz suchen.

Bei Nichtanmeldung: Bitte im Hörsaal bei der Aufsicht melden!
Dann wird Ihnen kurz vor 9.00 Uhr ein Platz zugewiesen.

1.2 Ausweise

Ausweise mitbringen!

Es werden die Ausweise kontrolliert:

Studentenausweis + (ev.) Lichtbildausweis.

2. Thema:

In den meisten Übungsgruppen blieb wenig Zeit für TA 3.3, Blatt 6. Deshalb holen wir heute diese Besprechung nach.

2.1 Nachtrag TA 3.3, Blatt 6

Zeigen Sie, dass im Folgenden Algebren $A = \langle S, \circ \rangle$ definiert werden, die bezüglich des binären Operators $\circ$ eine Gruppe bilden.

3. Sei $1 < n \in \mathbb{N}$ und $S = \mathbb{Z}_n^* = \{p \in \mathbb{Z}_n;\ \mathrm{ggT}(p, n) = 1\}$.
   $\circ$ sei gleich der Multiplikation ganzer Zahlen modulo n.

Beweis:

- Abgeschlossenheit:

  Zunächst ist zu zeigen, dass das Produkt $p \circ q$ zweier Elemente $p, q \in \mathbb{Z}_n^*$ wieder in $\mathbb{Z}_n^*$ liegt.

  Es ist also zu zeigen

  $$\mathrm{ggT}(p, n) = 1 \wedge \mathrm{ggT}(q, n) = 1 \implies \mathrm{ggT}((p \cdot q) \bmod n, n) = 1\,.$$

  Da $\mathrm{ggT}(p \cdot q, n) = 1$ gleichbedeutend ist mit
  $\mathrm{ggT}((p \cdot q) \bmod n, n) = 1$,
  genügt es, die folgende Implikation zu zeigen.

  $$\mathrm{ggT}(p, n) = 1 \ \wedge \ \mathrm{ggT}(q, n) = 1 \implies \mathrm{ggT}(p \cdot q, n) = 1\,,$$

Die folgende Überlegung ist elementar.

Falls $x = \mathrm{ggT}(p \cdot q, n)$,
d. h. falls $x|(p \cdot q)$ und $x|n$,

dann gilt $x = x_1 \cdot x_2$ mit $x_1|p$ und $x_2|q$,
und natürlich $x_1|n$, $x_2|n$.

Da p und q zu n teilerfremd sind, folgt $x_1 = 1$, $x_2 = 1$,
mithin $x = 1$.

Damit muss $\mathrm{ggT}(p \cdot q, n) = 1$ gelten.

- Assoziativität von $\circ$:

  Die Assoziativität von $\circ$ ist nichts anderes als die Assoziativität der Multiplikation modulo n.

  Diese wir von der Assoziativität der Multiplikation der ganzen Zahlen geerbt.

- A enthält 1 als ein neutrales Element bezgl. $\circ$.

- Existenz des Inversen von x:

  Gesetzt den Fall wir hätten ein x und ein y, welche die Gleichung

  $$x \cdot p + y \cdot n = 1$$

  erfüllen.

  Dann wäre $x \bmod n$ das Inverse zu p,
  denn aus $x \cdot p + y \cdot n = 1$ folgt offenbar

  $$((x \bmod n) \cdot p) \bmod n = (x \bmod n) \cdot_n p = 1\,,$$

  wobei klar ist, dass $\mathrm{ggT}(x, n) = 1$ und damit
  $\mathrm{ggT}(x \bmod n, n) = 1$, d. h. $x \bmod n \in \mathbb{Z}_n^*$.

Die Existenz des Inversen für ein $p \in \mathbb{Z}_n^*$ folgt also aus

$$(\exists x, y \in \mathbb{Z})\ [\, x \cdot p + y \cdot n = 1 \,],$$

was aber eine Konsequenz aus $\mathrm{ggT}(p, n) = 1$ ist, wie folgendermaßen gezeigt wird.

Sei $U = \{xp + yn\,;\, x, y \in \mathbb{Z}\}$.

Offenbar ist U eine Untergruppe von $\mathbb{Z}$,
d. h. $U = k \cdot \mathbb{Z}$ für ein bestimmtes $k \in \mathbb{N}$.

Daraus folgt aber, dass sowohl p als auch n Vielfache von k sind.

Also gilt $k \,|\, \mathrm{ggT}(p, n)$.

Es folgt $k = 1$.

Mithin ist $1 \in U$, d. h. $1 = xp + yn$ für bestimmte $x, y \in \mathbb{Z}$.

