Technische Universität Clausthal
Institut für Mathematik
Dr. Thomas Maxsein

Math.Methoden in der Informatik
WS 1998/99
Klausur/Lösungen

1. Aufgabe
   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 Primteile von n :

   Induktionsanfang: $r = 1$, $n = p^\alpha$. Die positiven Teiler von n sind dann $1, p, p^2, \dots, p^\alpha$, und daher ist $\sum_{l \leq d \leq n,\, d|n} \varphi(d) = 1 + (p-1) + \dots + (p^\alpha - p^{\alpha-1}) = p^\alpha = n$.

   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 . Die positiven Teiler von n sind daher $t = q^0 t, qt, \dots, q^{\alpha t}$, wobei t die positiven Teiler von n' durchläuft. Also ist

   $$\sum_{l \leq d \leq n,\, d|n} \varphi(d) = \sum_{j=0} \sum_{t|n'} \varphi(q^j t) = \sum_{j=0}^{\alpha} \varphi(q^j) \sum_{t|n'} \varphi(t) = q^\alpha n' = n$$

   Das Induktionsprinzip liefert die Behauptung.

2. Aufgabe
   Ist $(b, m) = 1$, so ist nach dem Satz von EULER $b^{\varphi(m)} \equiv 1 \bmod m$ und daher $b^{k\varphi(m)+1} \equiv b \bmod m$ für alle $k \in Z$.
   Daher ist $11^s \equiv a^{13 \cdot s} \equiv a \bmod 100$ sicher erfüllt, wenn $13 \cdot s \equiv 1 \bmod \varphi(100)$ gilt. Es ist $\varphi(100) = \varphi(4 \cdot 25) = \varphi(4) \cdot \varphi(25) = 2 \cdot 20 = 40$. Also ist $13 \cdot s \equiv 1 \bmod 40$ zu lösen. Offenbar ist $13 \cdot 3 \equiv -1 \bmod 40$ und daher $13 \cdot 37 \equiv 13 \cdot (-3) \equiv 1 \bmod 40$. (Diese Kongruenz kann man natürlich auch mit Hilfe des EUKLIDischen Algorithmus' lösen). Eine mögliche Wahl ist also $s = 37$; es ist $11^{37} \equiv a \bmod 100$.
   Wegen $37 = 1 \cdot 32 + 0 \cdot 16 + 0 \cdot 8 + 1 \cdot 4 + 0 \cdot 2 + 1 \cdot 1$ ist $a \equiv 11^{37} \equiv 11 \cdot 11^4 \cdot 11^{32} \bmod 100$. Es ist $11^2 \equiv 21 \bmod 100$, $11^4 \equiv 21^2 \equiv 41 \bmod 100$. $11^8 \equiv 41^2 \equiv 81 \bmod 100$, $11^{16} \equiv 81^2 \equiv 61 \bmod 100$, $11^{32} \equiv 61^2 \equiv 21 \bmod 100$.
   Daher ist $a \equiv 11 \cdot 11^4 \cdot 11^{32} \equiv 11 \cdot 41 \cdot 21 \equiv 71 \bmod 100$.

3. Aufgabe

   (a) Verfahren:

      i. Für alle $m \in R$ ist $1 \cdot x + (-1) \cdot x = 0 \in Z$, also ist „$\sim$" reflexiv.

ii. Gelte $x \sim y$, also $\exists n \in N$ und $\exists m \in Z \setminus \{0\}$, so daß $nx+my \in Z$ gilt.
1. Fall: $m \in N$: Dann ist $my+nx \in Z$, also $y \sim x$.
2. Fall: $-m \in N$: Dann ist $(-m)y+(-n)x \in Z$, also $y \sim x$.
Also ist „$\sim$" symmetrisch.

iii. Gelte $x \sim y$ und $y \sim z$, also $\exists n_1,\, n_2 \in N$ und $\exists m_1,\, m_2 \in Z \setminus \{0\}$, so daß $n_1x+m_1y \in Z$ und $n_2y+m_2 \in Z$ gilt; dann ist $n_1n_2x+m_1n_2y \in Z$ und $m_1n_2y+m_1m_2z \in Z$, also $n_1n_2x+(-m_1m_2)z \in Z$; wegen $n_1n_2 \in N$ und $(-m_1m_2) \in Z$ gilt $x \sim z$. Also ist „$\sim$ " transitiv.

iv. Aus i. bis iii. folgt, daß „$\sim$ " eine Äquivalenzrelation ist.

