Wintersemester 2002/2003 14.2.2003

Diskrete Strukturen II, Klausur

Name	Vorname	Matrikelnummer

Aufgabe	1	2	3	4	5	6	7	8	9	10	$\sum$
Punkte											

Bitte schreiben Sie auf jeden Zettel, den Sie abgeben, deutlich Ihren Namen. Bei Multiple-Choice-Aufgaben ergibt jedes korrekte, falsche bzw. nicht angekreuzte Kästchen $+1/2$, $-1/2$ bzw. 0 Punkte.

Aufgabe 1: *(2 + 4 + 4 Punkte)*

(a) Welche Elemente von $\mathbb{Z}/6\mathbb{Z}$ sind invertierbar (Begründung!)?

(b) Finden Sie einen Erzeuger der zyklischen Gruppe $(\mathbb{F}_{11}\backslash\{0\},\cdot)$. Berechnen Sie die Ordnungen der Elemente 3 und 4 in $(\mathbb{F}_{11}\backslash\{0\},\cdot)$.

(c) Berechnen Sie ein Inverses von 14 in $\mathbb{Z}/45\mathbb{Z}$ bezüglich der Multiplikation.

Aufgabe 2: *(3 Punkte)*
Faktorisieren Sie das Polynom X^2+1 in $\mathbb{Q}[X], \mathbb{R}[X], \mathbb{C}[X], \mathbb{F}_2[X]$ und $\mathbb{F}_3[X]$.

Aufgabe 3: *(6 Punkte, minimal 0 Punkte)*
Welche Aussagen gelten für $a, b, c \in \mathbb{Z}$?

	Wahr	Falsch
$n \in \mathbb{Z}$, $n \mid (a \cdot b) \quad \Rightarrow \quad n \mid a$ oder $n \mid b$.		
n Primzahl, $n \mid (a \cdot b) \quad \Rightarrow \quad n \mid a$ oder $n \mid b$.		
$n \in \mathbb{Z}$, $n \mid a \quad \Rightarrow \quad n \mid (a \cdot b)$.		
$n \in \mathbb{Z}, n \geq 2, \quad ac \equiv bc \pmod{n} \quad \Rightarrow \quad a \equiv b \pmod{n}$.		
$n \in \mathbb{Z}$, $n \mid (a+b) \quad \Rightarrow \quad n \mid a$ und $n \mid b$.		
$n \in \mathbb{Z}$, $n \mid (a+b)$, $n \mid a \quad \Rightarrow \quad n \mid b$.		

Welche Aussagen gelten in allen Körpern $(K, +, \cdot)$?

	Wahr	Falsch
Für alle $a, b \in K$: $\quad ab = 0 \quad \Rightarrow \quad (a = 0)$ oder $(b = 0)$.		
Für alle $a, b, c \in K$: $\quad (a+b) \cdot c = (a+c) \cdot (b+c)$.		
$(K, +)$ ist eine Gruppe.		
$(K, \cdot)$ ist eine Gruppe.		
Für alle $a \in K$ gibt es ein $b \in K$ mit $a \cdot b = 1$.		
Es gibt genau ein $e \in K$ mit $e + a = a + e = a$ für alle $a \in K$.		

Aufgabe 4: *(1 + 3 Punkte)*
Es sei $(G, \circ)$ eine Gruppe und e das neutrale Element von G. Außerdem gelte für alle $a \in G$: $a \circ a = e$. Zeigen Sie:

(a) Für alle $a \in G$ gilt: $a = a^{-1}$. (b) G ist eine abelsche Gruppe.

Aufgabe 5: *(3 + 2 Punkte)*
Berechnen Sie alle Lösungen $x, y \in \mathbb{Z}$ zu den Gleichungssystemen

$$\text{(a)} \quad \begin{aligned} x &\equiv 3 \pmod 5 \\ x &\equiv 4 \pmod 6, \end{aligned}$$

$$\text{(b)} \quad \begin{aligned} y &\equiv 3 \pmod 6 \\ y &\equiv 1 \pmod 3). \end{aligned}$$

Aufgabe 6: *(5 Punkte)*
Es seien

$$A := \begin{pmatrix} 1 & 2 & 0 \\ 2 & 0 & 2 \\ 0 & 2 & 1 \end{pmatrix} \in \mathbb{F}_3^{3\times 3}, \quad a := \begin{pmatrix} 2 \\ 2 \\ 0 \end{pmatrix} \in \mathbb{F}_3^3.$$

Lösen Sie die Gleichung $Ax = a$.

