WS 2009/10

Diskrete Strukturen

Dr. Werner Meixner

Fakultät für Informatik
TU München

http://www14.in.tum.de/lehre/2009WS/ds/uebung/

05. Februar 2010

ZÜ XIII Blatt 13, VA1 bis VA3

1. Blatt 13, VA 1

Im Folgenden nehmen wir 0 bzw. 1 als die entsprechenden neutralen Elemente bezüglich $\oplus$ bzw. $\odot$ in die Signatur von Ringen mit auf.
Man zeige:

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

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

Bemerkung:
In Ringen müssen wir zwischen
Inversen bezüglich der sogenannten „Addition“ und
Inversen bezüglich der sogenannten „Multiplikation“ unterscheiden.

Das Inverse von x bezüglich der „Addition“, hier also $\oplus$,
bezeichnen wir durch $-x$,

das Inverse von x bezüglich der „Multiplikation“, hier also $\odot$,
bezeichnen wir durch x^{-1}.

Für das Weglassen von Klammern übernehmen wir die übliche
Regel, dass die Multiplikation stärker bindet als die Addition.

Beweis:

- Es gilt $a \odot 0 = a \odot (0 \oplus 0) = a \odot 0 \oplus a \odot 0$.
  Daraus folgt $a \odot 0 = 0$.

  Da die Kommutativität der Multiplikation nicht vorausgesetzt wurde, müssen wir $0 \odot a = 0$ gesondert beweisen. Dies folgert man aber analog wie vorhin.

- 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 2 nicht-kommutative Ringe an.

Antwort:

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

Für die Matrixmultiplikation gilt beispielsweise

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

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

2. Blatt 13, VA 2

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 $\langle \mathbb{Z}_3, +_3, \cdot_3, 0, 1 \rangle$.

Beweis:

Nach Vorlesung ist $\langle S, \oplus \rangle$ eine abelsche Gruppe
mit neutralem Element 0
und $\langle S, \odot \rangle$ 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.

Bemerkung:
Man könnte von der Tatsache ausgehen, dass es bis auf Isomorphie nur eine einzige 3-elementige Gruppe gibt, und diese ist $\langle \mathbb{Z}_3, +_3 \rangle$.

Wir wollen aber direkt argumentieren, d. h. explizit die Operationen $\oplus$ und $\odot$ wie folgt herleiten.

- Es gilt $1 \oplus a = 0$:
  Aus $1 \oplus a = a$ würde, wegen $0 \oplus a = a$, mit Kürzungsregel $1 = 0$ folgen. Widerspruch!
  Aus $1 \oplus a = 1$ würde sofort $a = 0$ folgen. Widerspruch!
  Also bleibt nur $1 \oplus a = 0$.
- Es gilt $1 \oplus 1 = a$:
  Aus $1 \oplus 1 = 0$ würde, wegen $1 \oplus a = 0$, mit Kürzungsregel $1 = a$ folgen. Widerspruch!
  Aus $1 \oplus 1 = 1$ würde sofort $1 = 0$ folgen. Widerspruch!
  Also bleibt nur $1 \oplus 1 = a$.
- Es gilt $a \oplus a = 1$:
  Aus $a \oplus a = 0$ würde, wegen $1 \oplus a = 0$, mit Kürzungsregel $a = 1$ folgen. Widerspruch!
  Aus $a \oplus a = a$ würde sofort $a = 0$ folgen. Widerspruch!
  Also bleibt nur $a \oplus a = 1$.

Wir fassen zusammen

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

Dass diese Verknüpfungstafel eine Gruppe definiert, muss aber noch bewiesen werden!

Um nicht die Gruppengesetze mühsam einzeln nachweisen zu müssen, definiert man eine Abbildung $h : S \to \mathbb{Z}_3$ durch

$$h(0) = 0,\ h(1) = 1,\ h(a) = 2\,.$$

Offenbar ist h eine isomorphe Abbildung der Algebra $\langle S, \oplus \rangle$ auf die Gruppe $\langle \mathbb{Z}_3, +_3 \rangle$.
Daraus folgt, dass $\langle S, \oplus \rangle$ eine Gruppe ist.

Auch die Verknüpfungstafel für die Multiplikation ergibt sich zwingend.

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

Z. B. rechnet man $a \odot a$ wie folgt aus:

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

Dass alle Ringaxiome erfüllt sind, zeigt man wiederum mithilfe der obigen Abbildung h.

Natürlich sieht man sofort, dass h auch bezüglich der Multiplikation eine Isomorphie ist, und zwar von $\langle S, \odot \rangle$ auf $\langle \mathbb{Z}_3, \cdot_3 \rangle$.

Insgesamt definiert h also eine
isomorphe Abbildung der Algebra R auf den Ring $\langle \mathbb{Z}_3, +_3, \cdot_3, 0, 1 \rangle$.

