Technische Universität München
Fakultät für Informatik
Lehrstuhl für Informatik 15
Computergraphik & Visualisierung
Prof. Dr. Rüdiger Westermann
Dr. Werner Meixner

Wintersemester 2007/08
Lösungsblatt 12
31. Januar 2008

Diskrete Strukturen

Hausaufgabe 1 (5 Punkte)

Wir betrachten die Menge $S = \mathbb{R} \setminus \{1\}$ und definieren eine Abbildung $\diamond$ für alle $x, y \in S$ mit

$$x \diamond y = x + y - xy.$$

Zeigen Sie, dass durch $A = \langle S, \diamond \rangle$ eine Gruppe definiert ist.

Lösungsvorschlag

Die Lösung ist völlig analog zur Lösung von Vorbereitungsaufgabe 3.1 von Blatt 11.

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

   Seien $x, y \in \mathbb{R} \setminus \{1\}$. Es gilt offenbar $x \diamond y \in \mathbb{R}$, denn wir können 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 $\diamond$.

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

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

$$0 \diamond y = 0 + y - 0 \cdot y = y\,.$$

   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

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

   Die Existenz eines rechten inversen Elementes, mithin eines inversen Elementes ist damit bewiesen.

   Allein schon aus der offensichtlichen Kommutativität folgt hier, dass jedes rechte auch linkes Inverses ist. Es sei aber bemerkt, dass die Beziehung zwischen linken und rechten Inversen auch ohne Kommutativität ganz allgemein in Gruppen untersucht werden kann. Es genügt, allein die Existenz des rechten Inversen nachzuweisen.

Damit ist der Nachweis erbracht, dass G eine Gruppe ist.

Hausaufgabe 2 (5 Punkte)

Sei $G = \langle S, \circ \rangle$ eine Gruppe, die ein Element $a \in S$ endlicher Ordnung enthält.

1. Zeigen Sie, dass es ein k gibt, so dass $a^{-1} = a^k$ gilt.
2. Wir schreiben $\mathrm{ord}(x)$ für die Ordnung eines Elementes x. Welche Beziehung besteht zwischen $\mathrm{ord}(a)$ und $\mathrm{ord}(a^{-1})$?
3. Zeigen Sie, dass G nicht notwendigerweise eine endliche Ordnung besitzt.

Lösungsvorschlag

Im Folgenden bezeichnen wir das neutrale Element von G mit e.

1. Sei $k = \mathrm{ord}(a) > 0$. Falls $k = 1$, dann gilt $a^1 = e$ und trivialerweise $a^{-1} = e$.

   Allgemein gilt für $k > 0$: $\quad a \circ a^{k-1} = a^k = e$. Es folgt $a^{-1} = a^{k-1}$.

   Man beachte, dass $a^0 = e$ definiert wurde.

2. Falls a von endlicher Ordnung $\mathrm{ord}(a) = n$ ist, dann gilt für das Inverse $b = a^{-1}$ von a

$$b^n = (a^{-1})^n = (a^{n-1})^n = (a^n)^{n-1} = e^{n-1} = e\,,$$

   d. h. auch b besitzt endliche Ordnung $\mathrm{ord}(b) = m$ und es folgt $m \leq n$.

   Andererseits ist a das Inverse von b, weshalb auch $n \leq m$ gelten muss. Es folgt $n = m$.

3. In jeder Gruppe ist das neutrale Element e von endlicher Ordnung, denn es gilt $\mathrm{ord}(e) = 1$. Die additive Gruppe $\mathbb{Z}$ der ganzen Zahlen enthält unendlich viele Elemente, d. h. $\mathrm{ord}(\mathbb{Z}) = \infty$. Mit $G = \mathbb{Z}$ ist also die Aussage bewiesen.

Hausaufgabe 3 (5 Punkte)

Geben Sie alle Untergruppen der folgenden Gruppen an.

1. $\langle \mathbb{Z}_{12}, +_{12} \rangle$.
2. $\langle \mathbb{Z}, + \rangle$.

Welche der betrachteten Untergruppen sind zyklisch? Begründung!

Lösungsvorschlag

Vorab stellen wir fest, dass in jeder Gruppe $G = \langle S, \circ \rangle$ mit neutralem Element e die einelementige Menge $\{e\}$ eine zyklische Untergruppe bildet. Diese triviale Untergruppe werden wir im folgenden nicht mehr nennen.
Es gilt, dass jede Untergruppe einer zyklischen Gruppe selbst zyklisch ist. Da nun $\mathbb{Z}_{12}$ und $\mathbb{Z}$ zyklische Gruppen sind, genügt es also, zyklische Untergruppen zu betrachten.