Aufgabe 7: *(6 Punkte)*
Man löse das lineare Programm

$$\begin{aligned} -2x_1 + 3x_2 &\leq 12 \\ 2x_1 + x_2 &\leq 8 \\ x_2 &\leq 3 \end{aligned}$$

$$x_1, x_2 \geq 0, \quad Q(x_1, x_2) = -x_1 - x_2 = \text{ Min!}$$

mit dem Simplex-Algorithmus.

Aufgabe 8: *(1 + 3 + 2 Punkte)*
Ein Würfel und eine Münze werden geworfen. Es bezeichne X_1 die Zufallsvariable, die das Ergebnis des Würfelns (Werte $1, 2, \ldots, 6$) und X_2 die Zufallsvariable, die das Ergebnis des Münzwurfs angibt (Werte 0 und 1). Es sei $X = X_1 \cdot X_2$.

(a) Welche Werte nimmt die Zufallsvariable X an?

(b) Bestimmen Sie die Erwartungswerte $\mathrm{E}(X_1), \mathrm{E}(X_2)$ und $\mathrm{E}(X)$. Welcher Zusammenhang besteht zwischen ihnen?

(c) Bestimmen Sie die Varianz $\mathrm{Var}(X)$.

Aufgabe 9: *(2 + 3 Punkte)*
In einem Rechnerraum kommen drei verschiedene Computermodelle (Typ C_1, C_2 und C_3) und zwei verschiedene Betriebssysteme vor (B_1 und B_2). Die Hälfte der Computer sei vom Typ C_1 und ein Drittel vom Typ C_2. Das System B_1 (bzw. B_2) befindet sich auf einem Computer vom Typ C_1 mit der Wahrscheinlichkeit 0.3 (bzw. 0.1), auf einem Computer vom Typ C_2 mit der Wahrscheinlichkeit 0.15 (bzw. 0.33) und auf einem Computer vom Typ C_3 mit der Wahrscheinlichkeit 0.18 (bzw. 0.36).

(a) Wie groß ist die Wahrscheinlichkeit, auf einem (zufällig ausgewählten) Computer das System B_1 zu finden?

(b) Wie groß ist die Wahrscheinlichkeit, dass man an einem Computer vom Typ C_3 sitzt, wenn dort das System B_2 läuft?

Aufgabe 10: *(4 Punkte)*
Es seien $A_1, \ldots, A_n$ paarweise disjunkte Teilmengen eines Wahrscheinlichkeitsraumes und $B \subset A_1 \cup \ldots \cup A_n$. Zeigen Sie:

$$\mathrm{P}(B) = \sum_{i=1}^{n} \mathrm{P}(B \cap A_i).$$

Wintersemester 2002/2003 14.2.2003

Diskrete Strukturen II
Lösungen zur Klausur

Aufgabe 1:

(a) Die invertierbaren Elemente von $\mathbb{Z}/6\mathbb{Z}$ sind genau die $a \in \mathbb{Z}/6\mathbb{Z}$ mit $\mathrm{ggT}(a, 6) = 1$, d.h. 1 und 5.

(b) In $\mathbb{F}_{11}$ hat 2 die Potenzen $2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 5, 2^5 = 10, 9, 7, 3, 6, 1$ und ist somit ein Erzeuger von $\mathbb{F}_{11}^\times$. Bei 3 bzw. 4 hat man die Folgen von Potenzen $3, 9, 5, 4, 1$ bzw. $4, 5, 9, 3, 1$. Die Ordnungen von 3 bzw. 4 sind demnach 5 bzw. 5.