3. Hausaufgaben Besprechung Blatt 8

Wir beginnen mit HA 4, weil wir damit einen zweiten Beweis der Aussage über die Existenz von Inversen in $\mathbb{Z}_n^*$ behandeln.

3.1 HA 4

Berechnen Sie mit Hilfe des erweiterten Euklidschen Algorithmus ganze Zahlen a, b, so dass

$$a \cdot 53 + b \cdot 36 = 2\,.$$

Berechnung:

Wir führen den Euklidschen Algorithmus wie folgt aus.

$$
\begin{aligned}
r_0 &= 53\,, \\
r_1 &= 36\,, \\
r_2 &= 53 \bmod 36 &&= r_0 - 1 \cdot r_1 &&= 17\,, \\
r_3 &= 36 \bmod 17 &&= r_1 - 2 \cdot r_2 &&= 2\,, \\
r_4 &= 17 \bmod 2 &&= r_2 - 8 \cdot r_3 &&= 1\,.
\end{aligned}
$$

Es folgt $\mathrm{ggT}(53, 36) = 1$.

Nun führen wir den erweiterten Euklidschen Algorithmus in der Form der Rückeinsetzung aus.

$$
\begin{aligned}
1 &= r_4 \\
&= r_2 - 8r_3 && = r_2 - 8(r_1 - 2r_2) \\
&= -8r_1 + 17r_2 && = -8r_1 + 17(r_0 - r_1) \\
&= 17r_0 - 25r_1 \,.
\end{aligned}
$$

Es folgt $17r_0 - 25r_1 = 1$,
mithin,
für $a = 34$ und $b = -50$,

$$a \cdot 53 + b \cdot 36 = 2 \,.$$

3.2 HA 1

1. Berechnen Sie $(10^{117} + 5^{27} - 30^{1000}) \bmod 3$.
2. Bestimmen Sie $2^{7333333100} \bmod 12$.

1. Berechnung von $(10^{117} + 5^{27} - 30^{1000}) \bmod 3$:

Wir erhalten

$$
\begin{aligned}
&(10^{117}+5^{27}-30^{1000}) \bmod 3 \\
&\quad = \quad [(10 \bmod 3)^{117}+5 \cdot (5^2 \bmod 3)^{13}-(30 \bmod 3)^{1000}] \bmod 3 \\
&\quad = \quad [\,1^{117} + 5 \cdot 1^{13} - 0^{1000}\,] \bmod 3 \\
&\quad = \quad (1+5) \bmod 3 \;=\; 0\,.
\end{aligned}
$$

2. Bestimmung von $2^{7333333100} \bmod 12$:

Notwendigerweise müssen sich die Potenzen 2^k modulo 12 wiederholen (Schubfachprinzip).

Man rechnet z. B. sofort $2^2 \equiv 2^4 (\mathrm{mod}\, 12)$.

Entsprechend gilt für alle $k \geq 0$

$$2^{2+2k} \equiv 2^2 (\mathrm{mod}\, 12)\,,$$

d.h. für positive geradzahlige Potenzen n von 2

$$2^n \equiv 2^2 (\mathrm{mod}\, 12)\,.$$

Mithin folgt

$$2^{7346790100} \bmod 12 \;=\; 2^2 \bmod 12 = \; 4\,.$$

3.3 HA 2

Die Menge der Permutationen der Teilmenge $\{1, 2, 3, 4\}$ der natürlichen Zahlen bildet zusammen mit der Komposition $\circ$ von Abbildungen die Gruppe $\mathcal{S}_4$. Das neutrale Element der Gruppe sei id. Wir betrachten die in Zyklusschreibweise gegebenen Permutationen

$$p = (1\ 2)(3)(4) \qquad \text{und} \qquad q = (1)(2)(3\ 4)\,.$$

1. f heißt involutorisch, falls $f \circ f = id$ gilt.
   Zeigen Sie, dass p und q involutorisch sind.

Beweis:

$$(p \circ p)(1) = p(p(1)) = p(2) = 1,$$
$$(p \circ p)(2) = p(p(2)) = p(1) = 2,$$
$$(p \circ p)(3) = p(p(3)) = p(3) = 3,$$
$$(p \circ p)(4) = p(p(4)) = p(4) = 4.$$

Analog für $q \circ q$.

2. Zeigen Sie, dass $p \circ q = q \circ p$ gilt.

Beweis:

$$p \circ q = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \quad q \circ p = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

Daraus folgt $p \circ q = q \circ p$.

3. Seien $r = p \circ q$ und $U = \{id, p, q, r\}$.
   Geben Sie die $\circ$-Verknüpfungstafel für die Elemente aus U an.

