

Mathematik für Informatiker I
Prof. Dr. Frank-Olaf Schreyer, Janko Böhm
Übungsblatt 2 Musterlösung

1. $\mathbb{Q}[x]$ bezeichne die Menge aller Polynome mit rationalen Koeffizienten.

Sei

$$p(x) := a_d x^d + \dots + a_1 x + a_0 \in \mathbb{Q}[x]$$

ein Polynom vom Grad d , welches für große $n \in \mathbb{Z}$ ganzzahlige Werte annimmt, d.h. $\exists n_0 \in \mathbb{Z}$, sodaß gilt $p(n) \in \mathbb{Z} \forall n \geq n_0, n \in \mathbb{Z}$.

Zeigen Sie $\exists \alpha_0, \dots, \alpha_d \in \mathbb{Z}$, sodaß

$$p(x) = \sum_{k=0}^d \alpha_k \binom{x+k}{k}$$

Dabei sei

$$\binom{x+k}{k} := \prod_{j=1}^k \frac{x+j}{j} \in \mathbb{Q}[x]$$

Hinweis: Verwenden Sie Induktion nach d und das Differenzenpolynom $\Delta p \in \mathbb{Q}[x]$ definiert für $p \in \mathbb{Q}[x]$ durch

$$\Delta p(x) := p(x) - p(x-1)$$

Lösung:

Wir zeigen zunächst, daß jedes Polynom $p(x) = a_d x^d + \dots + a_1 x + a_0 \in \mathbb{Q}[x]$ eine eindeutig bestimmte Darstellung

$$p(x) = c_0 \cdot v_0(x) + \dots + c_d \cdot v_d(x)$$

mit

$$v_k(x) := \binom{x+k}{k}$$

und $c_0, \dots, c_d \in \mathbb{Q}$ hat.

Beweis mit Induktion nach dem Grad d :

Induktionsanfang $d = 0$:

Da $v_0 = 1$ ist, haben wir $c_0 = a_0$.

Induktionsschritt $d-1 \mapsto d$:

Wir schreiben

$$p(x) = a_d \cdot d! \cdot v_d + \underbrace{\left((a_{d-1} x^{d-1} + \dots + a_1 x + a_0) - a_d (d! \cdot v_d - x^d) \right)}_{=: q(x)}$$

$d! \cdot v_d - x^d$ und damit $q(x)$ hat Grad $d-1$ und damit gibt es nach Induktionsvoraussetzung eindeutig bestimmte $c_0, \dots, c_{d-1} \in \mathbb{Q}$ mit

$$q(x) = c_{d-1} v_{d-1} + \dots + c_1 v_1 + c_0 v_0$$

Es muß dann gelten

$$c_d = a_d \cdot d!$$

Nun zeigen wir mit Induktion nach dem Grad d , daß wenn es ein $n_0 \in \mathbb{Z}$ gibt, sodaß $p(n) \in \mathbb{Z} \forall n \geq n_0, n \in \mathbb{Z}$ schon

$$c_0, \dots, c_d \in \mathbb{Z}$$

sind:

Induktionsanfang $d = 0$:

$p(x) = a_0$ unabhängig von x , also muß $a_0 \in \mathbb{Z}$ sein.

Induktionsschritt $d - 1 \mapsto d$:

Es gilt

$$\Delta v_k(x) = \Delta \binom{x+k}{k} = \binom{x+k}{k} - \binom{x-1+k}{k} = \binom{x+k-1}{k-1} = v_{k-1}(x)$$

für $k \geq 1$ und $\Delta v_0(x) = 0$, also

$$\begin{aligned} \Delta p(x) &= p(x) - p(x-1) \\ &= (c_0 \cdot v_0(x) + \dots + c_d \cdot v_d(x)) - (c_0 \cdot v_0(x-1) + \dots + c_d \cdot v_d(x-1)) \\ &= c_0 \cdot \Delta v_0(x) + c_1 \cdot \Delta v_1(x) + \dots + c_d \cdot \Delta v_d(x) = c_1 \cdot v_0(x) + \dots + c_d \cdot \Delta v_{d-1}(x) \end{aligned}$$

Da $\Delta p(n)$ ein Polynom vom Grad $d-1$ ist, und $\Delta p(n) = p(n) - p(n-1) \in \mathbb{Z}$ für alle $n \geq n_0 + 1, n \in \mathbb{Z}$ gilt, folgt aus der Induktionsvoraussetzung, daß $c_1, \dots, c_d \in \mathbb{Z}$ sind.

