Lösungen zur Musterklausur Mathematische Methoden der Informatik WS 1998/99

12. August 1999

1. Aufgabe

(a) 1. Lösung: Für $n = 1$ ist die Behauptung richtig.
Jede natürliche Zahl $n > 1$ ist (bis auf die Reihenfolge) eindeutig als Produkt von Primzahlpotenzen darstellbar, $n = p_1^{\alpha_1} \cdot \dots \cdot p_r^{\alpha_r}$, p_ρ paarweise verschieden, $\alpha_\rho \geq 1$.
Induktion nach der Anzahl r der verschiedenen Primteiler von n:
Induktionsanfang: $r = 1$, $n = p^\alpha$. Dann ist $\frac{\varphi(n)}{n} = \frac{p^\alpha - p^{\alpha-1}}{p^\alpha} = 1 - \frac{1}{p}$.
Induktionsschritt: Die Behauptung sei für ein $r \geq 1$ bewiesen;
n besitze $r + 1$ verschiedene Primteiler, etwa $n = n' \cdot q^\alpha$;
hierbei ist q eine Primzahl, $(n', q) = 1$, und n' besitzt r verschiedene Primteiler.
Die Behauptung gilt nach Induktionsvoraussetzung für n' und nach Induktionsanfang für q^α .
Daher ist $\frac{\varphi(n)}{n} = \frac{\varphi(n' \cdot q^\alpha)}{n' \cdot q^\alpha} = \frac{\varphi(n') \cdot \varphi(q^\alpha)}{n' \cdot q^\alpha} = \prod_{p|n'} \left(1 - \frac{1}{p}\right) \cdot \left(1 - \frac{1}{q}\right) = \prod_{p|n} \left(1 - \frac{1}{p}\right)$DDas Induktionsprinzip liefert die Behauptung.

(b) 2. Lösung: Für $n = 1$ ist die Behauptung richtig.
$p^\alpha \| n$ heißt, daß α die genaue Potenz von p ist, die in n aufgeht, d.h. $p^\alpha \mid n$, $p^{\alpha+1}$ teilt nicht n . Dann ist $n = \prod_{p^\alpha \| n} p^\alpha$ und $\varphi(n) = \prod_{p^\alpha \| n} \varphi(p^\alpha) = \prod_{p^\alpha \| n} \left(p^\alpha \cdot \left(1 - \frac{1}{p}\right)\right) = \prod_{p^\alpha \| n} p^\alpha \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right) = n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right)$. Hieraus folgt die Behauptung.

2. Aufgabe

(a) 1. Lösung: Gesucht ist offenbar 321^{1999} mod 100. Zunächst ist $321^{1999} \equiv 21^{1999}$ mod 100. Ist $(a, m) = 1$, so ist nach dem Satz von Euler $a^{\varphi(m)} \equiv 1 \bmod m$. Es gilt $\varphi(100) = \varphi(4 \cdot 25) = \varphi(4) \cdot \varphi(25) = 2 \cdot 20 = 40$. Also ist $21^{40} \equiv 1$ mod 100 und $21^{1999} \equiv 21^{39} \equiv 21^{-1}$ mod 100. Es gilt $21^{-1} \equiv x$ mod 100 $\Leftrightarrow 21 \cdot x \equiv 1$ mod 100. Diese Kongruenz kann man z.B. mit Hilfe des Euklidischen Algorithmus' lösen:

$100 = 4 \cdot 21 + 16$, $21 = 1 \cdot 16 + 5, 16 = 3 \cdot 5 + 1$. Hieraus erhält man $1 = 16 - 3 \cdot 5 = 16 - 3 \cdot (21 - 1 \cdot 16) = 4 \cdot 16 - 3 \cdot 21 = 4 \cdot (100 - 4 \cdot 21) - 3 \cdot 21$ $= 4 \cdot 100 - 19 \cdot 21$.
Also ist $-19 \cdot 21 \equiv 1 \bmod 100$ oder $81 \cdot 21 \equiv 1 \bmod 100$.
Insgesamt erhält man: $321^{1999} \equiv 81 \bmod 100$. Die letzten beiden Ziffern von 321^{1999} sind 81.

(b) 2. Lösung: Wie oben zeigt man $321^{1999} \equiv 21^{39} \bmod 100$. Schreibt man 39 zur Basis 2, so ist $39 = 32 + 4 + 2 + 1$, und daher $21^{39} = 21^{32} \cdot 21^4 \cdot 21^1 \cdot 21$. Durch fortgesetztes Quadrieren erhält man $21^2 \equiv 41 \bmod 100$, $21^4 \equiv 41^2 \equiv 81 \bmod 100$, $21^8 \equiv 81^2 \equiv 61 \bmod 100$, $21^{16} \equiv 61^2 \equiv 21 \bmod 100$, $21^{32} \equiv 21^2 \equiv 41 \bmod 100$. Daher ist $21^{39} \equiv 21 \cdot 41 \cdot 81 \cdot 41 \equiv 81 \bmod 100$. Also sind 81 die letzten Ziffern von 321^{1999} .