(b) Es ist $x \sim 1 \Leftrightarrow \exists n \in N$ und $\exists m \in Z \setminus \{0\}$, so daß $nx+m \in Z$ gilt.
Es ist $x \sim 1 \Leftrightarrow \exists n \in N$, so daß $nx \in Z$ gilt$\Leftrightarrow x \in Q$.
Also ist $K(1) = Q$.
Es ist $x \sim \sqrt{2} \Leftrightarrow \exists n \in N$ und $\exists m \in Z \setminus \{0\}$, so daß $nx+m\sqrt{2} = k \in Z$ gilt $\Leftrightarrow \exists r \in Q$, $s \in Q \setminus \{0\}$, so daß $x = r+s\sqrt{2}$ gilt. $(r = \frac{k}{n},\, s = -\frac{m}{n})$; also ist $K(\sqrt{2}) = Q + Q \setminus \{0\} \cdot \sqrt{2}$

4. Aufgabe

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

i. f ist surjektiv: Sei $b \in K$, dann ist $e+b \in K$ und $f(e-b) = e+b-e = b$.

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

iii. f ist Homomorphismus: $f(a+b) = (a+b)-e = a-e+b-e+e = f(a) \oplus f(b)$;
$f(a \cdot b) = a \cdot b - e = a - e + b - e + (e - a - b + a \cdot b) = a-e+b-e+(a-e)\cdot(b-e) = f(a) \otimes f(b)$. (Mehrfach wurde die Kommutativität von K bezüglich „$+$" ausgenutzt und die Eigenschaften von e als Einselement von K bezüglich „$\cdot$ "). Da K ein Körper ist, ist $0 \neq e$; also ist $f(0+e) = 0 \neq e = f(e+e)$. Nach Satz 8.11(h) ist $(K,\, \oplus,\, \otimes)$ ein Körper, der wegen i. und ii. zu $(K,+,\cdot)$ isomorph ist.

(b) Für alle $a \in K$ ist $a \oplus (-e) = a$; daher ist $0^* := -e$ das neutrale Element von $(K,\oplus)$, und wegen $a \oplus (-a-e-e) = -e$ ist $-a-e-e$ invers zu $a \in K$.

(c) Für alle $a \in K$ ist $a \otimes 0 = a$; daher ist $e^* := 0$ das neutrale Element von $(K,\otimes)$; für $a \neq 0^* = -e$ ist $a+e \neq 0$; daher existiert $(e+a)^{-1} \in K$, und wegen $a \otimes -a\cdot(e+a)^{-1} = a+(-a)\cdot(e+a)^{-1}+a\cdot(-a)\cdot(e+a)^{-1} = (a\cdot(e+a)+(-a)+a\cdot(-a))\cdot(e+a)^{-1} = 0\cdot(e+a)^{-1} = 0 = e^*$ ist $-a\cdot(e+a)^{-1}$ invers zu $a \in K \setminus \{0^*\}$.

5. Aufgabe

(a) Wir verwenden das Unterraumkriterium. Offenbar ist das Nullpolynom $\in V$. Seien $f_1,\, f_2 \in V,\, \lambda,\, \mu \in R$. Dann ist $\lambda f_1 + \mu f_2 \in R_n[x]$ und $(\lambda f_1 + \mu f_2)(0) = \lambda f_1(0) + \mu f_2(0) = 0$; also ist $\lambda f_1 + \mu f_2 \in V$. Daher ist V ein Untervektorraum von $R_n[x]$.

(b) Es ist $[1,\, x,\, x^2,\, \ldots,\, x^n]$ eine Basis von $R_n[x]$; speziell ist $[1,\, x,\, x^2,\, \ldots,\, x^n]$ linear unabhängig. Ein Polynom $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in R_n[x]$ ist genau dann $\in V$, wenn $a_0 = 0$ ist. Daher ist $[x,\, x^2,\, \ldots,\, x^n]$ eine Basis von V , und es ist $\dim V = n$.

6. Aufgabe

(a) Für $z,\, w \in C,\, \lambda \in R$, ist $f(z+w) = \overline{z+w} = \overline{z} + \overline{w} = f(z) + f(w)$ und $f(\lambda z) = \overline{\lambda z} = \overline{\lambda} \cdot \overline{z} = \lambda \cdot \overline{z} = \lambda \cdot f(z)$. Also ist f ein Homomorphismus. Die Bijektivität von f ist klar.

(b) Für $z \in C,\, \lambda \in C$ ist $f(\lambda z) = \overline{\lambda \cdot z} = \overline{\lambda} \cdot \overline{z} \neq \lambda \cdot f(z)$ (im allgemeinen). Also ist f nicht linear.