Da

$$p(n) - (c_1 \cdot v_1(n) + \dots + c_d \cdot v_d(n)) \in \mathbb{Z}$$

für $n \geq \max\{n_0, 0\}$ ist auch $c_0 \in \mathbb{Z}$.

Bemerkung: Es folgt $p(n) \in \mathbb{Z} \forall n \in \mathbb{Z}$, denn

$$v_k(-n) = (-1)^k v_k(n+k) \in \mathbb{Z}$$

2. Äquivalenzrelationen:

(a) Wir definieren die folgende Äquivalenzrelation auf $M := \mathbb{N} \times \mathbb{N}$ durch $(a, b) \sim (c, d)$ genau dann, wenn $a + d = b + c$.

1. Zeigen Sie, daß dies eine Äquivalenzrelation auf M ist.
2. Beschreiben Sie die Äquivalenzklassen $[(1, 1)]$ und $[(3, 1)]$.
3. Definieren Sie die Addition von Äquivalenzklassen durch

$$[(a, b)] + [(c, d)] := [(a + c, b + d)]$$

Zeigen Sie, daß diese Addition wohldefiniert ist, d.h. unabhängig von den gewählten Repräsentanten der Äquivalenzklassen ist.

4. Zeigen Sie $[(a, b)] + [(2, 2)] = [(a, b)]$ und $[(2, 5)] + [(7, 5)] = [(1, 2)]$
5. Kennen Sie die Menge der Äquivalenzklassen $M/\sim$ unter anderem Namen?

Lösung:

1. Reflexivität:

$$(a, b) \sim (a, b) \quad \forall (a, b) \in M, \text{ denn } a + b = a + b.$$

Symmetrie:

Für $(a, b), (c, d) \in M$ gilt:

$$(a, b) \sim (c, d) \Leftrightarrow a + d = b + c \Leftrightarrow b + c = a + d \Leftrightarrow (c, d) \sim (a, b)$$

Transitivität:

Seien $(a, b), (c, d), (g, h) \in M$ mit

$$(a, b) \sim (c, d) \text{ und } (c, d) \sim (g, h)$$

d.h. $a + d = b + c$ und $c + h = d + g$. Addieren liefert

$$a + d + c + h = b + c + d + g$$

also

$$a + h = b + g$$

d.h. $(a, b) \sim (g, h)$.

2. Wir haben

$$[(1, 1)] = \{(a, b) \in M \mid a + 1 = b + 1\} = \{(a, a) \mid a \in \mathbb{N}\}$$

$$[(3, 1)] = \{(a, b) \in M \mid a + 1 = b + 3\} = \{(b + 2, b) \mid b \in \mathbb{N}\}$$

3. Wegen der Symmetrie genügt es zu zeigen: Sind $(a, b), (c, d), (g, h) \in M$ mit $[(c, d)] = [(g, h)]$, also $c + h = d + g$, dann gilt

$$[(a + c, b + d)] = [(a + g, b + h)]$$

Dies ist richtig, denn

$$(a + c) + (b + h) = a + b + (c + h) = a + b + (d + g) = (b + d) + (a + g)$$

4. Wir haben

$$\begin{aligned}
 [(a, b)] + [(2, 2)] &= [(a + 2, b + 2)] \\
 &= \{(c, d) \in M \mid c + b + 2 = a + 2 + d\} \\
 &= \{(c, d) \in M \mid c + b = a + d\} \\
 &= [(a, b)]
 \end{aligned}$$

und

$$\begin{aligned}
 [(2, 5)] + [(7, 5)] &= [(9, 10)] \\
 &= \{(c, d) \in M \mid c + 10 = 9 + d\} \\
 &= \{(c, d) \in M \mid c + 2 = 1 + d\} \\
 &= [(1, 2)]
 \end{aligned}$$

5. Betrachte die Abbildung

$$\begin{aligned}
 \alpha : \quad (M / \sim) &\rightarrow \mathbb{Z} \\
 [(a, b)] &\mapsto a - b
 \end{aligned}$$

α ist wohldefiniert:

Ist $(c, d) \in [(a, b)]$, dann gilt $c - d = a - b$.

α ist surjektiv:

Sei $n \in \mathbb{Z}$. Ist $n \geq 0$, dann ist $n = \alpha([(n, 0)])$. Ist $n < 0$, dann ist $n = \alpha([(0, -n)])$.