1. In endlichen Gruppen ist es relativ einfach, Untergruppen zu beschreiben, die von Teilmengen U gebildet werden. Es genügt zu fordern

   1. $e \in U$ und
   2. $x, y \in U \Rightarrow x \circ y \in U$.

   Mit jedem Element x enthält U dann automatisch auch sein Inverses x^{-1}.

   Wir listen alle Mengen

   $$U_i = \{(i \cdot k) \bmod 12 \mid k \in \mathbb{N}\}$$

   auf. Sie bilden die zyklischen Untergruppen und werden von einer Zahl $i \in \mathbb{Z}_{12}$ erzeugt. Die Listen der Mengenelemente ordnen wir in der Reihenfolge der auftretenden Potenzen.

   $$\begin{aligned}
   U_1 = \{(k) \bmod 12 \mid k \in \mathbb{N}\} &= \mathbb{Z}_{12}\,, \\
   U_2 = \{(2k) \bmod 12 \mid k \in \mathbb{N}\} &= \{0, 2, 4, 6, 8, 10\}\,, \\
   U_3 = \{(3k) \bmod 12 \mid k \in \mathbb{N}\} &= \{0, 3, 6, 9\}\,, \\
   U_4 = \{(4k) \bmod 12 \mid k \in \mathbb{N}\} &= \{0, 4, 8\}\,, \\
   U_5 = \{(5k) \bmod 12 \mid k \in \mathbb{N}\} &= \{0, 5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7\} = \mathbb{Z}_{12}\,, \\
   U_6 = \{(6k) \bmod 12 \mid k \in \mathbb{N}\} &= \{0, 6\}\,, \\
   U_7 = \{(7k) \bmod 12 \mid k \in \mathbb{N}\} &= \{0, 7, 2, 9, 4, 11, 6, 1, 8, 3, 10, 5\} = \mathbb{Z}_{12}\,, \\
   U_8 = \{(8k) \bmod 12 \mid k \in \mathbb{N}\} &= \{0, 8, 4\} = U_4\,, \\
   U_9 = \{(9k) \bmod 12 \mid k \in \mathbb{N}\} &= \{0, 9, 6, 3\} = U_3\,, \\
   U_{10} = \{(10k) \bmod 12 \mid k \in \mathbb{N}\} &= \{0, 10, 8, 6, 4, 2\} = U_2\,, \\
   U_{11} = \{(11k) \bmod 12 \mid k \in \mathbb{N}\} &= \{0, 11, 10, 9, 8, 7, 6, 5, 4, 3, 2, 1\} = \mathbb{Z}_{12}\,.
   \end{aligned}$$

2. $\langle \mathbb{Z}, + \rangle$ ist eine unendliche zyklische Gruppe, die von dem Element 1 erzeugt wird. Es gilt

   $$U_1 = \{(1 \cdot k) \mid k \in \mathbb{Z}\} = \mathbb{Z}$$

   Die erzeugenden Elemente durchlaufen nun aber alle natürlichen Zahlen. Wir erhalten die folgenden zyklischen Untergruppen für alle $i \in \mathbb{N}$

   $$U_i = \{(i \cdot k) \mid k \in \mathbb{Z}\}\,.$$

   Man beachte, dass alle U_i unendliche Ordnung besitzen.

Hausaufgabe 4 (5 Punkte)

Begründen Sie Ihre Antwort auf die folgenden Fragen.

1. Wie viele Elemente und wie viele Atome besitzt die Boolesche Potenzmengenalgebra $\langle \mathcal{P}([5]), \cap, \cup, \overline{\ } \rangle$?
2. Stellen Sie die Boolesche Algebra $\langle \{T, F\}, \wedge, \vee, \neg \rangle$ isomorph als Potenzmengenalgebra dar.
3. Wie viele Atome besitzt eine Boolesche Algebra mit 128 Elementen?

Lösungsvorschlag

Diese Aufgabe stützt sich auf die Tatsache, dass nach dem Darstellungssatz jede endliche Boolesche Algebra isomorph ist zu einer Potenzmengenalgebra $\langle \mathcal{P}([n]), \cap, \cup, \overline{\ } \rangle$.

1. Es gilt $|\mathcal{P}([5])| = 2^5 = 32$.
2. Es gilt $|\mathcal{P}([1])| = 2^1 = 2$. Also ist $\langle \mathcal{P}([1]), \cap, \cup, \overline{\ } \rangle$ isomorph zu $\langle \{T, F\}, \wedge, \vee, \neg \rangle$.
3. Eine Algebra $\langle \mathcal{P}([n]), \cap, \cup, \overline{\ } \rangle$ besitzt genau n Atome, da die Atome einer Potenzmengenalgebra gerade durch die einelementigen Teilmengen gegeben sind.