Lösung:

$\circ$	id	p	q	r
id	id	p	q	r
p	p	id	r	q
q	q	r	id	p
r	r	q	p	id

4. Seien $r = p \circ q$ und $U = \{id, p, q, r\}$.
   Beweisen Sie, dass die Menge U mit jedem Element $x \in U$ auch sein Inverses x^{-1} enthält (mit $x \circ x^{-1} = id$).

Lösung:

Für jedes Element $x \in U$ gilt $x^2 = id$. Damit ist jedes Element zu sich selbst invers.

3.4 HA 3

Wir betrachten Algebren $A = \langle S, \circ \rangle$ mit einer 2-elementigen Trägermenge $S = \{a, b\}$ und einem 2-stelligen Operator $\circ$. Bekanntlich gibt es 16 verschiedene Algebren dieser Art, auf die wir uns im Folgenden beziehen.

1. Geben Sie eine Verknüpfungstafel für einen nicht assoziativen und gleichzeitig nicht kommutativen Operator $\circ$ an.

Lösung:

Ansatz: Die Assoziativität ist verletzt, falls beispielsweise $a \circ (a \circ a) \neq (a \circ a) \circ a$ gilt.

Um dies zu erreichen kann nicht $a \circ a = a$ definiert werden, weil in diesem Fall $a \circ (a \circ a) = (a \circ a) \circ a$ gelten würde.

Wir versuchen den Ansatz $a \circ a = b$.

Dann müssen wir $a \circ b \neq b \circ a$ setzen.

Wir erhalten folgenden
nicht kommutativen und nicht assoziativen Verknüpfungstafel

$\circ$	a	b
a	b	a
b	b	a

2. Zeigen Sie, dass es genau zwei kommutative und gleichzeitig nicht assoziative Operatoren $\circ$ gibt.

Lösung:

Im kommutativen Fall gelten stets die Gleichungen

$a \circ (a \circ a) = (a \circ a) \circ a$, $b \circ (b \circ b) = (b \circ b) \circ b$,

$a \circ (b \circ a) = (a \circ b) \circ a$ und $b \circ (a \circ b) = (b \circ a) \circ b$.

Wenn dann noch

$a \circ (a \circ b) = (a \circ a) \circ b$ und $a \circ (b \circ b) = (a \circ b) \circ b$ gelten würde,

dann wäre $\circ$ sogar assoziativ.

Wir zeigen:

$a \circ a = a$ impliziert
$a \circ (a \circ b) = (a \circ a) \circ b$ und $a \circ (b \circ b) = (a \circ b) \circ b$

wie folgt:

Fall 1, $b \circ b = b$ und $a \circ b = a$:

Dann gilt

$a \circ (a \circ b) = a \circ a = a = a \circ b = (a \circ a) \circ b$ und

$a \circ (b \circ b) = a \circ b = (a \circ b) \circ b$.

Fall 2, $b \circ b = b$ und $a \circ b = b$:

Dann gilt

$a \circ (a \circ b) = a \circ a = (a \circ a) \circ b$ und

$a \circ (b \circ b) = a \circ b = b = b \circ b = (a \circ b) \circ b$.

Fall 3, $b \circ b = a$ und $a \circ b = a$:

Dann gilt

$a \circ (a \circ b) = a \circ a = a = a \circ b = (a \circ a) \circ b$ und

$a \circ (b \circ b) = a \circ a = a = a \circ b = (a \circ b) \circ b$.

Fall 4, $b \circ b = a$ und $a \circ b = b$:

Dann gilt

$a \circ (a \circ b) = a \circ b = (a \circ a) \circ b$ und

$a \circ (b \circ b) = a \circ a = a = b \circ b = (a \circ b) \circ b$.

Analog folgt:

$b \circ b = b$ impliziert
$a \circ (a \circ b) = (a \circ a) \circ b$ und $a \circ (b \circ b) = (a \circ b) \circ b$.

Wenn die Operation $\circ$ also nicht assoziativ sein soll, müssen wir $a \circ a = b$ und $b \circ b = a$ setzen

und wir erhalten die folgenden beiden Verknüpfungstafeln.

$\circ$	a	b
a	b	a
b	a	a

$\circ$	a	b
a	b	b
b	b	a

3. Geben Sie alle Booleschen Operatoren an, die kommutativ und gleichzeitig nicht assoziativ sind.

Lösung:

Wir haben gezeigt, dass es nur die beiden obigen Operationen geben kann, wenn wir $a = 0$ und $b = 1$ (oder umgekehrt) setzen.

Wir erhalten also die booleschen Operationen

NOR	0	1
0	1	0
1	0	0

NAND	0	1
0	1	1
1	1	0