α ist injektiv:

Seien $(a, b), (c, d) \in M$ mit

$$\alpha([(a, b)]) = \alpha([(c, d)])$$

also $a - b = c - d$. Dann ist

$$a + d = c + b$$

also

$$[(a, b)] = [(c, d)]$$

Die bijektive Abbildung α respektiert die Addition:

$$\begin{aligned}
 \alpha([(a, b)] + [(c, d)]) &= \alpha([(a + c, b + d)]) \\
 &= (a + c) - (b + d) \\
 &= (a - b) + (c - d) \\
 &= \alpha([(a, b)]) + \alpha([(c, d)])
 \end{aligned}$$

- (b) Betrachten Sie die Menge $M := \mathbb{R}^2 \setminus \{(0,0)\}$, d.h. die Menge aller Punkte der reellen Ebene ohne den 0-Punkt.

Wir definieren eine Äquivalenzrelation auf $M \times M$ durch $(x, y) \sim (x', y')$ genau dann, wenn es eine Gerade durch den Nullpunkt $(0,0) \in \mathbb{R}^2$ gibt, auf der sowohl der Punkt (x, y) als auch der Punkt (x', y') liegen.

1. Zeigen Sie, daß dies tatsächlich eine Äquivalenzrelation ist.
2. Finden Sie eine geometrische Darstellung der Menge der Äquivalenzklassen $M/\sim$ indem Sie in jeder Äquivalenzklasse einen geeigneten Repräsentanten wählen.

Lösung:

1. Reflexivität:

$(x, y) \sim (x, y)$, denn jeder Punkt liegt auf einer Geraden durch den 0-Punkt.

Symmetrie:

Die Definition von $\sim$ ist symmetrisch in (x, y) und (x', y') .

Transitivität:

Seien $(x, y), (x', y') \in M$. Es ist

$$(x, y) \sim (x', y') \Leftrightarrow \exists t \in \mathbb{R}_{\neq 0} \text{ mit } (x, y) = t \cdot (x', y')$$

Seien nun $(x, y), (x', y'), (x'', y'') \in M$ mit

$$(x, y) \sim (x', y') \text{ und } (x', y') \sim (x'', y'')$$

d.h. gibt es $s, t \in \mathbb{R}_{\neq 0}$ mit $(x, y) = t \cdot (x', y')$ und $(x', y') = s \cdot (x'', y'')$. Dann ist

$$(x, y) = (t \cdot s) \cdot (x'', y'')$$

d.h. $(x, y) \sim (x'', y'')$.

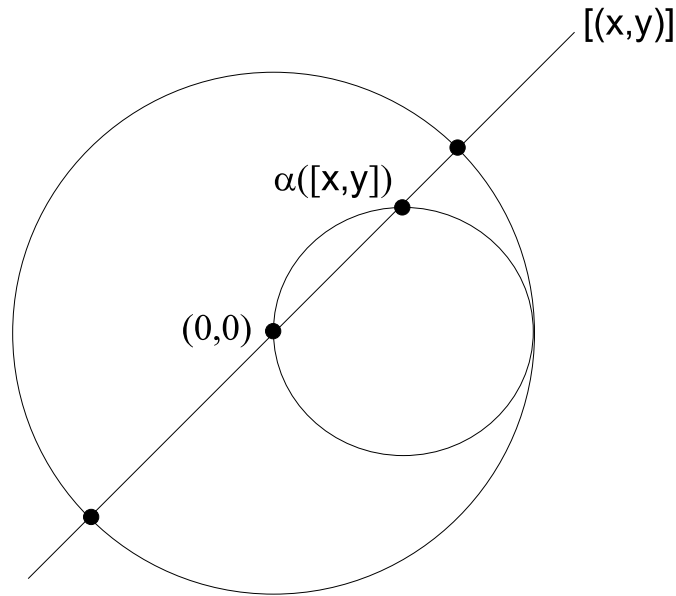
2. Wir zeigen: Für

$$K := \left\{ (x, y) \in \mathbb{R}^2 \mid \left(x - \frac{1}{2}\right)^2 + y^2 = \frac{1}{4} \right\}$$

ist die Abbildung

$$\alpha : \begin{array}{ccc} M/\sim & \rightarrow & K \\ [(x, y)] & \mapsto & \begin{cases} [(x, y)] \cap K & \text{für } x \neq 0 \\ (0, 0) & \text{für } x = 0 \end{cases} \end{array}$$

bijektiv. Ist $x \neq 0$, dann hat die punktierte Gerade $[(x, y)]$ genau einen Schnittpunkt mit K , den wir als Bildpunkt von $[(x, y)]$ unter α nehmen. Für $x = 0$ ist $[(x, y)]$ tangential an K im Punkt $(0, 0)$, den wir dann als Bildpunkt von $[(x, y)]$ unter α definieren.