(c) Erweiterter Eukidischer Algorithmus mit den Zahlen 45 und 14:

$$\begin{array}{rrcl} & 45 & = & 3 \cdot 14 + 3 \\ & 14 & = & 4 \cdot 3 + 2 \\ & 3 & = & 1 \cdot 2 + 1 \\ \Rightarrow & 1 & = & 3 - 2 = 3 - 14 + 4 \cdot 3 = \ldots = 5 \cdot 45 - 16 \cdot 14. \end{array}$$

Daraus ergibt sich

$$1 = 5 \cdot 45 - 16 \cdot 14 \equiv -16 \cdot 14 \pmod{45}$$

und $29 = 45 - 16$ ist das gesuchte Element.

Aufgabe 2:

Für alle a in $\mathbb{Q}$ oder $\mathbb{R}$ gilt $a^2 + 1 > 0$. Damit ist $X^2 + 1$ irreduzibel in $\mathbb{Q}[X]$ und in $\mathbb{R}[X]$.
In $\mathbb{C}[X]$ hat man $X^2 + 1 = (X - i) \cdot (X + i)$, wobei i eine Wurzel aus -1 ist. Auch in $\mathbb{F}_2[X]$ zerfällt das Polynom in Linearfaktoren: $X^2 + 1 = (X + 1)^2$.
In $\mathbb{F}_3$ hingegen ist $0^2 + 1 = 1$, $1^2 + 1 = 2$ und $2^2 + 1 = 2$. Also ist $X^2 + 1$ irreduzibel in $\mathbb{F}_3[X]$.

Aufgabe 4:

(a) Multipliziert man die Gleichung $a \circ a = e$ (die nach Voraussetzung gilt) mit a^{-1}, so hat man $a \circ a \circ a^{-1} = e \circ a^{-1}$ oder auch $a = a^{-1}$.

(b) Wählt man beliebige $a, b \in G$, so gilt:

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

d.h. G ist eine abelsche Gruppe.

Aufgabe 5:

(a) Die Zahlen 5 und 6 haben ggT 1. Der erweiterte Euklidische Algorithmus liefert die Kombination $1 = 1 \cdot 6 - 1 \cdot 5$.
Aus dem chinesischen Restsatz erhalten wir die Lösung $3 \cdot 1 \cdot 6 - 4 \cdot 1 \cdot 5 = -2$. Die weiteren Lösungen sind gegeben modulo dem kgV von 5 und 6, d.h. modulo 30; die Lösungsmenge ist also: $\{30 \cdot n - 2 \mid n \in \mathbb{Z}\}$.

(b) Aus der Bedingung $y \equiv 3 \pmod 6$ folgt, daß y durch 3 teilbar sein soll. Dann gilt aber $y \equiv 0 \pmod 3$, was der zweiten Gleichung widerspricht. Das Gleichungssystem hat keine Lösung.

Aufgabe 6:

Mit Hilfe des Gauß-Algorithmus berechnet man die eindeutige Lösung $(0, 1, 1) \in \mathbb{F}_3^3$ (A ist invertierbar):

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

Aufgabe 7:

Das Programm ist schon in Standardform gegeben. Der Algorithmus verläuft (zum Beispiel) folgendermaßen (das Pivotelement ist jeweils fett markiert):

	x_1	x_2	
x_3	-2	3	12
x_4	**2**	1	8
x_5	0	1	3
	-1	-1	0

$\Rightarrow$

	x_4	x_2	
x_3	1	4	20
x_1	$\frac{1}{2}$	$\frac{1}{2}$	4
x_5	0	**1**	3
	$\frac{1}{2}$	-$\frac{1}{2}$	-4

$\Rightarrow$

	x_4	x_5	
x_3	1	-4	8
x_1	0	-$\frac{1}{2}$	$\frac{5}{2}$
x_2	0	1	3
	$\frac{1}{2}$	$\frac{1}{2}$	-$\frac{11}{2}$

Eine Lösung ist dann $x_1 = \frac{5}{2}$, $x_2 = 3$ und $Q(x_1, x_2) = -\frac{11}{2}$.

Aufgabe 8:

(a) Der Wertebereich von X ist:
$W_X = \{x_1 \cdot x_2 \mid x_1 \in W_{X_1}, x_2 \in W_{X_2}\} = \{0, 1, 2, 3, 4, 5, 6\}$.