Hinweis: *Die im Folgenden als Vorbereitung bezeichneten Aufgaben werden nicht bewertet und dienen der häuslichen Vorbereitung der Tutoraufgaben, die ebenfalls nicht bewertet werden. Die Abgabe einer Bearbeitung der Vorbereitungsaufgaben zusammen mit der Bearbeitung der Hausaufgaben wird empfohlen. Tutoraufgaben werden in den Übungsgruppen bearbeitet.*

Vorbereitung 1

1. Zeigen Sie, dass gilt $\{(7k) \bmod 12 \mid k \in \mathbb{N}\} = \mathbb{Z}_{12}$.
2. Welche Ordnung besitzt 11 in $\langle \mathbb{Z}_{12}, +_{12} \rangle$? Beweis!

Lösungsvorschlag

1. Man könnte k von 1 bis 12 durchlaufen und nachsehen, ob modulo 12 alle Zahlen aus $\mathbb{Z}_{12}$ erscheinen. Tatsächlich ist das auch der Fall.

   Es geht aber auch eleganter wie folgt.

   Wegen $ggT(7, 12) = 1$ gibt es $m, n \in \mathbb{Z}$, so dass $7m + 12n = 1$ gilt. Man kann m positiv wählen, wenn man die Gleichung nur modulo 12 zu lösen braucht. Für jedes $x \in \mathbb{Z}_{12}$ gibt es deshalb ein $m \in \mathbb{N}$ und ein $l \in \mathbb{Z}$, so dass $7m + 12l \equiv x(mod 12)$ gilt.
2. Da $ggT(11, 12) = 1$ gilt, ist $11 \cdot 12$ das kleinste gemeinsame Vielfache von 11 und 12. Daraus folgt $\mathrm{ord}(11) = 12$.

Vorbereitung 2

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

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

$$\begin{aligned} a \cdot 0 &= 0 \cdot a = 0, \\ a \cdot (-b) &= (-a) \cdot b = -a \cdot b. \end{aligned}$$

2. Es gibt bis auf Isomorphie genau einen Ring $R = \langle S, +, \cdot, 0, 1 \rangle$ mit drei Elementen, d. h. $S = \{0, 1, a\}$. Insbesondere muß also R isomorph sein zum Ring $\langle \mathbb{Z}_3, +_3, \cdot_3, 0, 1 \rangle$.
3. Der Ring $R = \langle S, +, \cdot, 0, 1 \rangle$ mit drei Elementen ist ein Körper.

Lösungsvorschlag

1. Es gilt $a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a \cdot 0$. Daraus folgt $a \cdot 0 = 0$. Analog folgt $0 \cdot a = 0$.

   Andererseits gilt $0 = a \cdot 0 = a \cdot (b-b) = a \cdot b + a \cdot (-b)$. Daraus folgt $-a \cdot b = a \cdot (-b)$. Analog folgt $-a \cdot b = (-a) \cdot b$.

2. Wir untersuchen Existenz und Eindeutigkeit des gesuchten Ringes wie folgt:

   R muß zusammen mit $+$ eine abelsche Gruppe mit neutralem Element 0 bilden. Neutralität von 0 ergibt die folgende Verknüpfungstabelle

$+$	0	1	a
0	0	1	a
1	1	$\times$	?
a	a		

   An der Stelle $\times$ kann nicht die 0 stehen, weil sonst an der Stelle ? das Element a stehen müsste, im Widerspruch zur Kürzungsregel. Es ergibt sich zwangsläufig

$+$	0	1	a
0	0	1	a
1	1	a	0
a	a	0	1

   Man sieht sofort, dass dies die gleiche Verknüpfungstafel ist, wie die Verknüpfungstafel von $\langle \mathbb{Z}_3, +_3 \rangle$. Tatsächlich gibt es bis auf Isomorphie nur eine einzige Gruppe mit 3 Elementen.

   Für die Multiplikation gilt

$\cdot$	0	1	a
0	0	0	0
1	0	1	a
a	0	a	?

   An der Stelle ? steht der Wert von $a \cdot a$. Wir rechnen $a \cdot a = (1+1) \cdot (1+1) = 1+1+1+1 = 1$.

$\cdot$	0	1	a
0	0	0	0
1	0	1	a
a	0	a	1

   Man verifiziert sofort die Isomorphie zu $\langle \mathbb{Z}_3, \cdot_3 \rangle$, indem man $a = 2$ setzt.