Um den Bildpunkt von

$$[(x, y)] = \{t \cdot (x, y) \mid t \in \mathbb{R}, t \neq 0\}$$

explizit zu berechnen, müssen wir

$$\begin{aligned} \frac{1}{4} &= \left(t \cdot x - \frac{1}{2}\right)^2 + (t \cdot y)^2 \\ &= t^2 (x^2 + y^2) - x \cdot t + \frac{1}{4} \end{aligned}$$

also

$$t \cdot (t \cdot (x^2 + y^2) - x) = 0$$

nach t lösen und erhalten wegen $t \neq 0$, die Lösung

$$t = \frac{x}{(x^2 + y^2)}$$

und damit den gesuchten Schnittpunkt:

$$\begin{aligned} \alpha : M / \sim &\rightarrow K \\ [(x, y)] &\mapsto \left(\frac{x^2}{(x^2 + y^2)}, \frac{xy}{(x^2 + y^2)} \right) \end{aligned}$$

Wir rechnen noch anhand dieser Formel explizit nach, daß α wohldefiniert, surjektiv und injektiv ist:

- Wohldefiniertheit:

Seien $(x, y), (x', y') \in M$ mit $[(x, y)] = [(x', y')]$. Dann $\exists t \neq 0$ mit $(x', y') = t \cdot (x, y)$ und kürzen von t^2 liefert

$$\left(\frac{(tx)^2}{((tx)^2 + (ty)^2)}, \frac{txty}{((tx)^2 + (ty)^2)} \right) = \left(\frac{x^2}{(x^2 + y^2)}, \frac{xy}{(x^2 + y^2)} \right)$$

- Injektivität:

Seien $(x, y), (x', y') \in M$ mit $\alpha([(x, y)]) = (u, v) = \alpha([(x', y')])$. Ist $u \neq 0$, dann ist $x, x' \neq 0$ und

$$\frac{y}{x} = \frac{v}{u} = \frac{y'}{x'}$$

also $[(x, y)] = [(x', y')]$. Ist $u = 0$, dann muß auch $x = x' = 0$ sein, also $[(0, y)] = [(0, y')]$.

- Surjektivität:

Sei $(x, y) \in K$. Es gilt dann

$$x = x^2 + y^2$$

Für $x \neq 0$ ist also

$$\alpha([(x, y)]) = \left(x \frac{x}{(x^2 + y^2)}, y \frac{x}{(x^2 + y^2)} \right) = (x, y)$$

Für $x = 0$ haben wir auch $y = 0$ und

$$(0, 0) = \alpha([0, v])$$

für jedes $v \neq 0$.

3. Sei M eine **unendliche** Menge. Zeigen Sie:

- (a) Es gibt keine surjektive Abbildung $\varphi : M \rightarrow 2^M$.

Lösung:

Angenommen wir haben eine surjektive Abbildung $\varphi : M \rightarrow 2^M$. Wir betrachten

$$D := \{m \in M \mid m \notin \varphi(m)\}$$

$D \subset M$, also $D \in 2^M$, und φ ist nach Annahme surjektiv $\Rightarrow$

$$\exists a \in M : \varphi(a) = D$$

Ist $a \in D \Rightarrow a \notin \varphi(a) = D$ ein Widerspruch.

Ist $a \notin D = \varphi(a) \Rightarrow a \in D$ ein Widerspruch.

- (b) Es gibt keine injektive Abbildung $\psi : 2^M \rightarrow M$.

Lösung:

Angenommen wir haben eine injektive Abbildung $\psi : 2^M \rightarrow M$. Für $m \in M$ ist dann $\psi^{-1}(m)$ ein Element von 2^M . Wir betrachten

$$A := \{m \in \psi(2^M) \mid m \notin \psi^{-1}(m)\}$$

$A \subset M$, also $A \in 2^M$. Sei

$$b := \psi(A)$$

Da ψ injektiv ist, gilt

$$\psi^{-1}(b) = A$$

Ist $b \in A \Rightarrow b \notin \psi^{-1}(b) = A$ ein Widerspruch.