3. Aufgabe

(a) Wegen $1 \in Q$ gilt $x \sim x \forall x \in R \setminus \{0\}$, also ist $\sim$ reflexiv.
Gilt $x \sim y$, so ist $\frac{x}{y} \in Q \setminus \{0\}$. Dann ist auch $\frac{y}{x} \in Q$, also $y \sim x$. Daher ist $\sim$ symmetrisch.
Gilt $x \sim y$ und $y \sim z$, so ist $\frac{x}{y} \in Q$ und $\frac{y}{z} \in Q$. Dann ist auch $\frac{x}{z} = \frac{x}{y} \cdot \frac{y}{z} \in Q$, also $x \sim z$. Folglich ist $\sim$ transitiv. Insgesamt ist also $\sim$ eine Äquivalenzrelation.

(b) Es ist $x \sim 1 \Leftrightarrow x = \frac{x}{1} \in Q$; also ist $K(1) = Q \setminus \{0\}$.$x \sim \sqrt{2 \Leftrightarrow x = r \cdot \sqrt{2}}$ mit $r \in Q \setminus \{0\}$. Daher ist $K(\sqrt{2}) = Q \setminus \{0\} \cdot \sqrt{2 = \{x \in R \setminus \{0\} : x = r \cdot \sqrt{2}},r \in Q, r \neq 0\}$.

4. Aufgabe

- 1.Lösung
  zu zeigen: $(R, \oplus \otimes)$ ist Ring

  (a) $(R, \oplus)$ abelsche Gruppe
  Assoziativität: $(a \oplus b) \oplus c = (a + b - e) \oplus c$
  $= (a + b - e) + c - e$
  $= a + b + (-e + c) - e = a + b + (c - e) - e$ (da $(R, +)$ abelsch)
  $= a + b + c - e - e$
  $= a + (b - c - e) - e = a + (b \oplus c) - e = a \oplus (b \oplus c)$
  Neutrales Element bezüglich $\oplus$ ist e:
  $a \oplus e = a + e - e = a \ \forall a \in R$
  $e \oplus a = e + a - e = e - e + a = a$
  Zu $a \in R$ invers bezüglich $\oplus$ ist $-a + e + e = 2e - a$
  $a \oplus (-a + e + e) = a + (-a + e + e) - e = (a + (-a)) + e + (e - e) = e$
  Kommutativ: $a \oplus b = a + b - e = b + a + e = b \oplus a$
  $\Rightarrow$ abelsche Gruppe ist $(R, \oplus)$

(b) $(R, \otimes)$ Halbgruppe ist zu zeigen
Assoziativität: $(a \otimes b) \otimes c = (a + b - a \cdot b) \otimes c = (a + b - a \cdot b) + c - (a + b - a \cdot b) \cdot c$
$= a + b - a \cdot b + c - (a \cdot c + b \cdot c - a \cdot b \cdot c)$ (Distributivgesetz in $(R, +, \cdot)$
$= a + b + c - a \cdot b - a \cdot c - b \cdot c + a \cdot b \cdot c$ (Kommutativgesetz in $(R, +, \cdot)$
Ebenso ist $a \otimes (b \otimes c) = a \otimes (b + c - b \cdot c) = a + (b + c - b \cdot c) - a \cdot (b + c - b \cdot c)$
$= a + b + c - b \cdot c - a \cdot b - a \cdot c - a \cdot b \cdot c$
$\Rightarrow$ Assoziativität $\Rightarrow$ $(R, \otimes)$ ist Halbgruppe

(c) Distributivgesetze in $(R, \oplus \otimes)$
$(a \oplus b) \otimes c = (a + b - e) \otimes c = (a + b - e) + c - (a + b - e) \cdot c$
$= a + b - e + c - a \cdot c - b \cdot c + e \cdot c = a + b - e + c - a \cdot c - b \cdot c - e$
$= a + c - a \cdot c + b + c - b \cdot c - e = (a \otimes c) + (b \otimes c) - e = (a \otimes c) \oplus (b \otimes c)$
$a \otimes (b \otimes c)$ analog

