Technische Universität München
Fakultät für Informatik
Lehrstuhl für Informatik 7
Softwarezuverlässigkeit u. Theoretische Informatik
Prof. Dr. Javier Esparza
Dr. Werner Meixner

Wintersemester 2009/10
Übungsblatt 13
1. Februar 2010

Diskrete Strukturen

Abgabetermin: 8. Februar 2010, 14 Uhr in die **DS Briefkästen**

Hausaufgabe 1 (5 Punkte)

Sei $p \in \mathbb{N}$ eine Primzahl.

1. Beweisen Sie für alle ganzen Zahlen $x, y \in \mathbb{Z}$: $(x+y)^p \equiv x^p + y^p \pmod{p}$.
2. Berechnen Sie mit größtmöglicher Vereinfachung den Ausdruck $(p-1)^{p+1} \bmod p$.

Hausaufgabe 2 (5 Punkte)

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

1. Geben Sie eine Verknüpfungstafel (Operationstafel) für eine nicht assoziative und nicht kommutative Operation $\circ$ an.
2. Zeigen Sie, dass es genau 2 kommutative und nicht assoziative Operationen $\circ$ gibt.
3. Geben Sie alle Booleschen Operationen an, die kommutativ und nicht assoziativ sind?

Hausaufgabe 3 (5 Punkte)

1. Wie viele der Algebren $A = \langle S, \circ \rangle$ aus der vorausgegangenen HA sind Gruppen? Sind diese Gruppen isomorph? Sind sie kommutativ, zyklisch? Begründen Sie jeweils Ihre Antworten!
2. Kennzeichnen Sie die Relation, in der diese Gruppen zu $\langle \mathbb{Z}_2, +_2 \rangle$ bzw. $\langle \mathbb{Z}_3^*, \cdot_3 \rangle$ stehen!
3. Geben Sie eine Untergruppe von $\mathcal{S}_3$ mit 2 Elementen an.

Hausaufgabe 4 (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. Die Menge U aller Elemente x einer abelschen Gruppe G, deren Inverses x^{-1} eine Potenz von x ist, bildet eine Untergruppe von G. Beweis!

Hinweis: *Auf den Übungsblättern in diesem Semester wird es grundsätzlich die drei Aufgabentypen Vorbereitungsaufgabe, Tutoraufgabe und Hausaufgabe geben. Die als Vorbereitung bezeichneten Aufgaben dienen der häuslichen Vorbereitung der Tutoraufgaben. Tutoraufgaben werden in den Übungsgruppen bearbeitet. Dabei wird die Lösung der Vorbereitungsaufgaben vorausgesetzt. Die Vorbereitungsaufgaben werden in der Zentralübung unterstützt.*

Vorbereitung 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.
$$a \odot 0 \;=\; 0 \odot a \;=\; 0\,, \qquad\qquad a \odot b \;=\; (-a) \odot (-b)\,.$$
2. Geben Sie 2 nicht-kommutative Ringe an.

Vorbereitung 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 $\langle \mathbb{Z}_3, +_3, \cdot_3, 0, 1\rangle$.
2. Der Ring $R = \langle S, \oplus, \odot, 0, 1\rangle$ mit drei Elementen ist ein Körper.
3. Sei t_x die Anzahl der 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.

   Hinweis: $y \in S \setminus \{0\}$ ist ein Nullteiler von $x \in S \setminus \{0\}$, falls $x \odot y = 0$.

Vorbereitung 3

Mit $R = \mathbb{Z}_3[x]$ bezeichnen wir den Ring aller Polynome über einer Variablen 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.
$$\begin{aligned} r_2(x) &= a(x) - q_1(x) \cdot b(x)\,, \\ r_3(x) &= b(x) - q_2(x) \cdot r_2(x)\,. \end{aligned}$$
2. Bestimmen Sie ein Polynom $t(x) \in R$ möglichst hohen Grades, das ein gemeinsamer Teiler von $a(x)$ und $b(x)$ ist.
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.

Tutoraufgabe 1

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 ($ggT(p, q)$).

Tutoraufgabe 2

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

Tutoraufgabe 3

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!