Ist $b \notin A = \psi^{-1}(b) \Rightarrow b \in A$ ein Widerspruch.

4. Lösen Sie folgende simultane Kongruenzen:

$$\begin{aligned}(1) \quad & x \equiv 5 \pmod{6} \\(2) \quad & x \equiv 8 \pmod{15} \\(3) \quad & x \equiv 3 \pmod{10}\end{aligned}$$

Lösung:

Wir verwenden:

A Seien $a, b \in \mathbb{Z}$ und $n, m \in \mathbb{Z}_{>0}$. Dann sind die simultanen Kongruenzen

$$\begin{aligned}x &\equiv a \pmod{n} \\x &\equiv b \pmod{m}\end{aligned} \tag{I}$$

genau dann lösbar wenn

$$a \equiv b \pmod{\text{ggT}(n, m)}$$

Die Lösung ist eindeutig modulo dem $\text{kgV}(n, m)$.

Sei $d := \text{ggT}(n, m)$ und $k \in \mathbb{Z}$ mit

$$a = b + k \cdot d$$

und schreiben wir mit $u, v \in \mathbb{Z}$

$$d = u \cdot n + v \cdot m$$

dann sind die Lösungen der simultanen Kongruenzen (I) genau die x mit

$$x \equiv (a - k \cdot u \cdot n) \pmod{\text{kgV}(n, m)}$$

B Haben wir nun 3 (oder auch mehr) Kongruenzen

$$\begin{aligned}(1) \quad & x \equiv a_1 \pmod{n_1} \\(2) \quad & x \equiv a_2 \pmod{n_2} \\(3) \quad & x \equiv a_3 \pmod{n_3}\end{aligned}$$

mit $a_1, a_2, a_3 \in \mathbb{Z}$ und $n_1, n_2, n_3 \in \mathbb{Z}_{>0}$ gegeben, dann gilt:

$$\left\{ \begin{array}{l} \left\{ \begin{array}{l} (1) \\ (2) \end{array} \right\} \\ (3) \end{array} \right\} \Leftrightarrow \begin{array}{l} (1') \quad x \equiv y \pmod{\text{kgV}(n_1, n_2)} \\ (3) \quad x \equiv a_3 \pmod{n_3} \end{array} \right\} \Leftrightarrow x \equiv z \pmod{\text{kgV}(n_1, n_2, n_3)}$$

wobei wir y und die 1. Äquivalenz durch Anwendung von (A) auf (1) und (2) und z und die 2. Äquivalenz durch Anwendung von (A) auf (1') und (3) erhalten.

Lösen wir nun zunächst die Kongruenzen

$$\begin{aligned}(1) \quad & x \equiv 5 \pmod{6} \\(2) \quad & x \equiv 8 \pmod{15}\end{aligned}$$

In der Lösungsformel (A) ist

$$\begin{aligned}a &= 5 & n &= 6 \\b &= 8 & m &= 15 \\d &= ggT(6, 15) = 3 \\kgV(6, 15) &= 30\end{aligned}$$

Wir schreiben

$$a = 5 = 8 + (-1) \cdot 3 = b + k \cdot d$$

und mit dem erweiterten Euklidischen Algorithmus

$$d = 3 = (-2) \cdot 6 + 1 \cdot 15 = u \cdot n + v \cdot m$$

Dann ist

$$a - k \cdot u \cdot n = 5 - (-1) \cdot (-2) \cdot 6 = -7$$

und somit die Lösungen von (1) und (2) genau die x mit

$$x \equiv 23 \bmod 30$$

Schließlich lösen wir die simultanen Kongruenzen

$$\begin{aligned}(1') \quad x &\equiv 23 \bmod 30 \\(2) \quad x &\equiv 3 \bmod 10\end{aligned}$$

und sehen sofort, daß die Lösungen genau die x sind mit

$$x \equiv 23 \bmod 30$$

Wir können dies auch nochmals mit (A) nachrechnen:

$$\begin{aligned}a &= 23 & n &= 90 \\b &= 3 & m &= 10 \\d &= ggT(30, 10) = 10 \\kgV(10, 30) &= 30\end{aligned}$$

wir schreiben

$$d = 10 = 0 \cdot 90 + 1 \cdot 10 = u \cdot n + v \cdot m$$

und erhalten

$$a - k \cdot u \cdot n = 23$$