(d) Damit ist $(R, \oplus \otimes)$ ein Ring: Zeige die Isomorphie zu $(R, +, \cdot)$
Definiere $f : (R, +, \cdot) \to (R, \oplus \otimes)$
$f(a) = e - a$

i. f ist Ring-Isomorphismus
$f(a + b) = e - (a + b) = e - a + b = -a + e - b + e - e$
$= f(a) + f(b) - e = f(a) \oplus f(b)$
$f(a \cdot b) = e - a \cdot b$
$f(a) \otimes f(b) = f(a) + f(b) - f(a) \cdot f(b) = (e - a) \otimes (e - b)$
$= (e - a) + (e - b) - (e - a) \cdot (e - b)$
$= e - a + e - b - (e \cdot e - a \cdot e - e \cdot b + a \cdot b)$
$= e - a + e - b - e + a + b - a \cdot b$
$= e - a \cdot b = f(a \cdot b)$

ii. Injektivität
$f(a) = f(b) \ \Leftrightarrow \ e - a = e - b$ (Kürzungsregel)
$-a = -b \ \Leftrightarrow \ a = b$ (Eindeutigkeit des Inversen)
$\Rightarrow \ a = b$
Surjektivität:
$(\forall\, b \in R)\, \exists\, a \in R : f(a) = b$
Sei $b \in R$. Dann ist $b = f(a)$ mit $a = e - b$ denn $f(a) = f(e - b) = e - (e - b) = (e - e) + b = b$
$\Rightarrow \ f(a)$ Isomorphismus

- 2. Lösung:
Sei $f : R \to R$ definiert durch $f(a) = e - a$ für $a \in R$.

(a) f ist surjektiv: Sei $b \in R$; dann ist $e - b \in R$ und $f(e - b) = e - (e - b) = b$.

(b) f ist injektiv: Aus $f(a) = f(b)$ folgt $e - a = e - b$ und wegen der Kürzungsregel $a = b$.

(c) f ist Homomorphismus: $f(a + b) = e - (a + b) = e - a + e - b - e = f(a) \oplus f(b)$; $f(a \cdot b) = e - a \cdot b = e - a + e - b + (e - a - b + a \cdot b) =$

$e - a + e - b - (e - a) \cdot (e - b) = f(a) \otimes f(b)$. (Mehrfach wurde die Kommutativität von R bezüglich „+" ausgenutzt und die Eigenschaften von e als Einselement von R bezüglich „· ").
Nach Satz 8.11(a) ist $(R, \oplus \otimes)$ ein Ring, der wegen (a) und (b) zu $(R, +, \cdot)$ isomorph ist.

5. Aufgabe

- 1. Lösung:

  (a) Wir verwenden das Unterraumkriterium. Offenbar ist $(0,0,0)^T \in V$.
  Seien $(x_1, y_1, z_1)^T, (x_2, y_2, z_2)^T \in V, \lambda, \mu \in R$. Dann ist $\frac{\lambda x_1 + \mu x_2}{a} = \frac{\lambda y_1 + \mu y_2}{b} = \frac{\lambda z_1 + \mu z_2}{c}$; also ist $(\lambda x_1 + \mu x_2,\ \lambda y_1 + \mu y_2,\ \lambda z_1 + \mu z_2)^T = \lambda(x_1, y_1, z_1)^T + \mu(x_2, y_2, z_2)^T \in V$.
  Daher ist V ein Untervektorraum des R^3 .

  (b) Zeige, daß $B = \{(a,b,c)^T\}$ eine Basis von V ist; hieraus folgt dann $\dim V = 1$.
  Zunächst ist B linear unabhängig, da $(a,b,c)^T$ nicht der Nullvektor ist.
  Sei nun $(x.y,z)^T \in V, \lambda \in R$ mit $x = \lambda a$. Dann ist $y = \lambda b$ und $z = \lambda c$, also $(x,y,z)^T = \lambda(a,b,c)^T$. Also ist B ein Erzeugendensystem und daher wegen der linearen Unabhängigkeit eine Basis.

- 2. Lösung:

  (a) wie oben

  (b) Definiere $f : R^3 \to V$ durch $f((x,y,z)^T) = (x, xb/a, xc/a)^T$. Dann ist f ein Homomorphismus, Ker $f = \{(0,y,z)^T : y,z \in R\}$ und Im $f = V$. Nach der Dimensionsformel gilt dim(Im(f))=dim R^3− dim(Ker(f)), also $\dim V = 3 - 2 = 1$.
  Wie oben zeigt man, daß $B = \{(a,b,c)^T\}$ ein Erzeugendensystem ist; hieraus folgt, daß B eine Basis von V ist.

6. Aufgabels -l

7. Da f bijektiv ist, existiert die Umkehrabbildung $f^{-1} : W \to V$ und ist bijektiv. Es bleibt also zu zeigen, daß $f^{-1} : W \to V$ ein Homomorphismus ist.
Seien $x, y \in W, \lambda \mu \in K$. Da f bijektiv ist, existieren $a, b \in V$ mit $f(a) = x,\ f(b) = y$, also $f^{-1}(x) = a,\ f^{-1}(y) = b$. Dann ist $f^{-1}(\lambda x + \mu y) = f^{-1}(\lambda f(a) + \mu f(b))$
$= f^{-1}(f(\lambda a + \mu b) = \lambda a + \mu b = \lambda f^{-1}(x) + \mu f^{-1}(y)$.
Also ist f^{-1} ein Isomorphismus.