   Damit ist die Isomorphie von R mit $\langle \mathbb{Z}_3, +_3, \cdot_3, 0, 1 \rangle$ gezeigt.

3. Bekanntlich ist $\langle \mathbb{Z}_3, +_3, \cdot_3, 0, 1 \rangle$ ein Körper und damit ist R ein Körper.

Vorbereitung 3

Sei $p(x) = 3x^4 - 4x^2 - 5x + 10$. Bestimmen Sie p an der Stelle -1 mit dem Hornerschema, d. h., werten Sie $p(-1)$ mit dem Hornerschema aus.

Lösungsvorschlag

Hornerschema:

$$p(x) = (((3x + 0)x - 4)x - 5)x + 10\,.$$

Auswertung:

$$\begin{aligned} p(-1) &= (((3(-1) + 0)(-1) - 4)(-1) - 5)(-1) + 10 \\ &= ((-3(-1) - 4)(-1) - 5)(-1) + 10 \\ &= (-1(-1) - 5)(-1) + 10 \\ &= -4(-1) + 10 \\ &= 14\,. \end{aligned}$$

Tutoraufgabe 1

1. Die Charakteristik eines Körpers K, i. Z. $char(K)$, ist definiert als die Ordnung des Elements 1 in der additiven Gruppe von K. Man zeige:

   $$p = char(K) \in \mathbb{N} \Rightarrow p \text{ ist eine Primzahl}\,.$$

2. Geben Sie die Verknüpfungstafeln eines Körpers mit 4 Elementen an. Welche Charakteristik hat dieser Körper?

   Begründen Sie Ihre Angaben!

Lösungsvorschlag

1. Zur besseren Unterscheidung schreiben wir die Multiplikation in K als $\circ$. Wir betrachten $p = s \cdot t$. Dann gilt nach dem Distributivgesetz von $\circ$

   $$(\underbrace{1 + 1 + \ldots + 1}_{s\ \times}) \circ (\underbrace{1 + 1 + \ldots + 1}_{t\ \times}) = (\underbrace{1 + 1 + \ldots + 1}_{s \cdot t\ \times}) = 0\,,$$

   oder anders geschrieben

   $$(s \cdot 1) \circ (t \cdot 1) = (s \cdot t) \cdot 1 = p \cdot 1 = 0\,.$$

   Da ein Körper nullteilerfrei ist, folgt $s \cdot 1 = 0$ oder $t \cdot 1 = 0$. Da p die Charakteristik der additiven Gruppe von K ist, muss $s \geq p$ oder $t \geq p$ gelten, d. h. $p = s$ oder $p = t$. Damit kann aber p keine echten Teiler enthalten.

2. Wir notieren den Körper nun als $K = \langle \{0, 1, b, c\}, +, \cdot \rangle$ mit entsprechenden neutralen Elementen 0 bzw. 1.

   Die Charakteristik eines Körpers K mit 4 Elementen ist notwendig gleich 2, weil sie, wie oben bewiesen, sowohl Primzahl ist als auch Teiler der Anzahl der Körperelemente. Letzteres muss gelten, weil die Ordnung der von 1 additiv erzeugten Untergruppe die Ordnung von K teilen muss nach dem Satz von Lagrange.

Damit gilt $1+1=0$. Die Multiplikation mit einem $x \neq 0$ ergibt $x+x=0$. Damit können wir die additive Gruppe unmittelbar aus der in Tutoraufgabe 2.2, Blatt 10 gewonnenen Verknüpfungstafel gewinnen.

$+$	0	1	b	c
0	0	1	b	c
1	1	0	c	b
b	b	c	0	1
c	c	b	1	0

Die multiplikative Gruppe von K besitzt drei Elemente $1, b, c$. Für die Verknüpfungstafel gilt zunächst

$\cdot$	1	b	c
1	1	b	c
b	b	$\times$	$?$
c	c		

Falls man an die Stelle $\times$ die 1 setzen würde, entstünde an der Stelle ? ein Widerspruch zur Kürzungsregel. Die Vervollständigung ergibt sich damit zwingend wie folgt.