(b) Für die Erwartungswerte hat man:
$\mathrm{E}(X_1) = \sum_{x=1}^{6} x \cdot \mathrm{P}(X_1 = x) = \frac{7}{2}$,
$\mathrm{E}(X_2) = \sum_{x=0}^{1} x \cdot \mathrm{P}(X_2 = x) = \frac{1}{2}$,
$\mathrm{E}(X) = \sum_{x=0}^{6} x \cdot \mathrm{P}(X_1 \cdot X_2 = x) = \sum_{x=0}^{6} x \cdot \frac{1}{12} = \frac{7}{4}$.
Der Zusammenhang zwischen den Erwartungswerten ist
$\mathrm{E}(X_1 \cdot X_2) = \mathrm{E}(X_1) \cdot \mathrm{E}(X_2)$.
(Die Zufallsvariablen X_1 und X_2 sind unabhängig.)

(c) Für die Varianz haben wir die Formel $\mathrm{Var}(X) = \mathrm{E}(X^2) - \mathrm{E}(X)^2$. Der zweite Term ist
$\mathrm{E}(X^2) = \sum_{x=0}^{6} x^2 \cdot \mathrm{P}(X = x) = \sum_{x=1}^{6} x^2 \frac{1}{12} = \frac{91}{12}$,
und somit ist $\mathrm{Var}(X) = \frac{91}{12} - \frac{49}{16} = \frac{217}{48}$.

Aufgabe 9:

(a) Die Hälfte der Computer ist vom Typ C_1 und $\frac{1}{3}$ vom Typ C_2, also $\frac{1}{6}$ vom Typ C_3. Die Wahrscheinlichkeit , daß auf einem Computer das System B_1 ist, ist $\frac{1}{2} \cdot 0,3 + \frac{1}{3} \cdot 0,15 + \frac{1}{6} \cdot 0,18 = 0,23$.

(b) Es sei A das Ereignis, daß der Computer vom Typ C_3 ist, und B das Ereignis, daß das System B_2 ist. Dann ist

$$\mathrm{P}(A \mid B) = \frac{\mathrm{P}(A \cap B)}{\mathrm{P}(B)} = \frac{\frac{1}{6} \cdot 0,36}{\frac{1}{2} \cdot 0,1 + \frac{1}{3} \cdot 0,33 + \frac{1}{6} \cdot 0,36} = \frac{3}{11}.$$

Aufgabe 10:

Da $A_1, \dots, A_n$ paarweise disjunkt sind, sind auch $B \cap A_1, \dots, B \cap A_n$ paarweise disjunkt. Damit gilt:

$$\mathrm{P}(B) = \mathrm{P}\left(\bigcup_{i=1}^{n} B \cap A_i\right) = \sum_{i=1}^{n} \mathrm{P}(B \cap A_i).$$

Aufgabe 3:

	Wahr	Falsch
$n \in \mathbb{Z}$, $n \mid (a \cdot b) \quad \Rightarrow \quad n \mid a$ oder $n \mid b$.		$\times$
n Primzahl, $n \mid (a \cdot b) \quad \Rightarrow \quad n \mid a$ oder $n \mid b$.	$\times$	
$n \in \mathbb{Z}$, $n \mid a \quad \Rightarrow \quad n \mid (a \cdot b)$.	$\times$	
$n \in \mathbb{Z}, n \geq 2, \quad ac \equiv bc \pmod{n} \quad \Rightarrow \quad a \equiv b \pmod{n}$.		$\times$
$n \in \mathbb{Z}$, $n \mid (a+b) \quad \Rightarrow \quad n \mid a$ und $n \mid b$.		$\times$
$n \in \mathbb{Z}$, $n \mid (a+b)$, $n \mid a \quad \Rightarrow \quad n \mid b$.	$\times$	
Für alle $a, b \in K$: $\quad ab = 0 \quad \Rightarrow \quad (a = 0)$ oder $(b = 0)$.	$\times$	
Für alle $a, b, c \in K$: $\quad (a+b) \cdot c = (a+c) \cdot (b+c)$.		$\times$
$(K, +)$ ist eine Gruppe.	$\times$	
$(K, \cdot)$ ist eine Gruppe.		$\times$
Für alle $a \in K$ gibt es ein $b \in K$ mit $a \cdot b = 1$.		$\times$
Es gibt genau ein $e \in K$ mit $e + a = a + e = a$ für alle $a \in K$.	$\times$	