Es folgt, dass R ein Ring ist.
Die Eindeutigkeit ist eine Konsequenz der Herleitung.

Beweisen Sie:

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 $\langle S \setminus \{0\}, \odot \rangle$ eine kommutative Gruppe ist.

Man könnte den Beweis durch Hinweis
auf die Isomorphie mit $\langle \mathbb{Z}_3, +_3, \cdot_3, 0, 1 \rangle$ führen,
weil $\langle \mathbb{Z}_3, +_3, \cdot_3, 0, 1 \rangle$ bekanntlich ein Körper ist.

Aber wir führen den Beweis direkt wie folgt.

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

$\odot$	1	a
1	1	a
a	a	1

Offenbar definiert die Multiplikation eine kommutative Gruppe.

Sie ist isomorph zu $\langle \mathbb{Z}_2, +_2 \rangle$.

Beweisen Sie:

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 $t_x \oplus 1$ ein Teiler der Anzahl $n = |S|$ aller Ringelemente.

   Dabei heiße $y \in S \setminus \{0\}$ co-Nullteiler von $x \in S \setminus \{0\}$, falls $x \odot y = 0$.

Beweis:

Sei $N_x = \{y \in S \setminus \{0\} \mid x \odot y = 0\}$.
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 $x \odot (y \oplus z) = x \odot z \oplus x \odot y = 0$, 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.

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

3. Blatt 13, VA 3

Mit $R = \mathbb{Z}_3[x]$ bezeichnen wir den Ring aller Polynome über einer Variablen (*Unbestimmten*) x mit Koeffizienten aus dem Körper $\langle \mathbb{Z}_3, +_3, \cdot_3 \rangle$ der ganzen Zahlen modulo 3.
Seien $a(x), b(x) \in R$ gegeben durch

$$\begin{aligned} a(x) &= x^6 + 2x^4 + 2x^3 + x^2 + 1\,, \\ b(x) &= x^3 + x^2 + 1\,. \end{aligned}$$

1. Bestimmen Sie Polynome $r_2(x), r_3(x), q_1(x), q_2(x) \in R$ mit $\mathrm{grad}(r_3(x)) < \mathrm{grad}(r_2(x)) < \mathrm{grad}(b(x))$, so dass die folgenden Gleichungen gelten.

$$\begin{aligned} r_2(x) &= a(x) - q_1(x) \cdot b(x)\,, \\ r_3(x) &= b(x) - q_2(x) \cdot r_2(x)\,. \end{aligned}$$

Beweis:

$q_1(x)$ erhält man durch
Division von $a(x)$ durch $b(x)$ mit Rest $r_2(x)$.

Entsprechend erhält man $q_2(x)$ durch Division von $b(x)$ durch $r_2(x)$ mit Rest $r_3(x)$.

$$
\begin{aligned}
q_1(x) &= x^3 + 2x^2 + 1\,, \\
r_2(x) &= x^2\,, \\
q_2(x) &= x + 1\,, \\
r_3(x) &= 1\,.
\end{aligned}
$$

2. Bestimmen Sie ein Polynom $t(x) \in R$ möglichst hohen Grades, das ein gemeinsamer Teiler von $a(x)$ und $b(x)$ ist.

Beweis:

Gesucht ist also der größte gemeinsame Teiler von $a(x)$ und $b(x)$.

Es gilt: $t(x) = r_3(x) = 1$ ist das gesuchte Polynom.

Begründung:
$b(x)$ ist nicht durch $r_2(x)$ ohne Rest teilbar.
Aber $r_2(x)$ ist ohne Rest durch $r_3(x) = 1$ teilbar.
(Euklidscher Algorithmus)

3. Wir betrachten den Ring $R_{b(x)} = \mathbb{Z}_3[x]_{b(x)}$ der Polynome aus R modulo $b(x)$.

   Zeigen Sie $x^8 \equiv 1 \pmod{b(x)}$.

   Geben Sie in $R_{b(x)}$ das inverse Element zu x^2 an.

Beweis:

Entweder wir bestimmen den Rest der Division von x^8 durch $x^3 + x^2 + 1$ oder wir versuchen einen schnelleren Weg wie folgt.

$$\begin{aligned}
(x^2)^2 &\equiv [x^4 - x(x^3 + x^2 + 1)] \pmod{b(x)}, \\
&\equiv [(-x^3 - x) + (x^3 + x^2 + 1)] \pmod{b(x)}. \\
&\equiv (x^2 + 2x + 1) \pmod{b(x)}. \\
((x^2)^2)^2 &\equiv [(x^2 + 2x + 1)^2 - x(x^3 + x^2 + 1)] \pmod{b(x)} \\
&\equiv 1 \pmod{b(x)}.
\end{aligned}$$

Das Inverse von x^2 ist $x^6 \bmod b(x)$.