$\cdot$	1	b	c
1	1	b	c
b	b	c	1
c	c	1	b

Die gesamte Verknüpfungstafel für $\cdot$ ergibt sich durch Ergänzung der Multiplikation mit 0:

$$0 \cdot x = x \cdot 0 = 0 \quad \text{für alle} \quad x \in \{0, 1, b, c\}\,.$$

Tutoraufgabe 2

Wir betrachten Polynome $p(x), q(x) \in \mathbb{Q}[x]$, d. h. Polynome p, q in einer Unbestimmten (Variablen) x und Koeffizienten aus dem Körper $\mathbb{Q}$ der rationalen Zahlen mit

$$\begin{aligned} p(x) &= x^5 - 3x^4 + 3x^3 - 9x^2 + 2x - 6\,, \\ q(x) &= x^3 + 3x^2 + x + 3\,. \end{aligned}$$

Berechnen Sie mit dem (erweiterten) Euklidschen Algorithmus ein Polynom möglichst hohen Grades, das sowohl Teiler von $p(x)$ als auch Teiler von $q(x)$ ist ($ggT(p,q)$).

Lösungsvorschlag

Durch Polynomdivision $p(x) = q_1 q(x) + r_2$ erhalten wir

$$x^5 - 3x^4 + 3x^3 - 9x^2 + 2x - 6 = (x^3 + 3x^2 + x + 3)(x^2 - 6x + 20) + (-66x^2 - 66)\,,$$

d. h.

$$q_1 = x^2 - 6x + 20 \quad \text{und} \quad r_2 = -66x^2 - 66\,.$$

Durch Polynomdivision $q(x) = q_2 r_2 + r_3$ erhalten wir

$$x^3 + 3x^2 + x + 3 = (-66x^2 - 66)(-\frac{1}{66}x - \frac{1}{22}) = (x^2 + 1)(x + 3)\,.$$

Hier ist bereits $r_3 = 0$, und der Euklidsche Algorithmus ist beendet.
Offensichtlich ist x^2+1 ein gesuchter ggT, wenn man den Leitkoeffizienten auf 1 normiert. Die Erweiterung des Euklidschen Algorithmus besteht darin, den ggT als Ausdruck in den Ausgangspolynomen p und q darzustellen. Dies ist in diesem Beispiel wie folgt:

$$x^2 + 1 = -\frac{1}{66}p(x) + \frac{1}{66}q_1 q(x)\,.$$

Tutoraufgabe 3

Sei $\pi(x) = x^3 + 1$. Wir betrachten den Ring $R = \langle \mathbb{Z}_2[x]_{\pi(x)}, +_{\pi(x)}, \cdot_{\pi(x)} \rangle$. Seine Elemente werden repräsentiert durch die Reste bei Polynomdivision durch $x^3 + 1$.

1. Geben Sie die Menge aller Elemente von R an.
2. Wir betrachten das Element $a = x^2 \in \mathbb{Z}_2[x]_{\pi(x)}$. Bestimmen Sie die Zeile der Multiplikationstafel des Ringes R, die für alle $b \in \mathbb{Z}_2[x]_{\pi(x)}$ die Produkte $a \cdot_{\pi(x)} b$ auflistet.
3. Geben Sie die Menge der Nullteiler in R an.

   Hinweis: $p \in Z_2[x]_{\pi(x)}$ mit $\mathrm{grad}(p) \neq 0$ heißt Nullteiler, falls es ein $q \in Z_2[x]_{\pi(x)}$ mit $\mathrm{grad}(q) \neq 0$ gibt, so dass gilt $p \cdot_{\pi(x)} q = 0$.

Lösungsvorschlag

1. Für die Menge R' der Repräsentanten von R gilt
   $$R' = \mathbb{Z}_2[x]_3 = \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$$
2. | $\cdot$ | 0 | 1 | x | $x+1$ | x^2 | x^2+1 | x^2+x | x^2+x+1 |
   |---|---|---|---|---|---|---|---|---|
   | x^2 | 0 | x^2 | 1 | x^2+1 | x | x^2+x | $x+1$ | x^2+x+1 |
3. Offenbar ist 1 eine Nullstelle des Divisorpolynoms $\pi(x) = x^3 + 1$. Es gilt
   $\pi(x) = x^3 + 1 = (x+1)(x^2+x+1)$.

   Sei N_π die Menge der Teiler von $\pi(x)$. Bei Rechnung modulo π werden diese Teiler zu Nullteilern. Sei N die Menge der Nullteiler von R. Dann gilt also
   $$N_\pi = \{x+1, x^2+x+1\} \subseteq N.$$

   Um N zu erhalten, werden diejenigen Vielfachen $t(x)$ von Elementen aus N_π hinzugenommen, die die Gradbedingung $1 \leq \mathrm{grad}(t) < 3$ erfüllen. Ergebnis:

   $$\begin{aligned} N &= \{x+1, x^2+x+1\} \cup \{(x+1)x, (x+1)(x+1)\} \\ &= \{x+1, x^2+x+1, x^2+x, x^2+1\}\,. \end{aligned}$$